



Motorola Point-to-Multipoint (PMP) Solutions User Guide

supporting Release 9.4.2

PMP 100, PMP 400

PTP 100, PTP 200

Issue 1

May 2010



includes

Planning Guide

Installation and Configuration Guide

Operations Guide

Reference



Notices

See the following information:

- important regulatory and legal notices in Section 36 on Page 499.
- personal safety guidelines in Section 15 on Page 173.

Trademarks, Product Names, and Service Names

MOTOROLA, the stylized M Logo and all other trademarks indicated as such herein are trademarks of Motorola, Inc.® Reg. U.S. Pat & Tm. Office. Canopy is a registered trademark and MOTOwi4 is a trademark of Motorola, Inc. All other product or service names are the property of their respective owners.

Adobe Reader is a registered trademark of Adobe Systems Incorporated.

Java and all other Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation, and Windows XP is a trademark of Microsoft Corporation.

© 2010 Motorola, Inc. All rights reserved.

http://www.motorola.com/Business/US-EN/Business+Solutions/Industry+Solutions/Wireless+Operators/Wireless+Broadband+Solutions/wi4+Fixed_US-EN

TABLE OF SECTIONS

Guide To This User Guide	31
Overview of PMP Solutions	43
Planning Guide	127
Installation and Configuration Guide	171
Operations Guide	371
Reference Information	495
Glossary	515

TABLE OF CONTENTS

GUIDE TO THIS USER GUIDE.....31

1	New in This Issue.....	33
1.1	New Products and Features Described in This Guide	33
1.2	Portfolio of Wireless Broadband Solutions	33
1.3	Products Covered by This User Guide.....	33
1.4	Products Not Covered by This User Guide	34
1.5	Software Compatibility Described in This User Guide.....	34
2	Using This User Guide	35
2.1	Finding the Information You Need.....	35
2.1.1	<i>Becoming Familiar with This User Guide</i>	<i>35</i>
2.1.2	<i>Searching This User Guide</i>	<i>37</i>
2.1.3	<i>Finding Parameter and Field Definitions for Module Web Pages</i>	<i>37</i>
2.2	Interpreting Typeface and Other Conventions	40
2.3	Getting Additional Help.....	41
2.4	Sending Feedback	41

OVERVIEW OF PMP SOLUTIONS43

3	Advancing from Research to Implementation	45
4	Realizing a Wireless Ethernet Bridge Network	47
5	Exploring the Scope of Solutions	49
5.1	Product Names.....	49
5.2	Network Components.....	50
5.2.1	<i>Access Point Module Other Than 900-Mhz</i>	<i>50</i>
5.2.2	<i>Access Point Cluster</i>	<i>50</i>
5.2.3	<i>Subscriber Module Other Than 900-MHz</i>	<i>51</i>
5.2.4	<i>900-MHz AP and SM.....</i>	<i>52</i>
5.2.5	<i>PTP Series 100 Bridges.....</i>	<i>53</i>
5.2.6	<i>PTP 200 Series Bridges.....</i>	<i>53</i>

5.2.7	<i>PTP 300 Series Bridges</i>	54
5.2.8	<i>PTP 400 Series Bridges</i>	54
5.2.9	<i>PTP 500 Series Bridges</i>	54
5.2.10	<i>PTP 600 Series Bridges</i>	55
5.2.11	<i>Radio Adjustable Power Capabilities</i>	56
5.2.12	<i>Cluster Management Module-2 (Part 1008CK-2)</i>	56
5.2.13	<i>Cluster Management Module micro (Part 1070CK)</i>	56
5.2.14	<i>CMM4 (Part 1090CK)</i>	58
5.2.15	<i>Optional Ethernet Switch in CMM4</i>	59
5.2.16	<i>GPS Antenna (Part GPSANTPNM03D)</i>	60
5.2.17	<i>Surge Suppressor (Part 600SS)</i>	60
5.2.18	<i>Accessory Components</i>	60
5.3	Frequency Band Ranges	66
5.4	Product Comparisons	67
5.4.1	<i>Product Applications</i>	67
5.4.2	<i>Link Performance and Encryption Comparisons</i>	67
5.4.3	<i>Cluster Management Product Comparison</i>	70
5.5	Antennas for 900-MHz Connectorized Modules	71
5.6	Adjunctive Software Products	73
5.7	Prizm	74
5.7.1	<i>Network Definition and Element Discovery</i>	74
5.7.2	<i>Monitoring and Fault Management</i>	75
5.7.3	<i>Element Management</i>	75
5.7.4	<i>BAM Subsystem in Prizm</i>	76
5.7.5	<i>Northbound Interface</i>	76
5.8	License Management	77
5.9	Specifications and Limitations	78
5.9.1	<i>Radios</i>	78
5.9.2	<i>Cluster Management Products</i>	78
5.9.3	<i>600SS Surge Suppressor</i>	78
6	Differentiating Among Components	79
6.1	Interpreting Model Number	79
6.2	Sorted Model Numbers	81
6.3	Interpreting Electronic Serial Number (ESN)	82
6.4	Finding the Model (Part) Number and ESN	83

7	Link Characteristics	85
7.1	Understanding Bandwidth Management	85
7.1.1	Downlink Frame	85
7.1.2	Uplink Frame	85
7.1.3	Slot Calculation	86
7.1.4	Startup Sequence	86
7.1.5	Data Transfer Capacity	86
7.1.6	Maximum Information Rate (MIR) Parameters	87
7.1.7	Committed Information Rate	88
7.1.8	Bandwidth from the SM Perspective	89
7.1.9	Interaction of Burst Allocation and Sustained Data Rate Settings	89
7.1.10	High-priority Bandwidth	89
7.1.11	Traffic Scheduling	91
7.1.12	2X Operation	92
7.1.13	3X Operation	95
7.1.14	Engineering for 2X and 3X Operation	96
7.2	Understanding Synchronization	96
7.2.1	GPS Synchronization	97
7.2.2	Passing Sync in a Single Hop	98
7.2.3	Passing Sync in an Additional Hop	99
8	Meeting Link Requirements	101
8.1	AP-SM Links	101
8.2	BH-BH Links	103
9	Previewing Network Configurations	105
9.1	Viewing Typical Layouts	105
9.2	Viewing Case Studies	107
10	Accessing Features	109
10.1	Activating Features	117
10.1.1	Fixed License Keys	117
10.2	Enabling Features	117
11	Acquiring Proficiencies	119
11.1	Understanding RF Fundamentals	119
11.2	Understanding IP Fundamentals	119
11.3	Acquiring a Demonstration Kit	119

11.3.1	900-MHz with Integrated Antenna and Band-pass Filter Demonstration Kit	119
11.3.2	900-MHz with Connectorized Antenna Demonstration Kit	120
11.3.3	2.4-GHz with Adjustable Power Set to High Demonstration Kit	120
11.3.4	5.2-GHz Demonstration Kit	120
11.3.5	5.4-GHz Demonstration Kit	121
11.3.6	5.7-GHz with Connectorized Antenna and Adjustable Power Set to Low Demonstration Kit	121
11.3.7	Demonstration Kit Part Numbers	122
11.4	Acquiring a Starter Kit	122
11.4.1	900-MHz with Integrated Antenna and Band-pass Filter Starter Kit	122
11.4.2	900-MHz with Connectorized Antenna Starter Kit	123
11.4.3	2.4-GHz with Adjustable Power Set to High Starter Kit	123
11.4.4	5.2-GHz Starter Kit	123
11.4.5	5.4-GHz FSK Starter Kit	123
11.4.6	5.4-GHz OFDM Starter Kits	124
11.4.7	5.7-GHz with Integrated Antenna Starter Kit	124
11.4.8	Starter Kit Part Numbers	125
11.5	Evaluating Training Options	125
11.6	Attending On-line Knowledge Sessions	125

PLANNING GUIDE 127

12	Engineering Your RF Communications	129
12.1	Anticipating RF Signal Loss	129
12.1.1	Understanding Attenuation	129
12.1.2	Calculating Free Space Path Loss	129
12.1.3	Calculating Rx Signal Level	129
12.1.4	Calculating Fade Margin	130
12.2	Analyzing the RF Environment	131
12.2.1	Mapping RF Neighbor Frequencies	131
12.2.2	Anticipating Reflection of Radio Waves	132
12.2.3	Noting Possible Obstructions in the Fresnel Zone	132
12.2.4	Radar Signature Detection and Shutdown	133
12.3	Using Jitter to Check Received Signal Quality (FSK Only)	136
12.4	Using Link Efficiency to Check FSK Received Signal Quality	136
12.4.1	Comparing Efficiency in 1X Operation to Efficiency in 2X Operation	136

12.4.2	<i>When to Switch from 2X to 1X Operation Based on 60% Link Efficiency...</i>	137
12.5	Considering Frequency Band Alternatives	138
12.5.1	900-MHz Channels.....	138
12.5.2	2.4-GHz Channels.....	138
12.5.3	4.9-GHz OFDM Channels	139
12.5.4	5.2-GHz Channels.....	139
12.5.5	5.4-GHz FSK Channels.....	140
12.5.6	5.4-GHz OFDM Channels	140
12.5.7	5.7-GHz Channels.....	141
12.5.8	Channels Available for PTP 400 and PTP 600 Radios.....	142
12.5.9	Example Channel Plans for FSK AP Clusters.....	142
12.5.10	Multiple FSK Access Point Clusters.....	144
12.5.11	Example Channel Plan for OFDM AP Cluster.....	145
12.5.12	Multiple OFDM Access Point Clusters	145
12.6	Selecting Sites for Network Elements	146
12.6.1	Resources for Maps and Topographic Images	147
12.6.2	Surveying Sites.....	147
12.6.3	Assuring the Essentials.....	148
12.6.4	Finding the Expected Coverage Area	149
12.6.5	Clearing the Radio Horizon	149
12.6.6	Calculating the Aim Angles	149
12.7	Collocating Modules	150
12.8	Deploying a Remote AP	151
12.8.1	Remote AP Performance	152
12.8.2	Example Use Case for RF Obstructions	152
12.8.3	Example Use Case for Passing Sync	153
12.8.4	Physical Connections Involving the Remote AP.....	154
12.9	Diagramming Network Layouts	155
12.9.1	Accounting for Link Ranges and Data Handling Requirements.....	155
12.9.2	Avoiding Self Interference	155
12.9.3	Avoiding Other Interference	157
13	Engineering Your IP Communications	159
13.1	Understanding Addresses	159
13.1.1	IP Address.....	159
13.2	Dynamic or Static Addressing	159
13.2.1	When a DHCP Server is Not Found.....	159

13.3	Network Address Translation (NAT).....	160
13.3.1	<i>NAT, DHCP Server, DHCP Client, and DMZ in SM.....</i>	160
13.3.2	<i>NAT and VPNs.....</i>	165
13.4	Developing an IP Addressing Scheme.....	166
13.4.1	<i>Address Resolution Protocol.....</i>	166
13.4.2	<i>Allocating Subnets.....</i>	166
13.4.3	<i>Selecting Non-routable IP Addresses.....</i>	167
13.5	Translation Bridging.....	167
14	Engineering VLANs.....	169
14.1	Special Case VLAN Numbers.....	169
14.2	SM Membership in VLANs.....	169
14.3	Priority on VLANs (802.1p).....	170

INSTALLATION AND CONFIGURATION GUIDE 171

15	Avoiding Hazards.....	173
15.1	Exposure Separation Distances.....	173
15.1.1	<i>Details of Exposure Separation Distances Calculations and Power Compliance Margins.....</i>	173
15.2	Grounding the Equipment.....	176
15.2.1	<i>Grounding Infrastructure Equipment.....</i>	176
15.2.2	<i>Grounding SMs.....</i>	176
15.3	Conforming to Regulations.....	179
15.4	Protecting Cables and Connections.....	179
16	Testing the Components.....	181
16.1	Unpacking Components.....	181
16.2	Configuring for Test.....	181
16.2.1	<i>Configuring the Computing Device for Test.....</i>	181
16.2.2	<i>Default Module Configuration.....</i>	181
16.2.3	<i>Component Layout.....</i>	182
16.2.4	<i>Diagnostic LEDs.....</i>	183
16.2.5	<i>Standards for Wiring.....</i>	184
16.2.6	<i>Best Practices for Cabling.....</i>	184
16.2.7	<i>Recommended Tools for Wiring Connectors.....</i>	185
16.2.8	<i>Wiring Connectors.....</i>	185

16.2.9	<i>Alignment Tone—Technical Details</i>	186
16.3	Configuring a Point-to-Multipoint Link for Test	186
16.3.1	<i>Quick Start Page of the AP</i>	187
16.3.2	<i>Time Tab of the AP</i>	194
16.3.3	<i>Session Status Tab of the AP</i>	196
16.3.4	<i>Beginning the Test of Point-to-Multipoint Links</i>	200
16.3.5	<i>Remote Subscribers Tab of the AP</i>	201
16.3.6	<i>General Status Tab of the SM</i>	202
16.3.7	<i>Continuing the Test of Point-to-Multipoint Links</i>	205
16.3.8	<i>General Status Tab of the AP</i>	206
16.3.9	<i>Concluding the Test of Point-to-Multipoint Links</i>	210
16.4	Configuring a Point-to-Point Link for Test	211
16.4.1	<i>Quick Start Page of the BHM</i>	211
16.4.2	<i>Time Tab of the BHM</i>	214
16.4.3	<i>Beginning the Test of Point-to-Point Links</i>	216
16.4.4	<i>Continuing the Test of Point-to-Point Links</i>	220
16.4.5	<i>General Status Tab of the BHM</i>	221
16.4.6	<i>Concluding the Test of Point-to-Point Links</i>	224
17	Preparing Components for Deployment	225
17.1	Correlating Component-specific Information	225
17.2	Ensuring Continuing Access to the Modules.....	225
18	Configuring for the Destination	227
18.1	Configuring an AP for the Destination	227
18.1.1	<i>General Tab of the AP</i>	227
18.1.2	<i>IP Tab of the AP</i>	231
18.1.3	<i>Radio Tab of the AP</i>	233
18.1.4	<i>SNMP Tab of the AP</i>	241
18.1.5	<i>Quality of Service (QoS) Tab of the AP</i>	244
18.1.6	<i>Security Tab of the AP</i>	246
18.1.7	<i>VLAN Tab of the AP</i>	249
18.1.8	<i>VLAN Membership Tab of the AP</i>	252
18.1.9	<i>DiffServe Tab of the AP</i>	253
18.1.10	<i>Unit Settings Tab of the AP</i>	255
18.2	Configuring an SM for the Destination	256
18.2.1	<i>General Tab of the SM</i>	256

18.2.2	<i>NAT and IP Tabs of the SM with NAT Disabled</i>	260
18.2.3	<i>NAT and IP Tabs of the SM with NAT Enabled</i>	265
18.2.4	<i>Radio Tab of the SM</i>	271
18.2.5	<i>SNMP Tab of the SM</i>	274
18.2.6	<i>Quality of Service (QoS) Tab of the SM</i>	277
18.2.7	<i>Security Tab of the SM</i>	279
18.2.8	<i>VLAN Tab of the SM</i>	282
18.2.9	<i>VLAN Membership Tab of the SM</i>	285
18.2.10	<i>DiffServe Tab of the SM</i>	286
18.2.11	<i>Protocol Filtering Tab of the SM</i>	288
18.2.12	<i>PPPoE Tab of the SM</i>	289
18.2.13	<i>NAT Port Mapping Tab of the SM</i>	290
18.2.14	<i>Unit Settings Tab of the SM</i>	291
18.3	Setting the Configuration Source	292
18.4	Configuring a BH Timing Master for the Destination	294
18.4.1	<i>General Tab of the BHM</i>	295
18.4.2	<i>IP Tab of the BHM</i>	298
18.4.3	<i>Radio Tab of the BHM</i>	299
18.4.4	<i>SNMP Tab of the BHM</i>	303
18.4.5	<i>Security Tab of the BHM</i>	306
18.4.6	<i>VLAN tab of the BHM</i>	308
18.4.7	<i>DiffServe Tab of the BHM</i>	310
18.4.8	<i>Unit Settings Tab of the BHM</i>	311
18.5	Configuring a BH Timing Slave for the Destination	312
18.5.1	<i>General Tab of the BHS</i>	312
18.5.2	<i>IP Tab of the BHS</i>	316
18.5.3	<i>Radio Tab of the BHS</i>	318
18.5.4	<i>SNMP Tab of the BHS</i>	321
18.5.5	<i>Quality of Service (QoS) Tab of the BHS</i>	323
18.5.6	<i>Security Tab of the BHS</i>	324
18.5.7	<i>VLAN Tab of the BHS</i>	326
18.5.8	<i>DiffServe Tab of the BHS</i>	328
18.5.9	<i>Unit Settings Tab of the BHS</i>	329
18.6	Adjusting Transmitter Output Power	330

19	Installing Components	335
19.1	PDA Access to Modules.....	335
19.2	Installing an AP	338
19.2.1	Installing a PMP 100 Series AP	338
19.2.2	Installing a PMP 400 Series AP	339
19.3	Installing a Connectorized Flat Panel Antenna	344
19.4	Installing a GPS Antenna	345
19.5	Installing a Cluster Management Module	345
19.6	Installing an SM.....	345
19.6.1	Configuring the Laptop for Connection to SMS	345
19.6.2	Installing a PMP 100 Series SM.....	347
19.6.3	Installing a PMP 400 Series SM.....	353
19.7	Configuring an AP-SM Link.....	355
19.8	Monitoring an AP-SM Link.....	357
19.9	Installing a Reflector Dish.....	359
19.9.1	Both Modules Mounted at Same Elevation	359
19.9.2	Modules Mounted at Different Elevations	360
19.9.3	Mounting Assembly.....	360
19.10	Installing a BH Timing Master	361
19.10.1	Installing a PTP 100 Series BHM.....	361
19.10.2	Installing a PTP 200 Series BHM.....	363
19.11	Installing a BH Timing Slave	363
19.11.1	Installing a PTP 100 Series BHS.....	363
19.11.2	Installing a PTP 200 Series BHS.....	365
19.12	Upgrading a BH Link to BH20	365
19.13	Verifying a BH Link.....	365
20	Verifying System Functionality	369

OPERATIONS GUIDE **371**

21	Growing Your Network.....	373
21.1	Monitoring the RF Environment.....	373
21.1.1	Spectrum Analyzer.....	373
21.1.2	Graphical Spectrum Analyzer Display.....	374
21.1.3	Using the AP as a Spectrum Analyzer	375

21.2	Considering Software Release Compatibility	377
21.2.1	<i>Designations for Hardware in Radios</i>	377
21.2.2	<i>MIB File Set Compatibility</i>	378
21.3	Redeploying Modules.....	378
21.3.1	<i>Wiring to Extend Network Sync</i>	378
22	Securing Your Network	379
22.1	Isolating APs from the Internet.....	379
22.2	Encrypting Radio Transmissions.....	379
22.2.1	<i>DES Encryption</i>	379
22.2.2	<i>AES Encryption</i>	379
22.2.3	<i>AES-DES Operability Comparisons</i>	380
22.3	Managing Module Access by Passwords.....	381
22.3.1	<i>Adding a User for Access to a Module</i>	381
22.3.2	<i>Deleting a User from Access to a Module</i>	383
22.3.3	<i>Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH</i>	383
22.4	Requiring SM Authentication.....	385
22.5	Filtering Protocols and Ports	385
22.5.1	<i>Port Filtering with NAT Enabled</i>	385
22.5.2	<i>Protocol and Port Filtering with NAT Disabled</i>	385
22.6	Encrypting Downlink Broadcasts.....	387
22.7	Isolating SMs.....	387
22.8	Filtering Management through Ethernet.....	388
22.9	Allowing Management from Only Specified IP Addresses	388
22.10	Configuring Management IP by DHCP.....	388
23	Managing Bandwidth and Authentication	389
23.1	Managing Bandwidth without BAM.....	389
23.2	Bandwidth and Authentication Manager (BAM) Services and Features	389
23.2.1	<i>Bandwidth Manager Capability</i>	389
23.2.2	<i>Authentication Manager Capability</i>	391
24	Managing the Network From a Management Station (NMS)	393
24.1	Roles of Hardware and Software Elements	393
24.1.1	<i>Role of the Agent</i>	393
24.1.2	<i>Role of the Managed Device</i>	393
24.1.3	<i>Role of the NMS</i>	393

24.1.4	<i>Dual Roles for the NMS</i>	393
24.1.5	<i>Simple Network Management Protocol (SNMP) Commands</i>	393
24.1.6	<i>Traps from the Agent</i>	394
24.1.7	<i>AP SNMP Proxy to SMs</i>	394
24.2	Management Information Base (MIB)	394
24.2.1	<i>Cascading Path to the MIB</i>	394
24.2.2	<i>Object Instances</i>	395
24.2.3	<i>Management Information Base Systems and Interface (MIB-II)</i>	395
24.2.4	<i>Canopy Enterprise MIB</i>	396
24.3	Configuring Modules for SNMP Access	397
24.4	Objects Defined in the Canopy Enterprise MIB.....	398
24.4.1	<i>AP, SM, and BH Objects</i>	398
24.4.2	<i>AP and BH Timing Master Objects</i>	402
24.4.3	<i>SM and BH Timing Slave Objects</i>	406
24.5	Interface Designations in SNMP	409
24.6	Traps Provided in the Canopy Enterprise MIB	410
24.7	MIB Viewers	410
25	Using the Canopy Network Updater Tool (CNUT)	413
25.1	CNUT Functions.....	413
25.2	Network Element Groups	413
25.3	Network Layers	414
25.4	Script Engine	414
25.5	Software Dependencies for CNUT	414
25.6	CNUT Download	415
26	Using Informational Tabs in the GUI	417
26.1	Viewing General Status (All)	417
26.2	Viewing Session Status (AP, BHM).....	417
26.3	Viewing Remote Subscribers (AP, BHM)	418
26.4	Interpreting Messages in the Event Log (All)	418
26.4.1	<i>Time and Date Stamp</i>	418
26.4.2	<i>Event Log Data Collection</i>	418
26.4.3	<i>Messages that Flag Abnormal Events</i>	420
26.4.4	<i>Messages that Flag Normal Events</i>	420
26.5	Viewing the Network Interface Tab (All)	421
26.6	Viewing the Layer 2 Neighbors Tab (All).....	422

26.7	Interpreting Radio Statistics in the Scheduler Tab (All)	423
26.8	Viewing the List of Registration Failures (AP, BHM)	424
26.9	Interpreting Data in the Bridging Table (All)	425
26.10	Translation Table (SM)	425
26.11	Interpreting Data in the Ethernet Tab (All)	426
26.12	Interpreting RF Control Block Statistics in the Radio Tab (All)	428
26.13	Interpreting Data in the VLAN Tab (ALL)	430
26.14	Data VC (All)	431
26.15	Viewing Summary Information in the Overload Tab (All)	432
26.16	Filter (SM, BHS)	433
26.17	ARP (SM, BHS)	433
26.18	NAT Stats (SM)	433
	26.18.1 NAT DHCP Statistics (SM)	434
	26.18.2 Interpreting Data in the GPS Status Page (AP, BHM)	434
26.19	Accessing PPPoE Statistics About Customer Activities (SM)	435
27	Using Tools in the GUI	437
27.1	Using the Spectrum Analyzer Tool (SM, BHS)	437
27.2	Using the Alignment Tool (SM, BHS)	437
27.3	Using the Link Capacity Test Tool (All)	438
27.4	Using the AP Evaluation or BHM Evaluation Tool (SM, BHS)	441
27.5	Using the Frame Calculator Tool (All) for Collocation	446
27.6	Viewing the DFS Status Tab (All)	451
27.7	Using the SM Configuration Tool (AP, BHM)	452
27.8	Reviewing the Link Status Tool Results (AP)	453
27.9	Using the Remote Spectrum Analyzer Tool (AP)	454
27.10	Using the BER Results Tool (SM, BHS)	456
28	Maintaining Your Software	459
28.1	History of System Software Upgrades	459
	28.1.1 Release 8 Features	459
	28.1.2 Release 8 Fixes	460
	28.1.3 Release 9 Features	460
	28.1.4 Release 9 Fixes	460
28.2	History of CMMmicro Software Upgrades	461
28.3	Typical Contents of Release Notes	461

28.4	Typical Upgrade Process	461
28.4.1	<i>Downloading Software and Release Notes</i>	462
29	Rebranding Module Interface Screens	463
30	Toggling Remote Access Capability.....	467
30.1	Denying All Remote Access	467
30.2	Reinstating Remote Access Capability	467
31	Setting Up a Protocol Analyzer on Your Network.....	469
31.1	Analyzing Traffic at an SM	469
31.2	Analyzing Traffic at an AP or BH with No CMM	470
31.3	Analyzing Traffic at an AP or BH with a CMM.....	470
31.4	Example of a Protocol Analyzer Setup for an SM	471
32	Troubleshooting.....	479
32.1	General Planning for Troubleshooting.....	479
32.2	General Fault Isolation Process	479
32.3	Questions to Help Isolate the Problem.....	480
32.4	Secondary Steps	480
32.5	Procedures for Troubleshooting	481
32.5.1	<i>Module Has Lost or Does Not Establish Connectivity</i>	481
32.5.2	<i>NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity</i> .	482
32.5.3	<i>SM Does Not Register to an AP</i>	484
32.5.4	<i>BHS Does Not Register to the BHM</i>	485
32.5.5	<i>Module Has Lost or Does Not Gain Sync</i>	486
32.5.6	<i>Module Does Not Establish Ethernet Connectivity</i>	487
32.5.7	<i>Module Does Not Power Up</i>	487
32.5.8	<i>Power Supply Does Not Produce Power</i>	488
32.5.9	<i>CMM Does Not Pass Proper GPS Sync to Connected Modules</i>	489
32.5.10	<i>Module Software Cannot be Upgraded</i>	489
32.5.11	<i>Module Functions Properly, Except Web Interface Became Inaccessible</i> ..	489
33	Obtaining Technical Support.....	491
34	Getting Warranty Assistance.....	493

REFERENCE INFORMATION495

35	Administering Modules through telnet Interface	497
36	Regulatory and Legal Notices	499
36.1	Important Note on Modifications.....	499
36.2	National and Regional Regulatory Notices.....	499
36.2.1	<i>U.S. Federal Communication Commission (FCC) Notification</i>	<i>499</i>
36.2.2	<i>Industry Canada (IC) Notification</i>	<i>501</i>
36.2.3	<i>Regulatory Requirements for CEPT Member States (www.cept.org).....</i>	<i>502</i>
36.2.4	<i>European Union Notification for 5.7 GHz Product.....</i>	<i>503</i>
36.2.5	<i>Equipment Disposal</i>	<i>504</i>
36.2.6	<i>EU Declaration of Conformity for RoHS Compliance.....</i>	<i>504</i>
36.2.7	<i>UK Notification.....</i>	<i>504</i>
36.2.8	<i>Belgium Notification.....</i>	<i>504</i>
36.2.9	<i>Luxembourg Notification.....</i>	<i>505</i>
36.2.10	<i>Czech Republic Notification</i>	<i>505</i>
36.2.11	<i>Norway Notification</i>	<i>505</i>
36.2.12	<i>Greece Notification.....</i>	<i>505</i>
36.2.13	<i>Brazil Notification.....</i>	<i>505</i>
36.2.14	<i>Australia Notification.....</i>	<i>506</i>
36.2.15	<i>Labeling and Disclosure Table for China</i>	<i>506</i>
36.3	RF Exposure	507
36.4	Legal Notices	507
36.4.1	<i>Software License Terms and Conditions</i>	<i>507</i>
36.4.2	<i>Hardware Warranty in U.S.</i>	<i>509</i>
36.4.3	<i>Limit of Liability.....</i>	<i>509</i>
37	Additional Resources	511
38	History of Documentation	513

GLOSSARY.....515

LIST OF FIGURES

Figure 1: Pole-mounted AP cluster	50
Figure 2: OFDM AP - Antenna and Radio.....	50
Figure 3: Structure-mounted SM.....	51
Figure 4: OFDM SM, front and side views	51
Figure 5: Examples of antennas for 900-MHz modules	52
Figure 6: Dish-mounted 7.5- or 14-Mbps bridge	53
Figure 7: 21-Mbps bridge	53
Figure 8: PTP 300/400/500/600 Series Bridge common form	54
Figure 9: CMM2 enclosure.....	56
Figure 10: CMM2 pole-mounted	56
Figure 11: CMMmicro.....	57
Figure 12: Pole-mounted CMMmicro	57
Figure 13: CMM4 enclosure.....	59
Figure 14: CMM4	59
Figure 15: Motorola GPS antenna	60
Figure 16: 600SS surge suppressor	60
Figure 17: 27RD with mounted module.....	62
Figure 18: LENS mounted on a radio.....	62
Figure 19: SMMB1 SM support bracket.....	63
Figure 20: ACATHS-01 alignment headset.....	65
Figure 21: HSG-01 Housing.....	65
Figure 22: TDD dividing frames	86
Figure 23: Uplink and downlink rate caps adjusted to apply aggregate cap.....	88
Figure 24: Uplink and downlink rate cap adjustment example.....	88
Figure 25: One unsynchronized AP in cluster.....	97
Figure 26: GPS timing throughout the network (FSK shown)	98
Figure 27: Additional link to extend network sync, Design 3.....	99
Figure 28: Additional link to extend network sync, Design 4.....	100
Figure 29: Additional link to extend network sync, Design 5.....	100
Figure 30: Typical network layout with no BH.....	105
Figure 31: Typical network layout with BH.....	106
Figure 32: Typical multiple-BH network layout.....	106

Figure 33: Determinants in Rx signal level.....	130
Figure 34: Example layout of 7 FSK Access Point clusters	144
Figure 35: Example layout of 16 OFDM Access Point sectors	146
Figure 36: Fresnel zone in line of sight link.....	148
Figure 37: Fresnel zone in near line of sight link.....	148
Figure 38: Fresnel zone in non-line of sight link.....	148
Figure 39: Variables for calculating angle of elevation (and depression).....	149
Figure 40: Double-hop backhaul links.....	150
Figure 41: Remote AP deployment.....	151
Figure 42: Example 900-MHz remote AP behind 2.4-GHz SM.....	153
Figure 43: Remote AP wired to SM that also serves a customer.....	154
Figure 44: Remote AP wired to SM that serves as a relay	155
Figure 45: NAT Disabled implementation	161
Figure 46: NAT with DHCP Client and DHCP Server implementation.....	162
Figure 47: NAT with DHCP Client implementation.....	163
Figure 48: NAT with DHCP Server implementation	164
Figure 49: NAT without DHCP implementation.....	165
Figure 50: Example of IP address in Class B subnet.....	166
Figure 51: Base cover, detached and attached, FSK module.....	182
Figure 52: Base cover, detached and attached, OFDM module	182
Figure 53: RJ-45 pinout for straight-through Ethernet cable	185
Figure 54: RJ-45 pinout for crossover Ethernet cable.....	186
Figure 55: RJ-11 pinout for straight-through sync cable	186
Figure 56: Quick Start tab of AP, example.....	188
Figure 57: Region Settings tab of AP, example	189
Figure 58: Radio Carrier Frequency tab of AP, example	190
Figure 59: Synchronization tab of AP, example	191
Figure 60: LAN IP Address tab of AP, example.....	192
Figure 61: Review and Save Configuration tab of AP, example	193
Figure 62: Time tab of AP, example.....	194
Figure 63: Session Status tab data from AP, example	196
Figure 64: Remote Subscribers tab of AP, example	201
Figure 65: General Status tab of SM, example	202
Figure 66: General Status tab of AP (5.7 GHz), example	206

Figure 67: General Status tab of AP (900 MHz), example.....	207
Figure 68: Quick Start tab of BHM, example.....	212
Figure 69: Time tab of BHM, example	214
Figure 70: Remote Subscribers tab of BHM, example.....	216
Figure 71: General Status tab of BHS, example	216
Figure 72: General Status tab of BHM, example	221
Figure 73: General tab of AP, example.....	227
Figure 74: IP tab of AP, example	231
Figure 75: Radio tab of AP (900 MHz), example	233
Figure 76: Radio tab of AP (5.4 GHz), example.....	234
Figure 77: SNMP tab of AP, example	241
Figure 78: Quality of Service (QoS) tab of AP, example.....	244
Figure 79: Security tab of AP, example.....	246
Figure 80: VLAN tab of AP, example	249
Figure 81: VLAN Membership tab of AP, example	252
Figure 82: DiffServe tab of AP, example.....	253
Figure 83: Unit Settings tab of AP, example	255
Figure 84: General tab of SM, example	256
Figure 85: NAT tab of SM with NAT disabled, example.....	260
Figure 86: IP tab of SM with NAT disabled, example.....	263
Figure 87: NAT tab of SM with NAT enabled, example	265
Figure 88: IP tab of SM with NAT enabled, example	270
Figure 89: Radio tab of SM, example.....	271
Figure 90: SNMP tab of SM, example.....	274
Figure 91: Quality of Service (QoS) tab of SM, example	277
Figure 92: Security tab of SM, example	279
Figure 93: VLAN tab of SM, example.....	282
Figure 94: VLAN Membership tab of SM, example.....	285
Figure 95: DiffServe tab of SM, example	286
Figure 96: Protocol Filtering tab of SM, example	288
Figure 97: PPPoE tab of SM, example	289
Figure 98: NAT Port Mapping tab of SM, example	290
Figure 99: Unit Settings tab of SM, example.....	291
Figure 100: General tab of BHM, example.....	295

Figure 101: IP tab of BHM, example	298
Figure 102: Radio tab of BHM, example	299
Figure 103: SNMP tab of BHM, example	303
Figure 104: Security tab of BHM, example	306
Figure 105: VLAN tab of BHM, example	308
Figure 106: DiffServe tab of BHM, example.....	310
Figure 107: Unit Settings tab of BHM, example	311
Figure 108: General tab of BHS, example	313
Figure 109: IP tab of BHS, example.....	316
Figure 110: Radio tab of BHS, example.....	318
Figure 111: SNMP tab of BHS, example.....	321
Figure 112: Quality of Service (QoS) tab of BHS, example	323
Figure 113: Security tab of BHS, example	324
Figure 114: VLAN tab of BHS, example.....	326
Figure 115: DiffServe tab of BHS, example	328
Figure 116: Unit Settings tab of BHS, example.....	329
Figure 117: PDA Quick Status tab, example.....	335
Figure 118: PDA Spectrum Analyzer tab of BHS, example	336
Figure 119: PDA Spectrum Results tab of SM, example	336
Figure 120: PDA Information tab of SM, example.....	337
Figure 121: PDA AP Evaluation tab of BHM, example	337
Figure 122: PDA Aim tab of SM, example	338
Figure 123: Parts inventory for OFDM AP installation	339
Figure 124: Assembled upper bracket for OFDM AP.....	340
Figure 125: OFDM AP connected to its antenna	340
Figure 126: OFDM AP mounted to its antenna	340
Figure 127: OFDM AP ready for tower mount.....	341
Figure 128: Hanging OFDM AP assembly onto upper bracket of pole mount	342
Figure 129: OFDM AP attached to pole or tower	342
Figure 130: OFDM antenna lower bracket with quick-connect	342
Figure 131: Ground lug and coax cable of OFDM AP.....	343
Figure 132: Down tilt adjustment bracket of OFDM AP	344
Figure 133: Example Local Area Connection Properties window	346
Figure 134: Example Internet Protocol (TCP/IP) Properties window	346

Figure 135: SM attachment to reflector arm.....	348
Figure 136: SM grounding per NEC specifications	349
Figure 137: Internal view of Canopy 600SS Surge Suppressor.....	350
Figure 138: Override plug	351
Figure 139: Audible Alignment Tone kit, including headset and connecting cable	352
Figure 140: Example data from AP Evaluation tab	355
Figure 141: AP/SM link status indications in the AP Session Status tab	358
Figure 142: Correct mount with reflector dish	359
Figure 143: Incorrect mount with reflector dish	360
Figure 144: Mounting assembly, exploded view	361
Figure 145: BH attachment to reflector arm	362
Figure 146: Session Status tab of BHM	367
Figure 147: Spectrum Analyzer tab of SM, example.....	374
Figure 148: General Status tab view for GUEST-level account.....	382
Figure 149: Add User tab of SM, example	382
Figure 150: Delete User tab of SM, example	383
Figure 151: RJ-11 pinout for the override plug.....	384
Figure 152: Categorical protocol filtering	386
Figure 153: Session Status tab data, example	417
Figure 154: Event Log tab data, example	419
Figure 155: Network Interface tab of AP, example	421
Figure 156: Network Interface tab of SM, example.....	421
Figure 157: Layer 2 Neighbors tab, example	422
Figure 158: Scheduler tab of BHM, example	423
Figure 159: SM Registration Failures tab of AP, example	424
Figure 160: Bridging Table tab of AP, example	425
Figure 161: Translation Table tab of SM, example	426
Figure 162: Ethernet tab of BHM, example.....	426
Figure 163: Radio tab of Statistics page in SM, example	428
Figure 164: VLAN tab of AP, example	430
Figure 165: Data VC tab of BHM, example.....	431
Figure 166: Overload tab of BHM, example.....	432
Figure 167: Filter tab of SM, example	433
Figure 168: ARP tab of BHS, example.....	433

Figure 169: Nat Stats tab of SM, example	434
Figure 170: NAT DHCP Statistics tab of SM, example	434
Figure 171: PPPoE tab of SM, example	435
Figure 172: Alignment Tool tab of SM, example for a good link	437
Figure 173: Alignment Tool tab of SM, example for an acceptable link	437
Figure 174: Alignment Tool tab of SM, example for an unacceptable link	437
Figure 175: Link Capacity Test tab of BHM, example	438
Figure 176: Link Capacity Test tab with 1522-byte packet length, example	439
Figure 177: Link Capacity Test tab with 64-byte packet length, example	440
Figure 178: AP Evaluation tab of SM, example	442
Figure 179: Frame Calculator tab, example	447
Figure 180: Calculated Frame Results section of Frame Calculator tab, example	450
Figure 181: DFS Status tab of AP, example	451
Figure 182: DFS Status tab of SM, example	451
Figure 183: SM Configuration tab of AP, example	452
Figure 184: Link Status tab of AP, example	453
Figure 185: Remote Spectrum Analyzer tab of AP, example	455
Figure 186: BER Results tab of FSK SM, example	456
Figure 187: BER Results tab of OFDM SM, example	457
Figure 188: Example ftp session to transfer custom logo file	464
Figure 189: Example telnet session to activate custom logo file	465
Figure 190: Example telnet session to clear custom files	466
Figure 191: Protocol analysis at SM	469
Figure 192: Protocol analysis at AP or BH not connected to a CMM	470
Figure 193: Protocol analysis at AP or BH connected to a CMM	471
Figure 194: IP tab of SM with NAT disabled and local accessibility	472
Figure 195: Local Area Connection Properties window	473
Figure 196: Internet Protocol (TCP/IP) Properties window	474
Figure 197: Ethereal Capture Options window	475
Figure 198: Ethereal Capture window	476
Figure 199: <capture> - Ethereal window, Packet 1 selected	477
Figure 200: <capture> - Ethereal window, Packet 14 selected	478
Figure 201: NAT Table tab of SM, example	483

Figure 202: NAT DHCP Statistics tab of SM, example	484
Figure 203: Event Log tab of SM, example	486

LIST OF TABLES

Table 1: User guide organization scheme.....	35
Table 2: Examples of where to find information in this user guide.....	36
Table 3: Locations of screen captures and associated documentation	37
Table 4: Font types	40
Table 5: Admonition types.....	40
Table 6: Essential user guide elements for new wireless Ethernet bridge network implementation	47
Table 7: Fixed wireless broadband IP network product names	49
Table 8: Power supply descriptions	60
Table 9: Line Cords for Power Supplies.....	61
Table 10: Recommended outdoor UTP Category 5E cables	63
Table 11: Recommended indoor UTP Category 5E cables	64
Table 12: Recommended antenna cables	64
Table 13: Product applications per frequency band range.....	67
Table 14: Products with encryption options available per frequency band, PMP links	68
Table 15: Typical range and throughput per frequency band, PMP links	68
Table 16: Typical range and throughput per frequency band, PTP links	69
Table 17: Cluster management product similarities and differences	70
Table 18: Applications and tools	73
Table 19: Correct placement of license keys	77
Table 20: Model numbers	81
Table 21: Labels and locations of model (part) numbers and ESNs.....	83
Table 22: Characteristics of traffic scheduling	91
Table 23: Effect of 2X operation on throughput for the SM.....	93
Table 24: OFDM module performance at 1X, 2X, and 3X operation	95
Table 25: Effects of network conditions on PTMP throughput	102
Table 26: Comparison of SM products with CAP 130.....	102
Table 27: List of features.....	109
Table 28: Demonstration Kit part numbers	122
Table 29: Starter Kit part numbers	125
Table 30: Effect of DFS feature.....	134
Table 31: Signal quality levels indicated by jitter.....	136

Table 32: Recommended courses of action based on Efficiency in 2X operation	137
Table 33: Available center channels for single OFDM AP	141
Table 34: Example 900-MHz channel assignment by sector	142
Table 35: Example 2.4-GHz channel assignment by sector	143
Table 36: Example 5.2-GHz channel assignment by sector	143
Table 37: Example 5.4-GHz channel assignment by sector	143
Table 38: Example 5.7-GHz FSK channel assignment by sector	144
Table 39: Example 4.9-GHz OFDM channel assignment by sector.....	145
Table 40: Example 5.4-GHz OFDM channel assignment by sector.....	145
Table 41: VLAN filters in point-to-multipoint modules	170
Table 42: Exposure separation distances	173
Table 43: Calculated exposure distances and power compliance margins	174
Table 44: Statistical incidence of current from lightning strikes	176
Table 45: LEDs in AP and BHM.....	183
Table 46: Legacy Mode LEDs in SM and BHS	183
Table 47: Revised Mode LEDs in SM	184
Table 48: Recommended External Gain values for AP.....	237
Table 49: Control slot settings for all FSK APs in cluster.....	238
Table 50: Control slot settings for all OFDM APs in cluster	238
Table 51: Broadcast Downlink CIR achievable per Broadcast Repeat Count	245
Table 52: Recommended combined settings for typical operations.....	293
Table 53: Where feature values are obtained for an SM with authentication required ...	293
Table 54: Where feature values are obtained for an SM with authentication disabled ...	294
Table 55: Recommended External Antenna Gain values for BHM	301
Table 56: Recommended External Antenna Gain values for BHS.....	319
Table 57: Total gain per antenna	331
Table 58: Patch antenna and reflector gain	331
Table 59: Transmitter output power settings, example cases.....	333
Table 60: Hardware series by MAC address	377
Table 61: Hardware series differences	377
Table 62: Ports filtered per protocol selections	387
Table 63: Example times to download for typical tiers of service with CAP 120.....	390
Table 64: Example times to download for typical tiers of service with CAP 130.....	391
Table 65: Categories of MIB-II objects.....	395

Table 66: Canopy Enterprise MIB objects for APs, SMs, and BHs.....	398
Table 67: Canopy Enterprise MIB objects for APs and BH timing masters	402
Table 68: Canopy Enterprise MIB objects for SMs and BH timing slaves	406
Table 69: Event Log messages for abnormal events.....	420
Table 70: Event Log messages for normal events.....	420
Table 71: Supported telnet commands for module administration.....	497
Table 72: US FCC IDs and Industry Canada certification numbers and covered configurations	500
Table 73: Disclosure Table for China.....	507

LIST OF PROCEDURES

Procedure 1: Modifying a fixed license key for a module IP address.....	117
Procedure 2: Analyzing the spectrum	131
Procedure 3: Reducing transmitter output power.....	156
Procedure 4: Wrapping the cable.....	180
Procedure 5: Setting up the AP for Quick Start.....	186
Procedure 6: Bypassing proxy settings to access module web pages	187
Procedure 7: Using Quick Start to configure a standalone AP for test	189
Procedure 8: Setting up the SM for test.....	195
Procedure 9: Retrying to establish a point-to-multipoint link	196
Procedure 10: Verifying and recording information from SMs	205
Procedure 11: Verifying and recording information from the AP.....	210
Procedure 12: Setting up the BH for Quick Start	211
Procedure 13: Using Quick Start to configure the BHs for test.....	213
Procedure 14: Setting up the BHS for test.....	215
Procedure 15: Verifying and recording information from the BHS	220
Procedure 16: Verifying and recording information from the BHM.....	224
Procedure 17: Installing the FSK AP.....	338
Procedure 18: Installing the OFDM AP	339
Procedure 19: Configuring a Windows laptop.....	345
Procedure 20: Configuring a Linux laptop.....	347
Procedure 21: Installing the FSK SM	348
Procedure 22: Installing the OFDM SM	353
Procedure 23: Configuring the AP-SM link	355
Procedure 24: Monitoring the AP-SM link for performance.....	357
Procedure 25: Installing the FSK BHM	361
Procedure 26: Setting the Cyclic Prefix in a PTP 200 Series wireless Ethernet bridge ..	363
Procedure 27: Installing the FSK BHS	363
Procedure 28: Verifying performance for a BH link.....	365
Procedure 29: Verifying system functionality	369
Procedure 30: Using the Spectrum Analyzer in AP feature, VLAN disabled	375
Procedure 31: Using the Spectrum Analyzer in AP feature, VLAN enabled.....	376
Procedure 32: Extending network sync.....	378

Procedure 33: Fabricating an override plug	384
Procedure 34: Regaining access to a module	384
Procedure 35: Installing the Canopy Enterprise MIB files	396
Procedure 36: Performing a Link Capacity Test	440
Procedure 37: Using the Frame Calculator	449
Procedure 38: Replacing the Canopy logo on the GUI with another logo.....	463
Procedure 39: Changing the URL of the logo hyperlink.....	465
Procedure 40: Returning a module to its original logo and hyperlink.....	466
Procedure 41: Denying all remote access	467
Procedure 42: Reinstating remote access capability	467
Procedure 43: Setting up a protocol analyzer	472
Procedure 44: Troubleshooting loss of connectivity.....	481
Procedure 45: Troubleshooting loss of connectivity for NAT/DHCP-configured SM.....	482
Procedure 46: Troubleshooting SM failing to register to an AP	484
Procedure 47: Troubleshooting BHS failing to register to a BHM	485
Procedure 48: Troubleshooting loss of sync	486
Procedure 49: Troubleshooting loss of Ethernet connectivity	487
Procedure 50: Troubleshooting failure to power up	487
Procedure 51: Troubleshooting failure of power supply to produce power	488
Procedure 52: Troubleshooting CMM not passing sync	489
Procedure 53: Troubleshooting an unsuccessful software upgrade	489
Procedure 54: Restoring the web interface to a module	489

GUIDE TO THIS USER GUIDE

1 NEW IN THIS ISSUE

1.1 NEW PRODUCTS AND FEATURES DESCRIBED IN THIS GUIDE

This guide supersedes the Canopy System User Guide to support the following newer products and features:

- Release 8.2 and 8.4 features, including US and Canada DFS (Dynamic Frequency Selection) support for 5.4-GHz and 5.2-GHz modules
- Release 9.0, 9.2, and 9.4.2 features
- PMP 400 Series (OFDM AP and SM) in the 5.4-GHz band

1.2 PORTFOLIO OF WIRELESS BROADBAND SOLUTIONS

The Motorola portfolio of wireless broadband solutions provides a range of flexible, mix-and-match options including

- Fixed
 - unlicensed point-to-multipoint solutions
 - Expedience licensed point-to-multipoint solutions
 - point-to-point solutions, including
 - PTP 100 and PTP 200 Series bridges
 - PTP 400, PTP 500, and PTP 600 Series bridges
- Indoor, Enterprise Wireless LAN (WLAN) solutions
- Mesh, including the MOTOMESH series of products
- WiMAX, including infrastructure, CPE and devices, services, and IP core

1.3 PRODUCTS COVERED BY THIS USER GUIDE

Products covered by this user guide include

- PMP 100 Series FSK Access Points (CAPs) and Subscriber Modules (CSMs) in the following frequency bands:
 - 900 MHz - 5.2 GHz - 5.7 GHz
 - 2.4 GHz - 5.4 GHz
- PMP 400 Series OFDM Access Points (CAPs) and Subscriber Modules (CSMs) in the following frequency bands:
 - 4.9 GHz - 5.4 GHz
- PTP 100 Series FSK bridges in the following frequency bands:
 - 2.4 GHz - 5.2 GHz - 5.8 GHz
 - 5.1 GHz - 5.4 GHz
- PTP 200 Series OFDM bridges in the following frequency bands:
 - 4.9 GHz - 5.4 GHz
- 600SS Surge Suppressor

1.4 PRODUCTS NOT COVERED BY THIS USER GUIDE

Products with their own user guides include

- PTP 300, 400, 500, and 600 Series Bridges
- Cluster Management Module 2 (CMM2)
- Cluster Management Module micro (CMMmicro or CMM3)
- Cluster Management Module 4 (CMM4)
- LENS
- Prizm element management system
- Wireless Manager network management system

All of these products and solutions are covered by their own user guides and/or other documentation.

1.5 SOFTWARE COMPATIBILITY DESCRIBED IN THIS USER GUIDE

The following sections of this document provide details and caveats about the compatibility of products:

- [Designations for Hardware](#) on Page 377
- [MIB File Set Compatibility](#) on Page 378

2 USING THIS USER GUIDE

This document should be used with features in Software Release 9.4.2. The audience for this document includes system operators, network administrators, and equipment installers.

2.1 FINDING THE INFORMATION YOU NEED

2.1.1 Becoming Familiar with This User Guide

This is a guide to the guide. A high-level overview of the guide and some examples of where to look provide insight into how information is arranged and labeled.

The Table of Contents provides not only a sequential index of topics but also a visual glance at the organization of topics in this guide. A few minutes spent with the Table of Contents in either the paper or the electronic version of this guide can save much more time in finding information now and in the future. The List of Procedures may be especially useful in the paper version of this guide, particularly where you mark those procedures that you wish to frequently see.

In contrast, the List of Figures and List of Tables are most useful for automated searches on key words in the electronic version of this guide. If a match is present, the match is the first instance that the search finds.

Quick Reference

This user guide comprises six sections, as described in [Table 1](#).

Table 1: User guide organization scheme

Section	Purpose
Guide to This User Guide (this section)	Identifies <ul style="list-style-type: none"> ◦ products covered by this user guide. ◦ products covered by their own separate user guides. ◦ how this user guide is organized. ◦ where to find module web pages and parameter descriptions. ◦ what the various typefaces and admonitions indicate. ◦ how to contact Motorola.
Overview of Fixed Wireless Broadband IP Networks	Provides <ul style="list-style-type: none"> ◦ references to RF and networking theory. ◦ a list of sections to see if you are building only a backhaul network. ◦ overviews and comparisons of products and how they communicate. ◦ descriptions of data handling and synchronization. ◦ a review of optional features. ◦ resources for developing familiarity and proficiencies with networks.

Section	Purpose
Planning Guide	Provides essential information for <ul style="list-style-type: none"> ◦ evaluating an area for a network. ◦ specifying the IP addresses and frequency band ranges to use for each type of link.
Installation and Configuration Guide	Provides systematic approaches for <ul style="list-style-type: none"> ◦ avoiding hazards from RF and natural causes. ◦ testing, storing, and deploying equipment.
Operations Guide	Provides guidance for <ul style="list-style-type: none"> ◦ expanding network coverage. ◦ improving the security of wireless links. ◦ distributing bandwidth resources. ◦ monitoring and changing variables through SNMP.
Reference Information	Provides supplemental information such as <ul style="list-style-type: none"> ◦ authorizations, approvals, and notices. ◦ a bibliography of adjunctive information sources. ◦ a history of changes in documentation.
Glossary	Defines terms and concepts that are used in this user guide.

Examples

A list of common tasks and references to information that supports each task is provided in [Table 2](#).

Table 2: Examples of where to find information in this user guide

If you want to know...	then see...	because...
what the Spectrum Analyzer in SM and BHS feature does	Avoiding Self Interference on Page 155	this topic is important to RF planning.
	Monitoring the RF Environment on Page 373	this topic is also important to managing the network.
what types of slots compose the frame	Understanding Bandwidth Management on Page 85	this information is helpful for understanding networks.
how to calculate whether an object will interfere with a signal	Noting Possible Obstructions in the Fresnel Zone on Page 132	this topic is important to RF planning.
how long a cable you can use from the GPS antenna to the CMM	Cables on Page 35	cables are accessory components.
	the dedicated user guide that supports the CMM that you are deploying.	the advisory applies to mounting GPS antennas <i>and</i> CMMs.
how to react to a WatchDog Event Log message	Messages that Flag Abnormal Events on Page 420 <i>and</i> Messages that Flag Normal Events on Page 420	together, these two sections document all significant Event Log messages.

If you want to know...	then see...	because...
what beam angle the passive reflector dish produces	Specifications and Limitations on Page 77, then downward to a table for a part number that includes "RF."	the beam angle is a specification.
how to aim the passive reflector dish	Installing a Reflector Dish on Page 359	aiming is associated with installation of wireless bridges.
how to set Differentiated Services values so that traffic with original ToS byte formatting continues to be prioritized as it was before DSCP fields.	High-priority Bandwidth on Page 89	DSCP fields specify the level of priority that the device is requesting for the packet.

2.1.2 Searching This User Guide

To search this document and the software release notes of supported releases, look in the Table of Contents for the topic and in the Adobe Reader® search capability for keywords that apply.¹ These searches are most effective when you begin the search from the cover page because the first matches may be in titles of sections, figures, tables, or procedures.

2.1.3 Finding Parameter and Field Definitions for Module Web Pages

Because this user guide is sequentially arranged to support tasks, and various tasks require different settings and readings, parameter and field definitions are scattered according to the tasks that they support. The locations of these are provided in [Table 3](#).

Table 3: Locations of screen captures and associated documentation

Tab or Web Page Displayed	Page
Add User tab of SM, example	382
Alignment Tool tab of SM, example	437
AP Evaluation tab of SM, example	442
BER Results tab of FSK SM, example	456
Bridging Table tab of AP, example	425
Calculated Frame Results section of Frame Calculator tab, example	450
DiffServe tab of AP, example	253
DiffServe tab of BHM, example	310
DiffServe tab of BHS, example	328
DiffServe tab of SM, example	286
Ethernet tab of BHM, example	426
Event Log tab data, example	419

¹ Reader is a registered trademark of Adobe Systems, Incorporated.

Tab or Web Page Displayed	Page
Event Log tab of SM, example	486
General Status tab of AP (5.7 GHz), example	206
General Status tab of BHM, example	221
General Status tab of BHS, example	216
General Status tab of SM, example	202
General Status tab view for GUEST-level account	382
General tab of AP, example	227
General tab of BHM, example	295
General tab of BHS, example	313
General tab of SM, example	256
IP tab of AP, example	231
IP tab of BHM, example	298
IP tab of BHS, example	316
IP tab of SM with NAT disabled and local accessibility	472
IP tab of SM with NAT disabled, example	263
IP tab of SM with NAT enabled, example	270
LAN IP Address tab of AP, example	192
Link Capacity Test tab with 1522-byte packet length, example	439
Link Capacity Test tab with 64-byte packet length, example	440
NAT DHCP Statistics tab of SM, example	484
NAT Port Mapping tab of SM, example	290
NAT tab of SM with NAT disabled, example	260
NAT tab of SM with NAT enabled, example	265
NAT Table tab of SM, example	483
PDA Aim tab of SM, example	338
PDA AP Evaluation tab of BHM, example	337
PDA Information tab of SM, example	337
PDA Quick Status tab, example	335
PDA Spectrum Analyzer tab of BHS, example	336
PDA Spectrum Results tab of SM, example	336
Protocol Filtering tab of SM, example	288
Quality of Service (QoS) tab of AP, example	244
Quality of Service (QoS) tab of BHS, example	323
Quality of Service (QoS) tab of SM, example	277

Tab or Web Page Displayed	Page
Quick Start tab of AP, example	188
Quick Start tab of BHM, example	212
Radio Carrier Frequency tab of AP, example	190
Radio tab of AP (900 MHz), example	233
Radio tab of BHM, example	299
Radio tab of BHS, example	318
Radio tab of SM, example	271
Remote Subscribers tab of AP, example	201
Remote Subscribers tab of BHM, example	216
Review and Save Configuration tab of AP, example	193
Scheduler tab of BHM, example	423
Security tab of AP, example	246
Security tab of BHM, example	306
Security tab of BHS, example	324
Security tab of SM, example	279
Session Status tab data from AP, example	196
Session Status tab data, example	417
SM Configuration tab of AP, example	452
SM Registration Failures tab of AP, example	424
SNMP tab of AP, example	241
SNMP tab of BHM, example	303
SNMP tab of BHS, example	321
SNMP tab of SM, example	274
Spectrum Analyzer tab of SM, example	374
Synchronization tab of AP, example	191
Time tab of AP, example	194
Time tab of BHM, example	214
Unit Settings tab of AP, example	255
Unit Settings tab of BHM, example	311
Unit Settings tab of BHS, example	329
Unit Settings tab of SM, example	291
VLAN Membership tab of AP, example	252
VLAN Membership tab of SM, example	285

Tab or Web Page Displayed	Page
VLAN tab of AP, example	249
VLAN tab of SM, example	282

2.2 INTERPRETING TYPEFACE AND OTHER CONVENTIONS

This document employs distinctive fonts to indicate the type of information, as described in [Table 4](#).

Table 4: Font types


Font	Type of Information
variable width bold	Selectable option in a graphical user interface or settable parameter in the web-based interface to a component.
constant width regular	Literal system response in a command-line interface.
<i>constant width italic</i>	Variable system response in a command-line interface.
constant width bold	Literal user input in a command-line interface.
<i>constant width bold italic</i>	Variable user input in a command-line interface.





This document employs specific imperative terminology as follows:

- *Type* means press the following characters.
- *Enter* means type the following characters and then press Enter.

This document also employs a set of consistently used admonitions. Each of these types of admonitions has a general purpose that underlies the specific information in the box. These purposes are indicated in [Table 5](#).

Table 5: Admonition types

Admonition Label	General Message
	<p>NOTE: informative content that may</p> <ul style="list-style-type: none"> ◦ defy common or cursory logic. ◦ describe a peculiarity of the implementation. ◦ add a conditional caveat. ◦ provide a reference. ◦ explain the reason for a preceding statement or provide prerequisite background for what immediately follows.

Admonition Label	General Message
	<p><i>RECOMMENDATION:</i> suggestion for an easier, quicker, or safer action or practice.</p>
	<p><i>IMPORTANT!</i> informative content that may</p> <ul style="list-style-type: none"> ◦ identify an indication that you should watch for. ◦ advise that your action can disturb something that you may not want disturbed. ◦ reiterate something that you presumably know but should always remember.
	<p><i>CAUTION!</i> a notice that the risk of harm to equipment or service exists.</p>
	<p><i>WARNING!</i> a notice that the risk of harm to person exists.</p>

2.3 GETTING ADDITIONAL HELP

Help is available for problems with supported products and features. [Obtaining Technical Support](#) on Page 491 provides the sequence of actions that you should take if these problems arise.

2.4 SENDING FEEDBACK

Is this document accurate, complete, and clear? How can it be improved? Send your feedback on documentation to technical-documentation@canopywireless.com.

OVERVIEW OF PMP SOLUTIONS

3 ADVANCING FROM RESEARCH TO IMPLEMENTATION

Before you begin to research a possible implementation, you should have both

- basic knowledge of RF theory. See
 - [Understanding RF Fundamentals](#) on Page 119.
 - [Engineering Your RF Communications](#) on Page 129.
- network experience. See
 - [Link Characteristics](#) on Page 85.
 - [Understanding IP Fundamentals](#) on Page 119.
 - [Engineering Your IP Communications](#) on Page 159.

4 REALIZING A WIRELESS ETHERNET BRIDGE NETWORK

PTP 100 Series Bridges serving as backhaul modules (BHs) can connect access point clusters to the point of presence or be the backbone of a Metro WiFi mesh network. In other applications, the backhaul modules can be used to provide connectivity for

- cell sites, in lieu of leased T1/E1 telecommunications lines.
- buildings in corporate or institutional campuses.
- remote sites, including temporary sites set up for relief efforts.

These BHs are available in 10- or 20-Mbps modulation rates from the factory. The rate is distinguished as BH10 or BH20 in the Software Version field of the General Status tab (in the Home page) of the module GUI.

For these and any other backhaul networks, [Table 6](#) provides a quick reference to information that you would need to establish and maintain the wireless bridge network.

Table 6: Essential user guide elements for new wireless Ethernet bridge network implementation

Element	Title	Page
Section 1.4	Products Not Covered by This User Guide	34
Section 5.2.5	PTP Series 100 Bridges	53
Section 5.2.6	PTP 200 Series Bridges	53
Section 5.2.8	PTP 400 Series Bridges	54
Section 5.2.9	PTP 500 Series Bridges	54
Section 5.2.10	PTP 600 Series Bridges	55
Section 5.2.12	Cluster Management Module-2 (Part 1008CK-2)	56
Section 5.2.13	Cluster Management Module micro (Part 1070CK)	56
Section 5.2.14	CMM4 (Part 1090CK)	58
Table 16	Typical range and throughput per frequency band, PTP links	69
Section 8.2	BH-BH Links	101
Figure 32	Typical multiple-BH network layout	106
Section 12.2	Analyzing the RF Environment	131
Section 12.5	Considering Frequency Band	138
Section 15	Avoiding Hazards	173
Section 16.4	Configuring a Point-to-Point Link for Test	211
Section 17	Preparing Components for Deployment	225
Section 18.4	Configuring a BH Timing Master for the Destination	294
Section 18.5	Configuring a BH Timing Slave for the Destination	312
Section 19.4	Installing a GPS Antenna	345

Section 19.5	Installing a	345
Section 19.9	Installing a Reflector Dish	359
Section 19.10	Installing a BH Timing Master	361
Section 19.11	Installing a BH Timing Slave	363
Section 19.13	Verifying a BH Link	365
Section 22.2	Encrypting Radio Transmissions	379
Section 22.3	Managing Module Access	381
Section 24.4	Objects Defined in the Canopy Enterprise MIB	398
Section 24.5	Interface Designations in SNMP	409
Section 24.6	Traps Provided in the Canopy Enterprise MIB	410
Section 25	Using the Canopy Network Updater Tool (CNUT)	413
Section 28.3	Typical Contents of Release Notes	461
Section 28.4	Typical Upgrade Process	461
Section 31.2	Analyzing Traffic at an AP or BH with No CMM	470
Section 31.3	Analyzing Traffic at an AP or BH with a CMM	470
Section 32	Troubleshooting	479
Section 33	Obtaining Technical Support	491
Section 34	Getting Warranty	493

5 EXPLORING THE SCOPE OF SOLUTIONS

Fixed wireless broadband IP network applications include:

- local area network (LAN) extensions
- Internet subscriber service
- high-bandwidth point-to-point connections
- multicast video (for instruction or training, for example)
- private branch exchange (PBX) extensions
- point-to-multipoint data backhaul
- redundant network backup
- video surveillance
- voice over IP (VoIP)
- TDM over Ethernet (for legacy voice and data)

5.1 PRODUCT NAMES

Table 7: Fixed wireless broadband IP network product names

Protocol Type	Product Series	Product Name	Previous Names	Example Model
Point-to-Multipoint	PMP 100	CAP 120	CAP 100, Classic AP	5700AP
		CSM 120	CSM 100, SM	5700SM
		CSM 110	Lite SM	5760SM
		CAP 130	CAP 200, Advantage AP	5750AP
		CSM 130	CSM 200, Advantage SM	5750SM
	PMP 400	CAP 49400	4.9-GHz OFDM AP	4940AP
		CSM 49400	4.9-GHz OFDM SM	4940SM
		CAP 54400	5.4-GHz OFDM AP	5440AP
CSM 54400		5.4-GHz OFDM SM	5440SM	
Point-to-Point	PTP 100	PTP 110	2- or 4-Mbps BH	
		PTP 120	PTP 100 Lite, BH10 (7-Mbps)	5700BH
		PTP 130	PTP 100 Full, BH20 (14-Mbps)	5700BH20
	PTP 200	PTP 49200	4.9-GHz OFDM BH	4940BH
		PTP 54200	5.4-GHz OFDM BH	5440BH
<p>NOTE: Each product is available in multiple model numbers, which distinguish the model by such attributes as frequency band range, encryption type, or power adjustable for extended range. See Interpreting Model Number on Page 79 and Sorted Model Numbers on Page 81.</p>				

5.2 NETWORK COMPONENTS

Motorola fixed wireless broadband IP networks use some or all of the following components. For the components that provide a graphical user interface (GUI), access to the GUI is through a web browser. In Release 8 and later, cascading style sheets (CSS) configure the GUI. Thus an operator is able to customize the GUI by editing these style sheets.

5.2.1 Access Point Module Other Than 900-Mhz

The FSK Access Point (AP) module provides up to 14 Mbps aggregate throughput in a 60° sector. The CAP 120 FSK AP can communicate with only a CSM 120 SM, *not also* a CSM 130 or a Lite (CSM 110) SM. The CAP 130 or CAP 09130 AP distributes services as broadly as the CAP 120. However, the CAP 130 provides greater throughput and less latency. The CAP 130 communicates with all SMs in its frequency band range: CSM 110s, CSM 120s, and CSM 130s.

The OFDM AP provides up to 21 Mbps aggregate throughput in a 90° sector. An OFDM AP can communicate with only an OFDM SM.

An FSK or OFDM AP supports up to 200 subscribers and 4,096 MAC addresses, which may be directly-connected PCs, IP appliances, gateways, Subscriber Modules (SMs), and the AP, except that *no limit* applies behind subscriber network address translation (NAT) gateways. The AP is configurable through a web interface.

5.2.2 Access Point Cluster

An AP cluster covers as much as 360°.

The FSK (PMP 100 or PMP 400) AP cluster consists of two to six APs that together provide broadband connectivity to 1,200 or fewer subscribers. Each of these APs transmits and receives in a 60° sector.

The PMP 400 Series (OFDM) AP cluster consists of two to four APs that provide broadband connectivity to 800 or fewer subscribers. Each of these APs transmits and receives in a 90° sector.

An AP cluster is pictured in [Figure 1](#).



Figure 1: Pole-mounted AP cluster

The variety of available FSK and OFDM APs in frequency band range, power adjustability, and antenna configuration is shown under [Acquiring a Demonstration Kit](#), beginning on Page 119.

An OFDM AP, showing the antenna in front and the radio attached to it, is pictured in [Figure 2](#).



Figure 2: OFDM AP - Antenna and Radio

5.2.3 Subscriber Module Other Than 900-MHz

The Subscriber Module (SM) is a customer premises equipment (CPE) device that provides broadband services through communication with an AP. The SM is configurable through a web interface.

The variety of available FSK and OFDM SMs in frequency band range, power adjustability, and antenna configuration is shown under [Acquiring a Demonstration Kit](#), beginning on Page 119.



Figure 3: Structure-mounted SM

The CSM 130 or CSM 09130 provides the same configurability and services as the CSM 110 or CSM 120. However, in a link with a CAP 130 or CAP 09130, the CSM 130 or CSM 09130 provides uncapped sustained 2X throughput. See [2X Operation](#) on Page 92. A CSM 130 or CSM 09130 can communicate with only a CAP 130 or CAP 09130, respectively.

A PMP 100 Series (FSK SM) can communicate with either a CAP 120 or CAP 130. An FSK SM mounted directly to a structure is pictured in [Figure 3](#).

A PMP Series 400 (OFDM) SM can communicate with only an OFDM AP. An OFDM SM is shown in [Figure 4](#) in both front and side views.

Lite SMs (CSM 110 modules) cost less and provide less throughput than the CSM 120s or CSM 130s. They support the same radio frequencies, interference tolerance, and product reliability. They give operators the additional option to serve cost-sensitive customers who want standard services (web browsing, email, VoIP, and downloads), but do not require the higher throughput that is available with a regular SM. Lite SMs support an aggregate (uplink plus downlink) throughput of 512 kbps.

Through purchased floating licenses that Prizm manages, they are upgradeable to 1, 2, 4, or 7 Mbps aggregate throughput. A Lite SM can communicate with only a [CAP 130](#). A comparison of the CSM 110 to the CSM 120 and CSM 130 is provided in [Table 26](#) on Page 102.



Figure 4: OFDM SM, front and side views

5.2.4 900-MHz AP and SM

The 900 MHz AP (CAP 09130) and SM (CSM 09130) modules operate at a 3.3 Mbps carrier rate (compared to 10 Mbps for other FSK frequency bands).

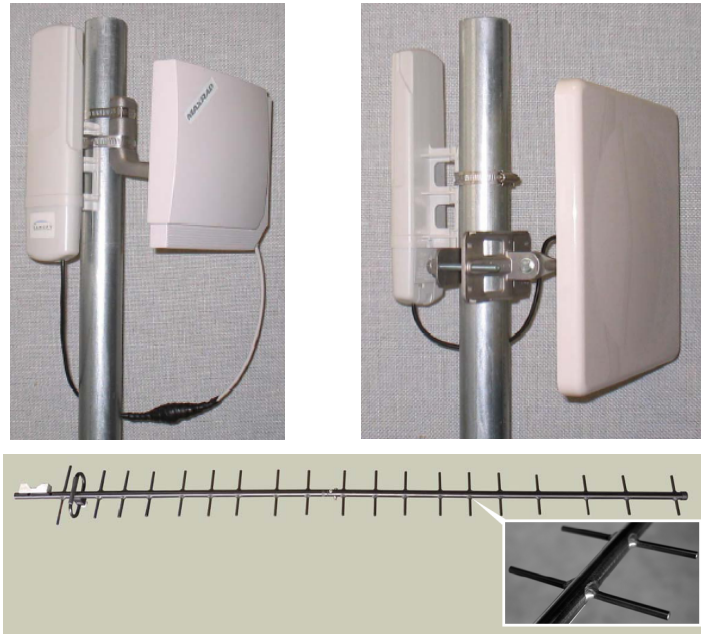


Figure 5: Examples of antennas for 900-MHz modules

These 900-MHz modules run the same software and provide the same parameters, network features, and connections as all other APs and SMs. The physics of longer-wavelength 900 MHz, the power allowed by regulatory authorities, and the low required level of Carrier-to-Interference (C/I) ratio combine to support

- line of sight (LOS) range of up to 40 miles (over 64 km)
- increased non-line of sight (NLOS) range, depending on RF considerations such as foliage, topography, and obstructions.

When collocated with an SM of another frequency band range, the 900-MHz AP may serve, without a tower or BH, as a *remote* AP (see [Deploying a Remote AP](#) on Page 151). 900-MHz AP/SM links are logical choices for extending radio networks where you wish to

- add subscriber-handling capacity to a tower that is either
 - fully used in the other frequency band ranges.
 - not available to any other frequency band range.
- reach sparsely populated areas.
- penetrate foliage.
- add a remote AP behind an SM that operates in another frequency band range.

With Only the Integrated Antenna

The enclosure of the 900-MHz integrated AP and SM houses both the hardware and antenna. These modules can be purchased with a band pass filter to improve performance in environments in which equipment (for example, a pager) is operating in the spectrum adjacent to the 900-MHz band.

Unlike the antennas in other FSK Motorola radios, the integrated antenna in the 900-MHz radio is *horizontally* polarized to reduce exposure to noise from vertically polarized signals, which predominate in this band.

Connectorized for External Antenna

The enclosure of the 900-MHz connectorized AP and SM includes a cable and N-type connector to which an external antenna can attach. In this case, network operators can select horizontal or vertical polarization and select the type of antenna to use. However, these connectorized modules can be used in the same architecture with the integrated modules only if the connectorized modules are *horizontally* polarized.

5.2.5 PTP Series 100 Bridges

A pair of PTP 100 Series wireless Ethernet bridges provides point-to-point connectivity as either a standalone link or a link through a cluster management module to an AP cluster.

You must configure a BH as either a timing master (BHM) or timing slave (BHS). The BHM provides synchronization signal (sync) to the BHS.

A BH mounted to a passive reflector dish is pictured in [Figure 6](#). Carrier applications for these modules include reaching remote AP clusters, interconnecting campus buildings or remote branch offices, extending private branch exchange (PBX) circuits, backhauling cell sites, and extending central office T1s/E1s.

These BHs are supported by this user guide. See [Realizing a Wireless Ethernet Bridge Network](#) on Page 47.



Figure 6: Dish-mounted 7.5- or 14-Mbps bridge

5.2.6 PTP 200 Series Bridges

The PTP 200 Series bridges securely transport data, voice, and video in both near-line-of-sight (nLOS) and line-of-sight (LOS) deployments at Ethernet data rates up to 21 Mbps. In the 4.9-GHz range, the public safety area of the spectrum, these bridges are a point-to-point solution for emergency services. In 5.4 GHz, they are a solution for enterprises. Orthogonal Frequency Division Multiplexing (OFDM) technology resists multi-path interference and fading that is otherwise caused by buildings and other obstructions.

Interference avoidance capability is ensured. The Dynamic Frequency Selection (DFS) feature switches channels to avoid interfering with priority signals. Moreover, these bridges can be collocated within the physical scope of an existing network, or used as part of a 5.4-GHz frequency band overlay network.



Figure 7: 21-Mbps bridge

These bridges are supported by this user guide. See [Realizing a Wireless Ethernet Bridge Network](#) on Page 47.

5.2.7 PTP 300 Series Bridges

PTP 300 Series wireless Ethernet bridges offer reliable and cost-effective backhaul at rates up to 25 Mbps for distances up to 155 miles (250 km) or, when enabled by a special license key, up to 50 Mbps in LOS deployments for distances up to 10 miles (16 km).

These bridges operate in the 5.4- or 5.8-GHz frequency band range. The form for these bridges is shown in [Figure 8](#). These bridges are supported by their own dedicated user guide.

5.2.8 PTP 400 Series Bridges

PTP 400 Series wireless Ethernet bridges offer reliable non-line-of-sight (NLoS) or long-distance line of sight (LoS) connection to the other bridge in the pair. Their features include adaptive modulation, intelligent Dynamic Frequency Selection, and a preset that denies connection to any unit other than the one in its pair. These are available as full (43-Mbps) or lite (21-Mbps) bridges.

Either variety is a solution for any of the following field applications:

- backhaul pair for PMP networks
- campus connection between buildings
- last-mile access and backbone
- voice over IP (VoIP) and video surveillance



Figure 8: PTP 300/400/500/600 Series Bridge common form

These bridges transmit and receive in the 4.9-GHz frequency band range, at 4.940 to 4.990. The form for these bridges is shown in [Figure 8](#). These bridges are supported by their own dedicated user guide.

5.2.9 PTP 500 Series Bridges

Motorola PTP 500 Series Bridges offer reliable non-line-of-sight (NLoS) and long-distance line of sight (LoS) connection to the other bridge in the pair. Their features include Multiple-input Multiple-output (MIMO), intelligent Orthogonal Frequency Division Multiplexing (i-OFDM), Advanced Spectrum Management, and Adaptive Modulation. These are available as 105-Mbps bridges. These bridges transmit and receive in 5.4- and 5.8-GHz frequency band ranges. The form for these bridges is shown in [Figure 8](#) on Page 54.

They are a solution for any of the following field applications:

- | | |
|---------------------------------------|---|
| ◦ high-speed backhaul | ◦ disaster recovery |
| ◦ campus connection between buildings | ◦ emergency services |
| ◦ telemedicine | ◦ voice over IP (VoIP) and video surveillance |

The PTP 500 Series Bridges offer many more SNMP-accessible element management parameters than do their PTP 400 and 600 Series counterparts; specifically, a significantly larger number of read-only fields, manageable objects, and notifications addressable to the NMS. Further, a new PTP LINKPlanner tool currently supports only PTP 500 Bridge networks. This tool allows operators to simultaneously see path calculations for configuring single and multiple links, using a Google Earth overview. In this way, the PTP LINKPlanner can be more useful than the Link Estimator tool, which continues to support the PTP 400 and 600 Series wireless bridges that Motorola offers.

These bridges are supported by their own dedicated user guide.

5.2.10 PTP 600 Series Bridges

Motorola PTP 600 Series Bridges offer reliable non-line-of-sight (NLoS) and long-distance line of sight (LoS) connection to the other bridge in the pair. Their features include adaptive modulation, intelligent Dynamic Frequency Selection, and a preset that denies connection to any unit other than the one in its pair. These are available as full (300-Mbps) or lite (150-Mbps) bridges.

Each pair of these bridges transmits and receives in one of the following frequency band ranges. The bridges manufactured for

- the 2.5-GHz range, which is the Educational Broadcast Service area of the spectrum, constitute a PTP solution for low-power high-speed distance learning with Internet access and email in any of the following field applications:
 - backhaul pair for PMP networks
 - last-mile access and backbone
 - campus connection between buildings
 - voice over IP (VoIP) and video surveillance
- the 4.5- and 4.8-GHz ranges, which together are the U.S. government and military and the NATO areas of the spectrum, constitute PTP solutions for
 - battlefield communications
 - training and simulation networks
 - campus connection between buildings
 - video surveillance and border security
- the 4.9-GHz range, which is the public safety area of the spectrum, constitute PTP solutions for
 - missing-person, DMV, and medical records
 - primary, secondary, and infill, ASTRO links
 - building blueprints and vehicle locations
 - part of a pre-mounted emergency site
- the 5.4-, 5.8-, and 5.9-GHz ranges constitute PTP solutions for unlicensed backhaul of bundled circuit-switched VoIP, video, and data communications.

The form for these bridges is shown in [Figure 8](#) on [Page 54](#). These bridges are supported by their own dedicated user guide.

5.2.11 Radio Adjustable Power Capabilities

Motorola offers adjustable power radios in all frequency bands. See [Adjusting Transmitter Output Power](#) on Page 330 to ensure that your radios do not exceed the maximum permitted EIRP.

5.2.12 Cluster Management Module-2 (Part 1008CK-2)

The Cluster Management Module-2 (CMM2) provides power, GPS timing from an antenna that is included, and networking connections for an AP cluster. The CMM2 can also connect to a BH, in which case the CMM2 is the central point of connectivity for the entire site. The CMM2 can connect as many as eight collocated modules—APs, BHMs, BHSs—and an Ethernet feed.

The CMM2 requires two cables for each connected module:

- One provides Ethernet communications and power. This cable terminates in an RJ-45 connector.
- The other provides synchronization (sync), GPS status, and time and date in a serial interface. This cable terminates in an RJ-11 connector.

A CMM2 is pictured in [Figure 9](#). A CMM2 as part of a mounted system is pictured in [Figure 10](#). CMM2 is no longer available for purchase, but it still a supported product. For documentation, it is supported by its own dedicated user guide.



Figure 9: CMM2 enclosure



Figure 10: CMM2 pole-mounted

5.2.13 Cluster Management Module micro (Part 1070CK)

The Cluster Management Module micro (CMMmicro) provides power, GPS timing, and networking connections for an AP cluster. The CMMmicro is configurable through a web interface.

The CMMmicro contains an 8-port managed switch that supports Power over Ethernet (PoE) on each port and connects any combination of APs, BHMs, BHSs, or Ethernet feed. The Motorola fixed wireless broadband IP networks PoE *differs from* IEEE Standard 803.3af PoE, and the two should not be intermixed. The CMMmicro can auto-negotiate speed to match inputs that are either 100Base-TX or 10Base-T, and either full duplex or

half duplex, where the connected device is set to auto-negotiate. Alternatively, these parameters are settable.

A CMMmicro requires only one cable, terminating in an RJ-45 connector, for each connected module to distribute

- Ethernet signaling.
- power to as many as 8 collocated modules—APs, BHMs, or BHSs. Through a browser interface to the managed switch, ports can be powered or not.
- sync to APs and BHMs. The CMMmicro receives 1-pulse per second timing information from Global Positioning System (GPS) satellites through an antenna (included) and passes the timing pulse embedded in the 24-V power to the connected modules.

GPS status information is available at the CMMmicro, however

- CMMmicro provides time and date information to BHMs and APs if both the CMMmicro is operating on CMMmicro Release 2.1 or later and the AP/BHM is operating on System Release 4.2 or later. See [Time Tab of the AP](#) on Page 194.
- CMMmicro *does not* provide time and date information to BHMs and APs if either the CMMmicro is operating on a release earlier than CMMmicro Release 2.1 or the AP/BHM is operating on a release earlier than System Release 4.2.

A CMMmicro is pictured in [Figure 11](#) and [Figure 12](#).

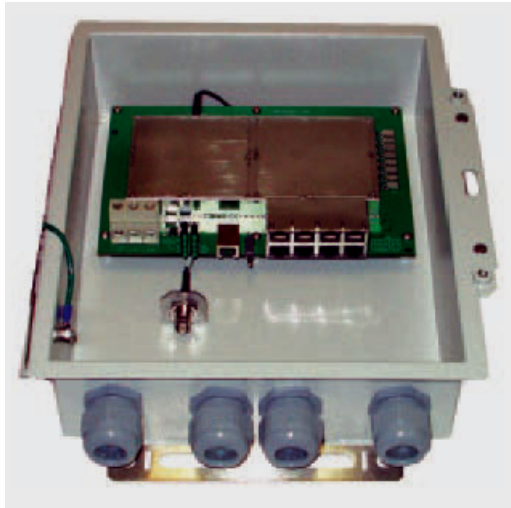


Figure 11: CMMmicro



Figure 12: Pole-mounted CMMmicro

This product is supported by its own dedicated user guide.

5.2.14 CMM4 (Part 1090CK)

The Cluster Management Module 4 (CMM4) provides power, GPS timing from an antenna that is included, and networking connections for an AP cluster, Backhubs, and Ethernet terrestrial feeds in a variety of configurations. The CMM4 provides reliable GPS network synchronization with an integrated solution that includes

- 9 access ports: eight 10/100Base-T ports and one copper 10/100/1000Base-T port
- a full featured Ethernet switch
- a Gigabit Ethernet port
- integrated lightning surge suppression on every data line, the GPS interface, the 29 V DC power inputs, and the coax line. These points include all RJ11 and RJ45 connectors.

The CMM4 has four major hardware components:

- the Cluster Controller. The controller injects power and synchronization on a per-port basis and is configured using a web interface.
- a separate hardened Ethernet switch housed within the same weatherized enclosure. This switch integrates switching technology with its own separate web-based management functions and provides a full array of networking features. (See [Optional Ethernet Switch in CMM4](#) on Page 59.)
- the GPS system. This includes an integrated GPS board, an antenna, and brackets for pole mounting the antenna.
- the power supply unit. This is a 20-volt, 40-watt supply that outputs on two connectors.

The CMM4 supports:

- Power over Ethernet (PoE) using a proprietary 30- or 56-VDC scheme that *differs from* IEEE Standard 803.af.
- synchronization and date and time on each port. Where the connected device is set to auto-negotiate, the CMM4 can auto-negotiate speed to match inputs that are either 100Base-TX or 10Base-T, and either full duplex or half duplex. Alternatively, these parameters are settable.
- management by a web browser, telnet, the console port, Prizm element management system, or a network manager that uses SNMP.
- dual power supply input redundancy. (Power supply is sold separately). The enclosure provides a 1-hole insert for a DC power cable gland.

This user guide introduces CMM4, but the dedicated *Cluster Management Module 4 (CMM4) User Guide* provides full documentation on this product, including installation instructions.

A CMM4 is pictured in [Figure 13](#) and [Figure 14](#).

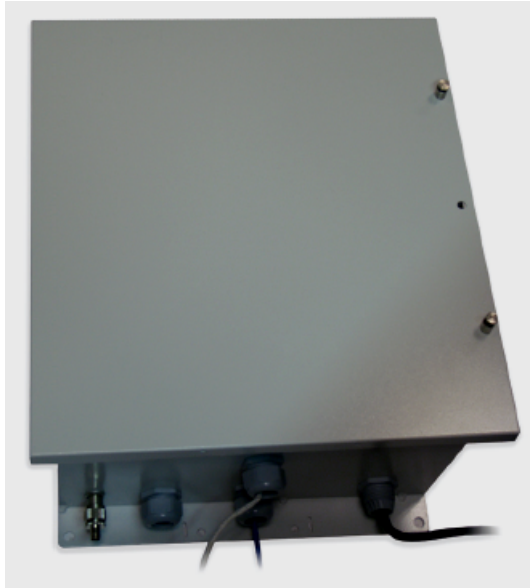


Figure 13: CMM4 enclosure

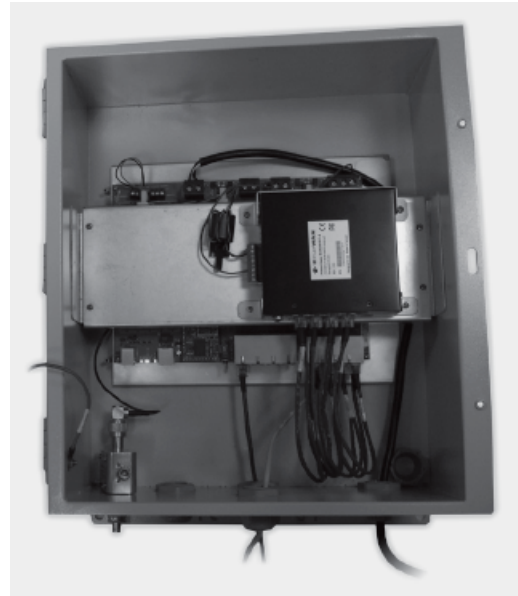


Figure 14: CMM4

5.2.15 Optional Ethernet Switch in CMM4

The Ethernet switch is a separate device enclosed within the CMM4 enclosure and connected to the CMM4 cluster controller via either the Gigabit port or one of the standard Ethernet ports. The switch may be accessed in any of three ways:

- through the administration console via RS-232 serial port. This access
 - requires either proximity to the switch or a dial-up connection.
 - is text-based, using Windows Hyperterminal.
 - does not require an IP address.
- through the web-based interface. This access requires that the IP address of the switch is accessible from the device on which the browser resides.
- through an external SNMP-based network management application. This access
 - communicates with switch functions at the MIB level.
 - requires SNMP element management software.

This is a hardened managed switch that provides

- 12 10/100Base-T ports, 8 of them powered
- 2 copper 10/100/1000Base-T (Gigabit) Ethernet port, copper connecting

The Ethernet Switch has many features not addressed in this document. For further information, either visit http://www.EtherWAN.com/manuals/es/EX96000_e1_Manual.pdf or see the EtherWAN switch manual provided with the CMM4.

5.2.16 GPS Antenna (Part GPSANTPNM03D)

The Motorola GPS antenna provides either

- timing pulses to the CMMmicro or CMM4
- timing pulses and positioning information to the CMM2.

The GPS antenna is pictured in [Figure 15](#).



Figure 15: Motorola GPS antenna

5.2.17 Surge Suppressor (Part 600SS)

The 600SS Surge Suppressor provides a path to ground (Protective Earth ↓) that reduces the risk to persons, buildings, and inside equipment from over-currents and over-voltages associated with lightning strikes. This accessory is RoHS compliant. A 600SS is pictured in [Figure 16](#).

The 600SS is available as Part Numbers 600SSC or 600SSD. Either of these models works properly and identically when deployed to protect either an FSK or an OFDM radio.



Figure 16: 600SS surge suppressor

5.2.18 Accessory Components

In addition to the above modules, the following accessories are available.

Power Supplies

The various power supplies are listed in [Table 8](#).

Table 8: Power supply descriptions

To Power			For Use With	Part Number	VAC In	VDC Out	Line Cord Included
CMM	PMP FSK	PMP OFDM					
CMM4			PMP 49400 PMP 500	SGPN4076	100 to 240	52.6	None.
CMM4 CMMmicro			PMP 100 PMP 54400	ACPS112WA	100 to 240	29	USA.
CMM4 CMMmicro			PMP 100 PMP 54400 and no power lead	ACPS112W-02A	100 to 240	29	None.

To Power			For Use With	Part Number	VAC In	VDC Out	Line Cord Included
CMM	PMP FSK	PMP OFDM					
		49400 500	PoE and RJ-45 pass-through	SGPN4063A	100 to 240	56	None.
	100	54400	network in USA or EU	ACPSSW-09B	90 to 240	29.5	USA, EU, UK.
	100	54400	network in Argentina	ACPSSW-10B	90 to 240	29.5	Argentina
	100	54400	network in Australia	ACPSSW-11	90 to 240	29.5	Australia
	100	54400	network in China	ACPSSW-12C	90 to 240	29.5	China
	100		network in USA, Canada, or Mexico	ACPSSW-13A	90 to 240	24	USA, Canada, Mexico.
		all	network in USA, Canada, or Mexico	ACPSSW-13B	90 to 240	29.5	USA, Canada, Mexico.

Region-compliant 56-V DC line cords for the power supplies are listed in [Table 9](#).

Table 9: Line Cords for Power Supplies

Region	Part Number
Argentina	SGKN4419A
Australia	SGKN4425A
Canada	SGKN4427A
China-Mainland	SGKN4424A
Europe	SGKN4426A
India	SGKN4420A
Japan	SGKN4423A
Korea	SGKN4422A
Mexico	SGKN4427A
Pakistan	SGKN4420A
Singapore-United Kingdom	SGKN4421A
South Africa	SGKN4420A
USA	SGKN4427A

Passive Reflector Dish Assembly

A 27RD Passive Reflector Dish on both ends of a BH link extends the distance range of the link and provides a narrower beam width, which can reduce both received and transmitted interference. A 27RD on an SM extends the distance range in some bands (notably 5.7-GHz and 2.4-GHz) and can reduce both received and transmitted interference in all bands. The module support tube provides the proper offset focus angle. See [Figure 17](#).

For 5.x-GHz radios, the reflector gain is 18dB and the 3 dB beam width is 6° in both azimuth and elevation. For 2.4-GHz radios, the reflector gain is 11dB and the 3 dB beam width is 17° in both azimuth and elevation.



Figure 17: 27RD with mounted module

LENS

The LENS product retrofits to a radio to

- improve range and resistance to interference, compared to those of the module with no reflector.
- provide less wind loading, easier mounting, and an appearance more consistent with the module form than has the reflector dish.

LENS focuses its beam in 60° azimuth and elevation and boosts signal gain by 9 to 10 dB. LENS is an option for 5.2-, 5.4-, and 5.7-GHz radios, but not an option for P7-through P9-series radios in the U.S.A. or Canada or for 2.4-GHz radios anywhere.

Viable use cases include all radio types (SM, BH, and AP), and installation in each case requires no tools. A dedicated user guide supports this product.

Currently, the radio types that support LENS retrofit are PTP 100, and PMP 100 and PMP 430 SM.



Figure 18: LENS mounted on a radio

Module Support Brackets

The SMMB1 support bracket facilitates mounting the SM to various surfaces of a structure and has slots through which chimney straps can be inserted. An SMMB1 is pictured in Figure 19. The SMMB1 is for use with an SM or an SM with a LENS. It is not for use with PMP 400 Series (OFDM) SMs or 900-MHz integrated or connectorized SMs, due to their greater weight and wind loading.

The SMMB2 is a heavy duty mounting bracket that comes with the 900-MHz integrated SM or AP, and with the 27D passive reflector. It is also available separately for use with 900-MHz connectorized SMs and APs, other connectorized modules, and 400 Series (OFDM) SMs.

The BH1209 is a pole-mount bracket kit for wireless Ethernet bridges.



Figure 19: SMMB1 SM support bracket

Cables

Modules that are currently or recently sold can auto-sense whether the Ethernet cable is wired as straight-through or crossover. Some modules that were sold earlier cannot. The MAC address, visible on the module, distinguishes whether the module can. All CMMmicros and CMM4s can auto-sense the cable scheme.

Where a non auto-sensing module is deployed

- a straight-through cable must be used for connection to a network interface card (NIC).
- a crossover cable must be used for connection to a hub, switch, or router.

Motorola-recommended Ethernet and sync cables can be ordered in lengths up to 328 ft (100 m) from Best-Tronics Manufacturing, Inc. at <http://www.best-tronics.com/motorola.htm>. These cables are listed in Table 10 and Table 11.

Table 10: Recommended outdoor UTP Category 5E cables

Best-Tronics Part #	Description
BT-0562	RJ-45 TO RJ-45; straight-through Ethernet cable
BT-0562S	RJ-45 TO RJ-45; shielded straight-through Ethernet cable
BT-0565	RJ-45 TO RJ-45; crossover Ethernet cable
BT-0565S	RJ-45 TO RJ-45; shielded crossover Ethernet cable
BT-0563	RJ-11 TO RJ-11; sync cable

Best-Tronics Part #	Description
BT-0563S	RJ-11 TO RJ-11; shielded sync cable
BT-0781S	RJ-45 to RJ-45; straight shielded Ethernet cable using outdoor STP Cat 5e cable, lower cost than plenum-rated, available only in black. Recommended for CMM4 to AP.



NOTE:

Shielded cable is strongly recommended for all AP cluster and BH installations.

Table 11: Recommended indoor UTP Category 5E cables

Best-Tronics Part #	Description
BT-0596	RJ-45 TO RJ-45; straight-through Ethernet cable
BT-0595	RJ-45 TO RJ-45; crossover Ethernet cable

Approved Ethernet cables can also be ordered as bulk cable:

- CA-0287
- CA-0287S (shielded)
- CA-0367 (lower cost, non-plenum-rated),
- CA-0367S (shielded, lower cost, non-plenum-rated)

Motorola-approved antenna cables can be ordered in lengths up to 100 ft (30.4 m), as listed in [Table 12](#).

Table 12: Recommended antenna cables

Best-Tronics Part #	Description
BT-0564	N TO N GPS antenna cable for CMM2
BT-0716	BNC TO N GPS antenna cable for CMMmicro and CMM4

Category 5 Cable Tester

For purchase within the U.S.A., the CTCAT5-01 Cable Tester is available.

Override Plug

An override plug (sometimes called a default plug) is available to provide access to a module whose password and/or IP address have been forgotten. This plug allows the AP, SM, or BH to be accessed using IP address 169.254.1.1 and no password. During the override session, you can assign any new IP address and set either or both user passwords (display-only and/or full access) as well as make other parameter changes.

This plug is available from Best-Tronics Manufacturing, Inc. at <http://www.best-tronics.com/motorola.htm> as Part BT-0583 (RJ-11 Default Plug). Alternatively if you wish, you can fabricate an override plug. For instructions, see [Procedure 33](#) on Page [384](#) and the pinout in [Figure 151](#) on Page [384](#).

Alignment Headset

The ACATHS-01 Alignment Headset facilitates the operation of precisely aiming an SM toward an AP (or a BHS toward a BHM). This device produces infinitely variable

- pitch, higher when the received signal is stronger.
- volume, louder when jitter is less.

An ACATHS-01 is pictured in [Figure 20](#).

Pinouts for an alternative listening device are provided under [Alignment Tone—Technical Details](#) on Page [186](#).




Figure 20: ACATHS-01 alignment headset

Module Housing

The HSG-01 Plastic Housing is available for replacement of a damaged housing on a module that is otherwise functional. The HSG-01 is pictured in [Figure 21](#).

The HSG-01 and all module housings of this design provide clearances for cable ties on the Ethernet and sync cables.



RECOMMENDATION:
Use 0.14" (40-lb tensile strength) cable ties to secure the Ethernet and sync cables to the cable guides on the module housing.

For the Ethernet cable tie, the Ethernet cable groove is molded lower at the top edge. For the sync cable tie, removal of a breakaway plug provides clearance for the sync cable, and removal of two breakaway side plates provides clearance for the sync cable tie.



Figure 21: HSG-01 Housing

**NOTE:**

No replacement housing is available for an OFDM radio.

5.3 FREQUENCY BAND RANGES

In the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency band ranges, APs, SMs, and wireless Ethernet bridges are available. APs and SMs are also available in the 900-MHz frequency band range. National restrictions may apply. See [Regulatory and Legal Notices](#) on Page 499.

To avoid self-interference, a network typically uses two or more of these ranges. For example, where properly arranged, all AP clusters and their respective SMs can use the 2.4-GHz range where the BH links use the 5.7-GHz range. In this scenario, subscriber links can span as far as 5 miles (8 km) with no reflector dishes, and the BH links can span as far as 35 miles (56 km) with reflector dishes on both ends or 16 miles (25 km) in 1X operation with LENS on both ends.

Within this example network, wherever the 2.4-GHz module is susceptible to interference from other sources, AP clusters and their linked SMs may use the 5.2-GHz range to span as far as 2 miles (3.2 km) with no reflector dishes. The network in this example takes advantage of frequency band range-specific characteristics of modules as follows:

- The 900-MHz modules cover a larger area, albeit with lower throughput, than modules of the other frequency bands. The 900-MHz modules can be used to
 - penetrate foliage
 - establish links that span greater distances
 - add subscribers
 - add overall throughput where modules of other frequency bands cannot be used (such as where interference would result or space on a tower is limited).
- The 2.4-GHz frequency band range supports AP/SM links of greater than 2-mile spans (with no reflectors).
- The 5.7-GHz frequency band range supports BH links that span as far as 35 miles.

5.4 PRODUCT COMPARISONS

5.4.1 Product Applications

The product applications per frequency band range are summarized in [Table 13](#).

Table 13: Product applications per frequency band range

Product	Frequency Band Range						
	900-MHz FSK	2.4-GHz FSK	4.9-GHz OFDM	5.2-GHz FSK	5.4-GHz FSK	5.4-GHz OFDM	5.7-GHz FSK
Access Point Module	•	•	•	•	•	•	•
Subscriber Module	•	•	•	•	•	•	•
Subscriber Module with Reflector ¹		•		•	•		•
Backhaul Module		•		•	•		•
Backhaul Module with Reflector ¹		•		•	•		•
CMMmicro	•	•	•	•	•	•	•
CMM2	•	•		•	•		•
CMM4	•	•	•	•	•	•	•
Power supply	•	•	•	•	•	•	•
Surge suppressor	•	•	•	•	•	•	•
NOTES:							
1. National or regional regulations may limit EIRP to the same as without a reflector, and therefore require Transmit Output Power to be reduced. In these cases							
<ul style="list-style-type: none"> ◦ the reflector used with an SM reduces beamwidth to reduce interference, but <i>does not</i> increase the range of the link. ◦ the reflector on both ends of a BH link reduces beamwidth to reduce interference and also increases the range of the link. 							

5.4.2 Link Performance and Encryption Comparisons

Encryption options are summarized in [Table 14](#). Typical Line-of-Site (LOS) range and aggregate useful throughput for PMP links are summarized in [Table 15](#). Typical Line-of-Site (LOS) range and aggregate useful throughput for PTP links are summarized in [Table 16](#).

Table 14: Products with encryption options available per frequency band, PMP links

Frequency Band	Products available with the following encryption options	
	DES or none	AES or none
900 MHz	•	•
2.4 GHz @100 mW (ETSI)	•	•
2.4 GHz @ 1W	•	•
4.9 GHz OFDM	•	
5.2 GHz	•	•
5.4 GHz FSK	•	•
5.4 GHz OFDM	•	
5.7 GHz	•	•

Table 15: Typical range and throughput per frequency band, PMP links

Frequency Band	CAP 130				CAP 120, 49400, 54400			
	Range		Aggregate Throughput Mbps	Round-trip Latency msec	Range		Aggregate Throughput Mbps	Round-trip Latency msec
	no SM Reflector mi (km)	with SM Reflector mi (km)			no SM Reflector mi (km)	with SM Reflector mi (km)		
900 MHz ⁴	40 (64)	na	4	15				
2.4 GHz ETSI	0.3 (0.5)	0.3 (0.5) ¹	14	6	0.6 (1)	0.6 (1) ¹	7	20
	0.6 (1)	0.6 (1) ¹	7	6				
2.4 GHz	2.5 (4)	7.5 (12)	14	6	5 (8)	15 (24)	7	20
	5 (8)	15 (24)	7	6				
4.9 GHz OFDM	1X				5 (8)		7	TBD
	2X				2.5 (4)		14	TBD
	3X				1.25 (2)		21	TBD
5.2 GHz	1 (1.6)	na ²	14	6	2 (3.2)	na ²	7	20
	2 (3.2)	na ²	7	6				
5.4 GHz	1 (1.6)	1 (1.6) ³	14	6	2 (3.2)	2 (3.2) ³	7	20
	2 (3.2)	2 (3.2) ³	7	6				
5.4 GHz OFDM	1X				5 (8)		7	TBD
	2X				2.5 (4)		14	TBD
	3X				1.25 (2)		21	TBD

Frequency Band	CAP 130				CAP 120, 49400, 54400			
	Range		Aggregate Throughput Mbps	Round-trip Latency msec	Range		Aggregate Throughput Mbps	Round-trip Latency msec
	no SM Reflector mi (km)	with SM Reflector mi (km)			no SM Reflector mi (km)	with SM Reflector mi (km)		
5.7 GHz	1 (1.6)	5 (8)	14	6	2 (3.2)	10 (16)	7	20
	2 (3.2)	10 (16)	7	6				

REFERENCED NOTES:

1. In Europe, 2.4-GHz ETSI and 5.4-GHz SMs can have a reflector added to focus the antenna pattern and reduce interference, but transmit output power must be reduced to maintain the same EIRP as without a reflector, so the throughput and range specs for PTMP links remain the same.
2. In the US and Canada, the use of a reflector with a full power radio in the 5.2-GHz frequency band is not allowed.
3. In US, Europe, and Australia, 5.4-GHz SMs can have a reflector added to focus the antenna pattern, reduce interference, and improve downlink gain, but transmit output power must be reduced to maintain the same EIRP as without a reflector, so the throughput and range specs for PTMP links remain the same. Reflectors are not allowed on 5.4-GHz SMs in Canada at this time.
4. All 900-MHz APs are CAP 09130s.

GENERAL NOTES:

Range is affected by RF conditions, terrain, obstacles, buildings, and vegetation.

A CAP 130 has an aggregate (sum of uplink plus downlink) throughput or capacity of 14 Mbps, if RF conditions, range, and SM hardware version permit.

An CSM 130 has an aggregate sustained throughput of 14 Mbps if RF conditions and range permit.

A regular SM can burst to 14 Mbps if RF conditions and range permit, then run at 7 Mbps sustained throughput.

An OFDM SM has an aggregate throughput or capacity of 21 Mbps, if RF conditions and range permit.

Table 16: Typical range and throughput per frequency band, PTP links

Frequency Band	Modulation Rate (Mbps)	Throughput	
		No Reflectors	Both Reflectors
2.4 GHz @100 mW (ETSI)	10	7.5 Mbps to 2 km	7.5 Mbps to 16 km
	20	14 Mbps to 1 km	14 Mbps to 8 km
2.4 GHz @ 1W	10	7.5 Mbps to 5 mi (8 km)	7.5 Mbps to 35 mi (56 km)
	20	14 Mbps to 3 mi (5 km)	14 Mbps to 35 mi (56 km)
4.9 GHz OFDM	1X	7 Mbps to 5 mi (8 km)	
	2X	14 Mbps to 2.5 mi (4 km)	
	3X	21 Mbps to 1.25 mi (2 km)	
5.2 GHz	10	7.5 Mbps to 2 mi (3.2 km)	
	20		
5.2 GHz ER	10		7.5 Mbps to 10 mi (16 km)
	20		14 Mbps to 5 mi (8 km)

Frequency Band		Modulation Rate (Mbps)	Throughput	
			No Reflectors	Both Reflectors
5.4 GHz		10	7.5 Mbps to 2 mi (3.2 km)	7.5 Mbps to 10 mi (16 km) ¹
		20	14 Mbps to 1 mi (1.6 km)	14 Mbps to 5 mi (8 km) ¹
5.4 GHz OFDM	1X		7 Mbps to 5 mi (8 km)	
	2X		14 Mbps to 2.5 mi (4 km)	
	3X		21 Mbps to 1.25 mi (2 km)	
5.7 GHz		10	7.5 Mbps to 2 mi (3.2 km)	7.5 Mbps to 35 mi (56 km)
		20	14 Mbps to 1 mi (1.6 km)	14 Mbps to 35 mi (56 km)

NOTES:

1. These ranges are with power reduced to within 1 W (30 dBm) EIRP.
2. Use the Link Estimator tool to estimate throughput for a given link.

5.4.3 Cluster Management Product Comparison

Motorola offers a choice among products for cluster management: CMM2, CMMmicro, or CMM4. Your choice should be based on the installation environment and your requirements. The similarities and differences between these two products are summarized in [Table 17](#).

Table 17: Cluster management product similarities and differences

Characteristic	CMM2	CMMmicro	CMM4
Approximate size	17" H x 13" W x 6.5" D (43 cm H x 33 cm W x 7 cm D)	12" H x 10" W x 3" D (30 cm H x 25 cm W x 8 cm D)	20.75" H x "14.75" x W x "7.75" D (52.7 cm H x 37.5 cm W x 19.7 cm D)
Approximate weight	25 lb (11.3 kg)	8 lb (3.5 kg)	14 lb (6.4 kg)
Cabling	one Ethernet/power cable per radio. one sync cable per radio.	one Ethernet/power/sync cable per radio.	one Ethernet/power/sync cable per radio.
Network interconnection	8 Ethernet ports	8 Ethernet ports	8 Ethernet ports
Data throughput	auto-negotiates to full or half duplex	auto-negotiates to full or half duplex	auto-negotiates to full or half duplex
Ethernet operating speed standard	auto-negotiates to 10Base-T or 100Base-TX	auto-negotiates to 10Base-T or 100Base-TX	auto-negotiates to 10Base-T or 100Base-TX
Additional Ethernet ports	one for data feed one for local access (notebook computer)	none	one copper 10/100/1000Base-T

Characteristic	CMM2	CMMmicro	CMM4
Optional Ethernet switch	none	none	12 10/100Base-T ports 1 copper Gigabit port 1 fiber optic Gigabit port
Power supply	integrated 24-V DC to power APs, BHs, and GPS receiver	external 24-V DC to power APs, BHs, and GPS receiver	20-v DC power output
SNMP management capability	none	provided	provided
Sync (to prevent self-interference)	carried by the additional serial cable to each AP and BHM	embedded in power-over-Ethernet cable	embedded in power-over-Ethernet cable
Time & Date	carried by the additional serial cable to each AP and BHM	provided by NTP (Network Time Protocol). CMMmicro can be an NTP server.	provided by NTP (Network Time Protocol). CMM4 can be an NTP server.
Weatherized	enclosure and power supply	only the enclosure (not the power supply)	only the enclosure (not the power supply)
Web interface	none	web pages for status, configuration, GPS status, and other purposes	web pages for status, configuration, GPS status, and other purposes
NOTE: Auto-negotiation of data throughput and Ethernet operating speed depend on the connected device being set to auto-negotiate as well.			

Each of these cluster management products is supported by its own dedicated user guide that which provides instructions for mounting and cabling the unit and verifying its connectivity to the network.

5.5 ANTENNAS FOR 900-MHz CONNECTORIZED MODULES

Like the 2.4-, 5.2-, 5.4-, and 5.7-GHz module, the 900-MHz connectorized module has

- the same housing.
- a covered Ethernet port.
- a utility port for an alignment headset, sync cable to CMM2, or override plug.

The 900-MHz AP or SM is available either

- as a connectorized unit with a 16-inch (approximately 40-cm) cable with a male N-type connector for connection to the antenna.
- with an integrated *horizontally*-polarized antenna in a different form factor.

Motorola has certified three connectorized flat panel antenna options. Motorola resells one of these. The three flat panel options are as follows:

- 10 dBi Maxrad Model # Z1681 (MP9027XFPT or Motorola AN900A), 26 dBm (390 mW). See <http://www.maxrad.com/>.
- 10 dBi Mars Model # MA-IS91-T2, 26 dBm (390 mW). See <http://www.mars-antennas.com/>.
- 10 dBi MTI Model # MT-2630003/N (MT-263003/N), 26 dBm (390 mW). See <http://www.mtiwe.com/>.

The attributes of each of these options are identical:

- gain—10 dBi
- polarization—vertical or horizontal
- cable—12-inch (30.5 cm)
- connector—female N-type
- beamwidth—approximately 60° vertical and 60° horizontal at 3 dBm

Motorola has certified other antennas, which are available through product resellers. The attributes of one of these other certified antennas include

- gain—10 dBi
- dimensions—12 x 12 x 1 inches (30.5 x 30.5 x 2.5 cm)
- weight—3.3 lbs (1.5 kg)
- polarization—vertical or horizontal
- connector—female N-type
- beamwidth—approximately 60° vertical and 60° horizontal at 3 dBm

An additional certified antenna is as follows: 17 dBi Last Mile Gear Cyclone Model # 900-17H Yagi, 18 dBm (63 mW). See <http://www.lastmilegear.com/>.

Examples of these antennas are pictured in [Figure 5](#) on [Page 52](#).

5.6 ADJUNCTIVE SOFTWARE PRODUCTS

The capabilities of available applications and tools are summarized for comparison in [Table 18](#). In this table, Prizm represents the element management system capabilities of Prizm, CNUT represents Canopy Network Updater Tool, and BAM represents the Bandwidth and Authentication Manager capabilities in Prizm.

Table 18: Applications and tools

Capability	Application or Tool		
	Prizm		CNUT
	Prizm Server	BAM Server	
authenticates SMs	•	•	
controls authentication in APs	•		•
manages Committed Information Rate (CIR)	•	•	
has dependency on another application ³			•
automatically discovers elements	•		•
exports network information with hierarchy	•		•
supports user-defined folder -based operations	•		•
senses FPGA version on an element	•		•
upgrades FPGA version on an element			•
manages the high-priority channel	•	•	
imports network information with hierarchy	•		•
interface to a higher-level network management system (NMS)	•		
interface to an operations support system (OSS)	•		
manages Maximum Information Rate (MIR)	•	•	
automatically works from root (highest) level			•
element selection can be individual or multiple	•	•	•
element selection can be criteria based	•		
element selection can be user-defined branch	•		•
senses software release on an element	•		•
upgrades software release on an element			•
manages VLAN parameters	•	•	
provides access to element web interface	•		

5.7 Prizm

Prizm Release 3.2 supports discovery and management of elements that run System Release 9.4.2.

5.7.1 Network Definition and Element Discovery

Prizm allows the operator to partition the entire network into criteria-based subsets that can be independently managed. To assist in this task of defining networks, Prizm auto discovers network elements that are in

- user-defined IP address ranges
- SM-to-AP relationships with APs in the user-defined range
- BHS-to-BHM relationships with BHMs in the user-defined range.

For an AP, SM, wireless Ethernet bridge, CMMmicro, or CMM4, Prizm

- auto discovers the element to the extent possible.
- includes the element in the network tree.
- shows general information.
- shows software-driven information.
- supports software-specific operations.

For a generic element, Prizm

- auto discovers the element as only a generic network element.
- includes the element in the network tree.
- shows general information.
- shows events and alerts.
- charts port activity.

For passive elements (such as CMM2 or a non-manageable switch or hub), Prizm allows you to enter into the network tree a folder/group with name, asset/owner information, and descriptive information.

In Prizm Release 3.2, supported element types include

- Canopy Access Point Module
- Canopy Prizm EMS
- Canopy Subscriber Module
- Cluster Management Module micro
- Cluster Management Module-4
- Cluster Management Module-4 Switch
- Cluster Management Module-4 Switch 14 Port
- Generic Group
- Generic SNMP Device
- Generic SNMP Device (08 Port)
- Generic SNMP Device (16 Port)
- Generic SNMP Device (24 Port)
- Generic SNMP Device (26 Port)
- PMP 400 AP (Canopy 4.9 OFDM Access Point)
- PMP 400 AP (Canopy 5.4 OFDM Access Point)
- PMP 400 SM (Canopy 4.9 OFDM Subscriber Module)
- PMP 400 SM (Canopy 5.4 OFDM Subscriber Module)
- PMP 500 AP (Canopy 3.5 OFDM Access Point)
- PMP 500 SM (Canopy 3.5 OFDM Subscriber Module)
- PTP 100 Master (Canopy Backhaul Master Module)
- PTP 100 Slave (Canopy Backhaul Slave Module)
- PTP 200 Master (Canopy 4.9 OFDM Backhaul Master Module)
- PTP 200 Master (Canopy 5.4 OFDM Backhaul Master Module)
- PTP 200 Slave (Canopy 4.9 OFDM Backhaul Slave Module)
- PTP 200 Slave (Canopy 5.4 OFDM Backhaul Slave Module)
- PTP 300 Master (High-Speed Backhaul Master Module)
- PTP 300 Slave (High-Speed Backhaul Slave Module)
- PTP 400 Master (High-Speed Backhaul Master Module 30/60 Mbps)
- PTP 400 Slave (High-Speed Backhaul Slave Module 30/60 Mbps)
- PTP 500 Master (High-Speed Backhaul Master Module)
- PTP 500 Slave (High-Speed Backhaul Slave Module)
- PTP 600 Master (High-Speed Backhaul Master Module 150/300 Mbps)
- PTP 600 Slave (High-Speed Backhaul Slave Module 150/300 Mbps)
- Powerline MU/Gateway
- Powerline Modem

5.7.2 Monitoring and Fault Management

Prizm receives the traps that elements send and generates an alert for each of these. Prizm also allows the user to establish sets of criteria that would generate other alerts and trigger email notifications. Optionally, the user can specify a trap template. In this case, Prizm receives traps for generic elements in the network.

For any individual element that the user selects, Prizm offers text and graphed displays of element configuration parameters and performance statistics from an interval that the user specifies.

5.7.3 Element Management

Prizm allows the user to perform any of the following operations on any specified element or group of elements:

- Manage
 - large amounts of SNMP MIB data.
 - module passwords.
 - IP addresses.

- other communications setup parameters.
- site information: Site Name, Site Location, and Site Contact parameters.
- o Reset the element.

5.7.4 BAM Subsystem in Prizm

Prizm integrates Bandwidth and Authentication Manager (BAM) functionality and supports the maintenance of authentication and bandwidth data on a RADIUS server.

Either of the following modes is available for the Prizm server, subject to licensing:

- o BAM-only functionality, which manages only authentication, bandwidth service plans, and VLAN profiles of SMs.
- o Full Prizm functionality, which manages attributes for all elements and authentication of SMs.

One difference between a service plan (or VLAN profile) and a configuration template that has the identical set of attributes is that the former is a long-term association whereas the latter is a one-time push to the element. When a service plan or VLAN profile is modified, the change is automatically applied to all elements that have the association. Another difference is that a configuration template cannot overwrite any values that a service plan or VLAN profile has set in an element.

5.7.5 Northbound Interface

Prizm provides three interfaces to higher-level systems:

- o a Simple Network Management Protocol (SNMP) agent for integration with a network management system (NMS).
- o a Simple Object Access Protocol (SOAP) XML-based application programming interface (API) for web services that supports integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system.
- o console automation that allows such higher-level systems to launch and appropriately display the Prizm management console in GUI that is custom developed, using the *PrizmEMS™ Software Development Kit (SDK)*, which Motorola provides for this purpose.

Together these interfaces constitute the Northbound Interface feature. Prizm server administrator tasks and GUI developer information are provided in the *PrizmEMS™ Software Development Kit (SDK)*. This SDK also describes the how to define new element types and customize the Details views.

All other features of the Prizm product are supported by the dedicated document *Motorola Canopy Prizm Release 3.2 User Guide* and associated release notes.

5.8 LICENSE MANAGEMENT

Under the original licensing regime, licenses were permanently tied to the Media Access Control (MAC) address of the equipment that was licensed or that used the licensed feature. Thus, they were not transferable. Under server-based license management, for some functionalities, Motorola offers licenses that

- float upon demand within the network.
- are tied to only the MAC address of the license management server for which they were ordered.

Server-based license management adds flexibility and makes available licenses that previously would have been held by de-commissioned equipment. License management technology from Macrovision, based on a FLEXnet™ Publisher license management model, provides the platform for server-based licensing. Capabilities that are authorized by licenses on this platform are *FLEXenabled* products. In this platform, the license management server checks and then either assigns or declines to assign a license in real time.

The total number of floating license keys that you need for any feature is the highest number that you will ever want to have simultaneously in use. The proper placement of these keys and the number and placement of fixed licenses are listed in [Table 19](#).

Table 19: Correct placement of license keys

In This Release	License Key	Must Be in Directory	If This Platform	On This Server Device
Prizm for full mgmt	PrizmEMS Server, Element Pack BAM Server, AP Auth Server (APAS), Cap 2 Canopy Lite	C:\Canopy\Prizm\FLEXnet\license_files	Windows	LM server ¹
		/usr/local/Canopy/Prizm/FLEXnet/license_files	Enterprise Linux	
Prizm for BAM-only or redundant BAM	BAM Server, AP Auth Server (APAS), Cap 2 Canopy Lite	C:\Canopy\Prizm\FLEXnet\license_files	Windows	LM server ²
		/usr/local/Canopy/Prizm/FLEXnet/license_files	Enterprise Linux	
NOTES:				
1. One BAMServer key and one PrizmEMSServer key required per each full management Prizm server.				
2. One key required per each deployed BAM server.				

5.9 SPECIFICATIONS AND LIMITATIONS

5.9.1 Radios

Radio specifications are provided at

<http://www.motorola.com/business/v/index.jsp?vnextoid=7cc777c8cd658110VgnVCM100008406b00aRCRD&vnextchannel=926577c8cd658110VgnVCM100008406b00aRCRD&applInstanceName=default> for all radios, and specifically at

- <http://www.motorola.com/business/v/index.jsp?vnextoid=7cc777c8cd658110VgnVCM100008406b00aRCRD&vnextchannel=926577c8cd658110VgnVCM100008406b00aRCRD&applInstanceName=default> for PTP bridges.
- <http://www.motorola.com/business/v/index.jsp?vnextoid=7cc777c8cd658110VgnVCM100008406b00aRCRD&vnextchannel=926577c8cd658110VgnVCM100008406b00aRCRD&applInstanceName=default> for PMP modules.

5.9.2 Cluster Management Products

CMM specifications are provided in the documents that support the various models of CMM.

5.9.3 600SS Surge Suppressor

600SS Surge Suppressor specifications are as follows:

Dimensions	H 5.2" x W 5.0" x D 1.7" (132 mm x 127 mm x 43.2 mm)
Space between mounting holes	4.24" (108 mm)
Size of Knockouts	0.75" (19 mm)
Weight	0.4 lbs
Operating Temperature	-40°C to +55°C (-40°F to 131°F)
Internal Connectors	RJ-45
Capacity	1500J peak energy dissipation with 10/10000 micro sec waveform
Digital Noise Isolation Option (to eliminate ground loops)	Yes

6 DIFFERENTIATING AMONG COMPONENTS

6.1 INTERPRETING MODEL NUMBER

The model number of a module typically represents

- the model number, which may indicate
 - radio frequency band range.
 - link distance range.
 - whether the module is a CAP/CSM 130 or not.
 - the factory-set encryption standard.
- the module type.
- whether the reflector dish is included.
- the antenna scheme of the module.
- whether adjustable power in the module is preset to low.
- the modulation capability.

Radio Frequency Band Range

The leading two digits usually indicate the frequency band range in which the module can operate. For example, if the model number is 5700BH, then the frequency band range of the module is 5.7 GHz.



5 7 0 0 B H

You cannot change the frequency band range of the module.

Link Distance Range or Series 130/09130

The third digit in the model number may indicate whether the module is an extended range, or a 130/09130 instead of a 120 in the PMP 100 Series. 1 indicates extended range, with power adjustable up to 23 dBm. 5 in the third position (5250AP, for example) indicates that the module is a CAP 130 or CSM 130. However, model numbering for 900-MHz APs and SMs differs from this general rule. All APs and SMs in this frequency band range are 09130, but none of their model numbers use 5 in the third position.



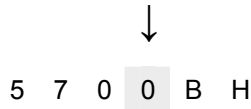
5 7 0 0 B H

0 in the third position (5200AP, for example) indicates that the module is standard (not extended range, but rather capped to the maximum of 5 dBm, and not a CAP 130 or CSM 130).

You cannot change the link distance range of the module. However, you can license an SM to uncaps its aggregate throughput (for capability of the CSM 130).

Encryption Standard or Frequency Band Range

The fourth digit in the model number usually indicates the encryption standard that was preset at the factory. 1 indicates the Advanced Encryption Standard (AES). 0 indicates the Data Encryption Standard (DES) standard. For example, if the model number is 5701BH, then transmissions from the module are encrypted according to AES. If the model number is 5700BH, then transmissions from the module are encrypted according to DES.



You cannot change the encryption basis (from DES to AES, for example), but you can enable or disable the encryption.

Module Type

The next two alpha characters indicate the module type. For example, CK indicates that the module is a Cluster Management Module.



The module type cannot be changed.

Reflector Added

In specifications tables and price lists, the trailing characters RF or RF20 indicate that the associated information applies to the module being

- mounted to the 27RD Passive Reflector Dish, in the case of specifications.
- ordered with the 27RD Passive Reflector Dish, in the case of price lists.



However, this designation is not shown on either label of the module, and a module ordered with the dish can be deployed without the dish.

Antenna Scheme, Low Power Option, or Indoor Module

In specifications tables and price lists, the trailing character C indicates that the module is connectorized for an external antenna. CLP indicates that the module is low power and connectorized (for example, 2400SMCLP).



An F in this position indicates that the module has an integrated (internal) antenna with a band-pass, also known as interference migration, filter (for example, 9000APF). F2 in this position indicates that the module has a 2-channel band-pass filter (9000APF2). HZ indicates that the module has a horizontally polarized internal antenna (5200SMHZ).

A Q in this position indicates that the module has an integrated antenna and is designed for indoor deployment (for example, 9000SMQ).

You cannot transform a module from connectorized to internal antenna or from internal antenna to connectorized, but you may have flexibility in what external antenna you deploy with it.

Modulation Capability

A trailing 20 indicates that the module is capable of being set to either

- 20-Mbps modulation (aggregate throughput of 14 Mbps) for Full operation
- 10-Mbps modulation (aggregate throughput of 7 Mbps) for Lite operation.



2 4 0 0 B H R F 2 0

The absence of a trailing 20 indicates that the module is capable of only 10-Mbps modulation (Lite).

6.2 SORTED MODEL NUMBERS

Model numbers of PMP 100, PMP 400, PTP 100, and PTP 200 series modules are listed in [Table 20](#). Not all products are available in all regions or in all markets. Check with your distributor or reseller for availability.

Table 20: Model numbers

Range	Integrated Antenna				Connectorized for Antenna			
	Except 130 Series		130 PMP 100		Except 130 Series		130 PMP 100	
	DES	AES	DES	AES	DES	AES	DES	AES
900 MHz			9000AP 9000APF 9000APF2 9000SM 9000SMF 9000SMF2 9000SMQ	9001AP 9001APF 9001APF2 9001SM 9001SMF 9001SMF2			9000APC 9000SMC	9001APC 9001SMC
2.4 GHz	2400AP 2400SM 2400BH 2400BH20 2400BHRF 2400BHRF20	2401AP 2401SM 2401BH 2401BH20 2401BHRF 2401BHRF20	2450AP 2450SM	2451AP 2451SM	2400SMCLP	2401SMCLP		

Range	Integrated Antenna				Connectorized for Antenna			
	Except 130 Series		130 PMP 100		Except 130 Series		130 PMP 100	
	DES	AES	DES	AES	DES	AES	DES	AES
4.9 GHz	4940AP 4940SM 4940BH	4941AP 4941SM 4941BH			4940APC 4940SMC 4940BHC	4941APC 4941SMC 4941BHC		
5.2 GHz	5200AP 5200APHZ 5200SM 5200SMHZ 5200BH 5210BHRF 5210BHRF20	5201AP 5201SM 5201BH 5211BH20 5211BHRF 5211BHRF20	5250AP 5250APHZ 5250SM 5250SMHZ	5251AP 5251SM				
5.4 GHz FSK	5400AP 5400APHZ 5400SM 5400SMHZ 5400BH 5400BH20 5400BHRF 5400BHRF20	5401AP 5401SM 5401BH 5401BH20 5401BHRF 5401BHRF20	5450AP 5450APHZ 5450SM 5450SMHZ	5451AP 5451SM				
5.4 GHz OFDM	5440AP 5440SM 5440BH	5441AP 5441SM 5441BH			5440APC 5440SMC 5440BHC	5441APC 5441SMC 5441BHC		
5.7 GHz	5700AP 5700APHZ 5700SM 5700SMHZ 5700BH 5700BH20 5700BHRF 5700BHRF20	5701AP 5701SM 5701BH 5701BH20 5701BHRF 5701BHRF20	5750AP 5750APHZ 5750SM 5750SMHZ	5751AP 5751SM	5700APC 5700BHC 5700BHC20	5701APC 5701BHC	5750APC	5751APC

6.3 INTERPRETING ELECTRONIC SERIAL NUMBER (ESN)

Module labels contain a product serial number that could be significant in your dealings with Motorola or your supply chain. This is the electronic serial number (ESN), also known as the Media Access Control (MAC) address, of the module. This hexadecimal number identifies the module in

- communications between modules.
- the data that modules store about each other (for example, in the **Registered To** field).
- the data that the BAM software applies to manage authentication and bandwidth.
- Prizm auto discovery of SMs through the AP (or BHS through the BHM).
- software upgrades performed by CNUT.
- information that CNUT passes to external tools.

6.4 FINDING THE MODEL (PART) NUMBER AND ESN

The labels and locations of module model (part) numbers and ESNs are shown in [Table 21](#).

Table 21: Labels and locations of model (part) numbers and ESNs

Numeric String	Label and Location	
	Older Modules	Newer Modules
Model number	PN outside	Model # outside
ESN/MAC address	S/N inside	ESN outside

7 LINK CHARACTERISTICS

7.1 UNDERSTANDING BANDWIDTH MANAGEMENT

7.1.1 Downlink Frame

A full frame consists of a downlink frame and an uplink frame. The downlink frame transmitted from the AP consists of

- a beacon
- an uplink map that tells each SM which slots it can use in the next uplink frame
- broadcast and per-SM data.

Each SM retrieves broadcast data and data addressed to that SM and passes that data through its Ethernet port to connected devices.

The beacon communicates

- timing
- ratio of uplink to downlink allocation
- ESN of the AP
- color code
- protocol (point-to-point or point-to-multipoint)
- number of registered SMs
- frame number
- number of reserved control slots
- air delay, subject to the value of the Max Range parameter in the AP.

7.1.2 Uplink Frame

The uplink frame transmitted from the SMs consists of

- per-SM data in slots assigned by the uplink map in the previous downlink frame
- bandwidth requests for data slots in future uplink frames.

Bandwidth requests are sent as control slots, which are half the size of a data slot. The operator configures a number of reserved control slots. In addition to the reserved control slots, space in any data slots in a given uplink frame not assigned by the uplink map is also available for bandwidth requests.

An SM makes a bandwidth request when it has data to transmit. Bandwidth requests are contention requests and are the only part of the Media Access Layer that uses contention. If two or more SMs make bandwidth requests using the same control slot (or half-unused-data slot), it is likely the AP will not be able to understand the requests. The SMs retransmit any bandwidth requests that do not result in assignments in the uplink map.

7.1.3 Slot Calculation

The frame consists of slots which hold 64-byte fragments of packet data. The number of uplink and downlink data slots is determined by

- the **Downlink Data %** configured by the operator, which determines the ratio of downlink to uplink data slots.
- the **Max Range** setting configured by the operator, which determines how much time in the frame must be reserved for air delay and not used for data.
- the number of reserved **Control Slots** configured by the operator. Control slots are half the size of data slots and every other reserved control slot (starting with either the first or second, depending on how the **Max Range** setting has influenced frame structure) reduces the number of data slots by one.

7.1.4 Startup Sequence

When an SM boots, the following sequence occurs:

1. The SM detects the beacon slot from an AP.
2. The SM synchronizes with the AP.
3. If BAM is configured on the AP, and the AP is licensed for authentication, then
 - a. the AP sends a Registration Request message to Prizm for authentication.
 - b. following a successful challenge, Prizm returns an Authentication Grant message to the AP.
 - c. the AP sends a Registration Grant to the SM.

If BAM is not configured on the AP, or if the AP is not licensed for authentication, then the AP simply returns the Registration Grant to the SM.

This Registration Grant includes the air delay (distance) between the AP and SM. The SMs are at various distances from the AP, and each of them uses its air delay value to determine when to begin its uplink transmission. This results in uplink transmissions from multiple SMs at various distances all being in sync when the AP receives them.

7.1.5 Data Transfer Capacity

Modules use Time Division Duplex (TDD) on a common frequency to divide frames for uplink (orange) and downlink (green) usage, as shown in [Figure 22](#).

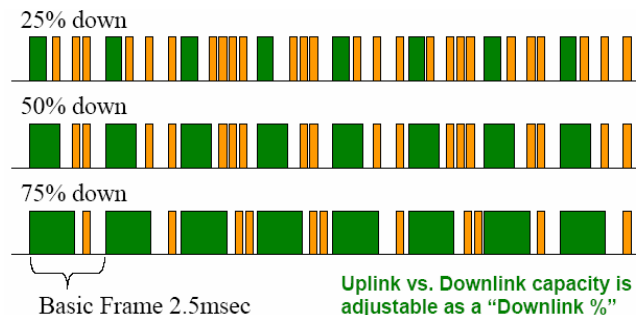


Figure 22: TDD dividing frames

7.1.6 Maximum Information Rate (MIR) Parameters

Point-to-multipoint links use the following four MIR parameters for bandwidth management:

- **Sustained Uplink Data Rate** (kbps)
- **Uplink Burst Allocation** (kb)
- **Sustained Downlink Data Rate** (kbps)
- **Downlink Burst Allocation** (kb)

You can independently set each of these parameters per AP or per SM.

Token Bucket Algorithm

The software uses a *token bucket* algorithm that

- stores credits (tokens) for the SM to spend on bandwidth for reception or transmission.
- drains tokens during reception or transmission.
- refills with tokens at the sustained rate set by the network operator.

For each token, the SM can send toward the network in the uplink (or the AP can send toward the SM in the downlink) an equivalent number of kilobits. Two buckets determine the permitted throughput: one in the SM for uplink and one in the AP for downlink.

The applicable set of **Uplink Burst Allocation** and **Downlink Burst Allocation** parameters determine the *number* of tokens that can fill each bucket. When the SM transmits (or the AP transmits) a packet, the equivalent number of tokens is removed from the uplink (or downlink) bucket.


Except when full, the bucket is continuously being refilled with tokens at *rates* that the applicable set of **Sustained Uplink Data Rate** and **Sustained Downlink Data Rate** parameters specify. The bucket often drains at a rate that is much faster than the sustained data rate but can refill at only the sustained data rate. Thus, the effects of the allocation and rate parameters on packet delay are as follows:

- the burst allocation affects how many kilobits are processed before packet delay is imposed.
- the sustained data rate affects the packet delay that is imposed.

Which set of these MIR parameters are applicable depends on the interactions of other parameter values. These interactions are described under [Setting the Configuration Source](#) on Page 292. Also, where the **Configuration Source** parameter setting in the AP specifies that BAM values should be used, they are used only if Prizm is configured to send the values that it stores for the MIR parameters.

MIR Data Entry Checking

Uplink and downlink MIR is enforced as shown in [Figure 23](#).



NOTE:
In these figures, *entry* refers to the setting in the data rate parameter, not the burst allocation parameter.

$$\text{uplink cap enforced} = \frac{\text{uplink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

$$\text{downlink cap enforced} = \frac{\text{downlink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

Figure 23: Uplink and downlink rate caps adjusted to apply aggregate cap

For example, in the SM, if you set the **Sustained Uplink Data Rate** parameter to 2,000 kbps and the **Sustained Downlink Data Rate** parameter to 10,000 kbps, then the uplink and downlink MIR that will be enforced for the SM can be calculated as shown in [Figure 24](#).

$$\text{uplink cap enforced} = \frac{2,000 \text{ kbps} \times 7,000 \text{ kbps}}{2,000 \text{ kbps} + 10,000 \text{ kbps}} = 1,167 \text{ kbps}$$

$$\text{downlink cap enforced} = \frac{10,000 \text{ kbps} \times 7,000 \text{ kbps}}{2,000 \text{ kbps} + 10,000 \text{ kbps}} = 5,833 \text{ kbps}$$

Figure 24: Uplink and downlink rate cap adjustment example

In this example case, the derived 1,167-kbps uplink and 5,833-kbps downlink MIR sum to the fixed 7,000-kbps aggregate cap of the SM.

7.1.7 Committed Information Rate

The Committed Information Rate (CIR) capability feature enables the service provider to guarantee to any subscriber that bandwidth will never decrease to below a specified minimum, unless CIR is oversubscribed. Bandwidth can be, and typically will be, higher than the minimum, but this guarantee helps the WISP to attract and retain subscribers.

In BAM Release 2.1 and in Prizm Release 2.0, CIR configuration is supported as follows:

- The GUI allows you to view and change CIR configuration parameters per SM.
- When an SM successfully registers and authenticates, if BAM or Prizm has CIR configuration data for the SM, then messages make the CIR configuration available to the SM, depending on the Configuration Source setting. (See [Setting the Configuration Source](#) on Page 292.)
- The operator can disable the CIR feature in the SM without deleting the CIR configuration data.

7.1.8 Bandwidth from the SM Perspective

In the SM, normal web browsing, e-mail, small file transfers, and short streaming video are rarely rate limited with practical bandwidth management (QoS) settings. When the SM processes large downloads such as software upgrades and long streaming video or a series of medium-size downloads, the bucket rapidly drains, the burst limit is reached, and some packets are delayed. The subscriber experience is more affected in cases where the traffic is more latency sensitive.

Example download times for various arbitrary tiers of service are shown in [Table 63](#) on Page 390 and [Table 64](#) on Page 391.

7.1.9 Interaction of Burst Allocation and Sustained Data Rate Settings

If the Burst Allocation is set to 1200 kb and the Sustained Data Rate is set to 128 kbps, a data burst of 1000 kb is transmitted at full speed because the Burst Allocation is set high enough. After the burst, the bucket experiences a significant refill at the Sustained Data Rate. This configuration uses the advantage of the settable Burst Allocation.

If both the Burst Allocation and the Sustained Data Rate are set to 128 kb, a burst is limited to the Burst Allocation value. This configuration does not take advantage of the settable Burst Allocation.

If the Burst Allocation is set to 128 kb and the Sustained Data Rate is set to 256 kbps, the actual rate will be the burst allocation (but in kbps). As above, this configuration does not take advantage of the settable Burst Allocation.

7.1.10 High-priority Bandwidth

To support low-latency traffic such as VoIP (Voice over IP) or video, the system implements a high-priority channel. This channel does not affect the inherent latencies in the system but allows high-priority traffic to be immediately served. The high-priority pipe separates low-latency traffic from traffic that is latency tolerant, such as standard web traffic and file downloads.



IMPORTANT!

The number of channels available to the AP is reduced by the number of SMs configured for the high-priority channel. With this feature enabled on all SMs, an AP can support 100 SMs (instead of 200).

A module prioritizes traffic by

- reading the Low Latency bit (Bit 3) in the IPv4 Type of Service (ToS) byte in a received packet.
- reading the 802.1p field of the 802.1Q header in a received packet, where VLAN is enabled on the module.
- comparing the 6-bit Differentiated Services Code Point (DSCP) field in the ToS byte of a received packet to a corresponding value in the DiffServe tab of the Configuration page of the module.

Low Latency Bit

Bit 3 is set by a device outside the system. In the uplink frame, the SM monitors Bit 3. If this bit is set, then

- the SM prioritizes this traffic in its high-priority queue according to AP configuration settings for the high-priority channel.
- the system sends the packet on the high-priority channel and services this channel before any normal traffic.

802.1P Field

See [Priority on VLANs \(802.1p\)](#) on Page 170.

DSCP Field

Like Bit 3 of the original IPv4 ToS byte, the DSCP field (Bits 0 through 5) in the redefined ToS byte is set by a device outside the system. A packets contains no flag that indicates whether the encoding is for the Low Latency bit or the DSCP field. For this reason, you must ensure that all elements in your trusted domain, including routers and endpoints, set and read the ToS byte with the same scheme.

Modules monitor ToS bytes with DSCP fields, but with the following differences:

- The 6-bit length of the field allows it to specify one of 64 service differentiations.
- These correlate to 64 individual (**CodePoint**) parameters in the DiffServe tab of the Configuration page.
- Per RFC 2474, 3 of these 64 are preset and cannot be changed. (See <http://www.faqs.org/rfcs/rfc1902.html>.)
- For any or all of the remaining 61 CodePoint parameters, you can specify a value of
 - 0 through 3 for low-priority handling.
 - 4 through 7 for high-priority handling.



RECOMMENDATION:

Ensure that your Differentiated Services domain boundary nodes mark any entering packet, as needed, so that it specifies the appropriate Code Point for that traffic and domain. This prevents theft of service level.

An example of the DiffServe tab in the Configuration page and parameter descriptions are provided under [DiffServe Tab of the AP](#) on Page 253. This tab and its rules are identical from module type to module type. However, any of the 61 configurable Code Points can be set to a different value from module to module, thus defining unique per-hop behavior for some traffic.

This tab in the AP and BHM sets the priorities for the various packets in the downstream (sent from the public network). This tab in the SM and BHS sets the priorities for the various packets in the upstream (sent to the public network).

Typically, some SMs attach to older devices that use the ToS byte as originally formatted, and others to newer devices that use the DSCP field. The *default* values in the DiffServe tab allow your modules to prioritize traffic from the older devices roughly the same as they traditionally have. However, these default values may result in more high-priority traffic as DSCP fields from the newer devices are read and handled. So, after making any changes in the DiffServe tab, carefully monitor the high-priority channel for high packet rates

- in SMs that you have identified as those to initially set and watch.
- across your network when you have broadly implemented Code Point values, such as via SNMP.

7.1.11 Traffic Scheduling


This release requires APs, BHs, and AES SMs to be Series P9 or later hardware.² The characteristics of traffic scheduling in a sector are summarized in [Table 22](#).

Table 22: Characteristics of traffic scheduling

Category	Factor	Treatment
Throughput	Aggregate throughput, less additional overhead	14 Mbps
Latency	Number of frames required for the scheduling process	1
	Round-trip latency ¹	≈ 6 ms
	AP broadcast the download schedule	No

² See [Designations for Hardware in Radios](#) on Page 377.

Category	Factor	Treatment
High-priority Channel	Allocation for <i>uplink</i> high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Allocation for <i>downlink</i> high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Order of transmission	<ol style="list-style-type: none"> 1. CIR high-priority 2. CIR low-priority 3. Other high-priority 4. Other low-priority
Transmit Frame Spreading	Support for Transmit Frame Spreading feature	In Release 7.0 and later
CIR	Capability	In all releases
NOTES: 1. For 2.4- and 5. <i>n</i> -GHz modules.		



CAUTION!
 Power requirements affect the recommended maximums for power cord length feeding the CMMmicro or CMM4. See the dedicated user guide that supports the CMM that you are deploying. However, the requirements *do not* affect the maximums for the CMM2.

Packets that have a priority of 4 to 7 in either the DSCP or a VLAN 802.1p tag are automatically sent on the high-priority channel, but only where the high-priority channel is enabled.

7.1.12 2X Operation

A General tab option in both CSM 130s and hardware series P9 and greater CSM 120s provides double the aggregate throughput for SMs that are nearer than half of the maximum typical range from the AP. The requirements of this feature are as follows:

- The AP must be a CAP 130 (Advantage AP).
- The SM must be near the AP, roughly half the range of 1X.
- The SM must be of the P9 hardware series or later and enabled for hardware scheduling. See [Designations for Hardware](#) on Page 377.
- The **2X Rate** parameter in the SM must be set to enabled. This is the default setting.
- The amount of noise and multipath must be low enough to allow the receiver in the 6 dB less sensitive (2X) state to maintain a high carrier-to-interference (C/I) ratio.

The flexibility of this feature is as follows:

- At the time of registration, signaling is at the 1X rate. However, if the above requirements are all met, then the SM switches to 2X.
- Thereafter, whenever RF conditions are unfavorable for 2X operation, the SM switches to 1X. When favorable RF conditions allow, the SM switches back to 2X, if user data is present at that time.
- Similarly, whenever no user data is present, the SM switches to 1X. When user data flow resumes, the SM switches back to 2X, if RF conditions allow.
- Both links for the SM (uplink and downlink) are independent for this feature. (One can be operating at 2X operation while the other is operating at 1X.)
- Other SMs in the sector can be communicating with the AP at the other modulation rate.
- Although subscribers with CSM 120s realize higher bursts, and subscribers with CSM 130s and CSM 09130s realize both higher burst and higher sustained throughput, the network operator realizes higher sector throughput capacity in the AP.

The effect of 2X operation on aggregate throughput for the SM is indicated in [Table 23](#).

Table 23: Effect of 2X operation on throughput for the SM

Type of SM	Typical Aggregate Rates ¹	
	Sustained ²	Burst ²
CSM 09130	4 Mbps	4 Mbps
CSM 120 with at least P9 Hardware Series	7 Mbps	14 Mbps
CSM 54400	14 Mbps	14 Mbps
NOTES:		
1. Subject to competition among all SMs in the sector.		
2. Can be less if limited by the value of Downlink Data set in the Radio tab of the Configuration page in the AP.		

Competition for Bandwidth

When multiple SMs vie for bandwidth, the AP divides its bandwidth among them, considering their effective CIR and MIR values. However, 2X operation uses bandwidth twice as efficiently as 1X, even where MIR values apply. This is because, in 2X operation, the modules transmit their data in 4-level frequency shift keying (FSK), not 2-level as they would in 1X operation. This moves twice the data per slot. Thus, for the sum of all bandwidth that 2X-eligible customers use, the bandwidth available to the remaining customers increases by half of that sum when these eligible customers are transmitting and receiving in 2X operation.

Checking Link Efficiencies in 2X Operation

Unlike in 1X operation, efficiencies below 90% on the Link Capacity Test tab in the Tools web page of the SM may be acceptable for stable operation. An efficiency of 60% in 2X operation is equivalent to an efficiency of 120% in 1X. If you read efficiency between 60% and 90%, check the status of 2X operation (as described below) to confirm that the link is operating at 2X.

Since received signal strength typically varies over time, you should perform link tests at various times of day and on various days of the week. Efficiencies should consistently be 60% or greater for 2X operation. You may be able to achieve better efficiencies by re-aiming the SM, mounting it elsewhere, or adding a reflector dish.

Checking the Status of 2X Operation

The Session Status tab in the Home page of the AP provides operation status information about each *SM-to-AP* link. Under the MAC address of each SM, the data in this tab includes a line such as the following:

```
RATE : VC 19 Rate 2X/2X VC 255 Rate 2X/1X
```

Interpret this information is as follows:

- VC means virtual channel. If one VC is displayed, the high-priority channel is disabled. If two are displayed, the high-priority channel is enabled and is using the higher number VC (255 in the above example).
- 2X/2X indicates that the SM-to-AP link is in 2X operation.
- 2X/1X indicates that the SM is capable of 2X operation but the SM-to-AP link is in 1X operation. This can be for either of the following reasons:
 - The SM has not sent data on the channel yet.
 - The received signal does not support 2X operation.
- 1X/1X indicates that the SM is capable of only 1X operation. This can be for either of the following reasons:
 - The SM does not support 2X operation (SM is of the hardware series P7 or P8).
 - The **2X Rate** parameter is disabled in the General tab of the Configuration page in the SM or the AP.



CAUTION!

2X operation requires approximately 3 to 5% more power than 1X operation. This additional power affects the recommended maximum for power cord length feeding the CMMmicro or CMM4. See the dedicated user guide that supports the CMM model that you are deploying. However, 2X operation *does not* affect the maximums for the CMM2.

Disabling 2X Operation

Disabling 2X operation for an SM can be helpful for alignment, troubleshooting, or preventing frequent automatic switches between 2X and 1X, where RF conditions are only marginally favorable to 2X. The ability to disable 2X for an SM is inherent since the 2X Operation feature was introduced.

Disabling 2X operation for a sector can be helpful for identifying a baseline for 1X-to-2X comparison, broader troubleshooting activities, or forcing all SMs to 1X rather than disabling 2X in each SM. The General tab of the Configuration page in the AP provides a **2X Rate** parameter:

- If you click **Disable**, then **Save Changes** and **Reboot**, 2X operation is disabled for the sector, regardless of the 2X Rate setting in each SM.
- If you later click **Enable**, then **Save Changes** and **Reboot**, 2X operation is enabled in the sector for SMs with 2X Rate enabled on their Configuration>General page. SMs with 2X Rate disabled on their Configuration>General page (or P7 or P8 SMs that don't support 2X Rate) will only operate at 1X.

If you want to cap the bandwidth usage of certain SMs, it is generally wiser to use the Maximum Information Rate (MIR) parameters of those SMs to do so, instead of locking down the operation rate for the entire sector. See [Maximum Information Rate \(MIR\) Parameters](#) on Page 87.

7.1.13 3X Operation

OFDM modules offer an additional modulation scheme that provides 3X operation as an alternative to 1X or 2X operation. In clear space, 3X operation is possible over half the range of 2X (which means it is possible over one-fourth the range of 1X). However, in NLOS installations, multipathing may be the predominant RF issue, not free-space attenuation, so the relationship between 1X, 2X, and 3X range may differ from clear space situations.

The effect of operation rate on the performance of OFDM modules in 10-MHz channel width deployment is generalized in [Table 24](#). Aggregate throughput refers to the sum of the uplink throughput plus the downlink throughput.


Table 24: OFDM module performance at 1X, 2X, and 3X operation

Product	Performance Specification	Performance Details		
		1X	2X	3X
PMP 49400 PTP 49200	Modulation	QPSK	16 QAM	64 QAM
	Typical Maximum Range	15 mi (24 km)	4 mi (6.5 km)	2 mi (3.2 km)
	Typical Maximum Aggregate Throughput	7 Mbps	14 Mbps	20 Mbps
	Nominal Receive Sensitivity including FEC	-89 dBm	-80 dBm	-71 dBm
	Latency	5-7 ms	5-7 ms	5-7 ms
PMP 54400 PTP 54200	Modulation	QPSK	16 QAM	64 QAM
	Typical Maximum Range	5 mi (8 km)	2.5 mi (4 km)	1.25 mi (2 km)
	Typical Maximum Aggregate Throughput	7 Mbps	14 Mbps	20 Mbps PMP 21 Mbps PTP
	Nominal Receive Sensitivity including FEC	-89 dBm	-78 dBm	-70 dBm
	Latency	5-7 ms	5-7 ms	5-7 ms

Product	Performance Specification	Performance Details		
		1X	2X	3X
PMP 58430	Modulation	QPSK	16 QAM	64 QAM
	Typical Maximum Range	7 mi (11.2 km)	3 mi (4.8 km)	2 mi (3.2 km)
	Typical Maximum Aggregate Throughput	7.5 Mbps	15 Mbps	22.5 Mbps
	Nominal Receive Sensitivity including FEC	-89 dBm	-78 dBm	-70 dBm
	Latency	5-7 ms	5-7 ms	5-7 ms

3X operation is configured on an OFDM module's Configuration => General page using the **Dynamic Rate Adapt** drop-down list under MAC Control Parameters.

For information such as how to check link efficiencies or the status of 3X operation or how to disable 3X operation, see the PMP 400-430 and PTP 200 User Guide. These are available for download at <http://motorola.wirelessbroadbandsupport.com/software/>:

 [Download](#) PMP 400-430 and PTP 200 User Guide 1.64MB Issue 4. Includes 5.8-GHz, 4.9-GHz, and 5.4-GHz OFDM products.

7.1.14 Engineering for 2X and 3X Operation

The following priorities should guide your implementation of 2X and 3X operation:

- In the near quarter of the distance range of the AP
 - identify the customers who use the most bandwidth on OFDM SMs.
 - enable their SMs first for 3X operation.
- In the near half of the distance range of the AP
 - identify the customers who use the most bandwidth.
 - enable their SMs first for 2X operation.
- When you have deployable P7 and P8 SMs, *do not* deploy CSM 130s, CSM 09130s, or CSM 120 P9s beyond half the distance range of the AP. At this distance, steady and reliable 2X operation typically is not achievable. Deploy the P7 and P8 SMs here.
- Wherever practical, implement
 - 10 MHz of channel separation for 3X operation.
 - 25 MHz of channel separation for 2X operation.

7.2 UNDERSTANDING SYNCHRONIZATION

The system uses Time Division Duplexing (TDD) - one channel alternately transmits and receives - rather than using one channel for transmitting and a second channel for receiving. To accomplish TDD, the AP must provide sync to its SMs – it must keep them in sync. Furthermore, collocated APs must be synced together - an unsynchronized AP that transmits during the receive cycle of a collocated AP can prevent that second AP from being able to decode the signals from its SMs. In addition, across a geographical area, APs that can “hear” each other benefit from using a common sync to further reduce self-interference within the network.

7.2.1 GPS Synchronization

The Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS) uses 24 satellites to relay information for precise derivation of position and time.

The cluster management module (CMM) contains a Motorola Oncore GPS Receiver. The CMM is a critical element in the operation of the system. At one AP cluster site or throughout an entire wireless system, the CMM provides a GPS timing pulse to each module, synchronizing the network transmission cycles.

The Oncore GPS Receiver tracks eight or more satellites. The CMM uses the signal from at least four of these satellites to generate a one-second interval clock that has a rise time of 100 nsec. This clock directly synchronizes APs and BHM's which, in turn, synchronize the SMs and BHSs in the network.

The Oncore GPS Receiver also provides

- the latitude and longitude of the GPS antenna (collocated with the CMM)
- the number of satellites that are being tracked
- the number of satellites that are available
- the date
- the time in Universal Coordinated Time (UCT)
- the altitude of the GPS antenna
- other information that can be used to diagnose network problems.

Alternative to GPS Sync

A link can operate without *GPS sync*, but cannot operate without sync. The alternative to GPS sync is to configure the AP or BHM in the link to generate a sync pulse to pass to the SM or BHS, respectively. Depending on the RF environment in which the link operates, this latter alternative may or may not be plausible.

For example, in [Figure 25](#), AP4

- is not synchronized with any of the other APs.
- is transmitting nearby the other APs while they are expecting to receive SM transmissions from a maximum distance.

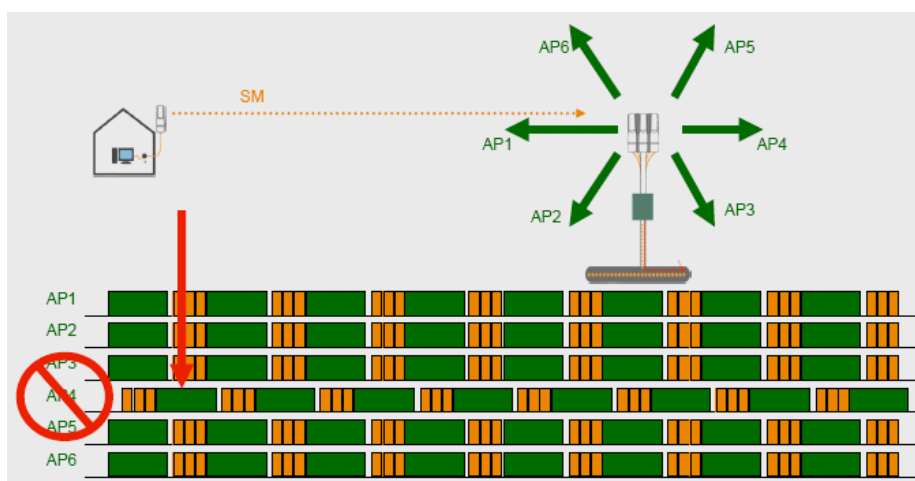


Figure 25: One unsynchronized AP in cluster

The result is self-interference. In this scenario, the self-interference can be avoided only by synchronizing the TDD transmit cycles of all APs that operate in the same frequency band.

An AP that is isolated by at least 5 miles (8 km) from any other equipment, or a BHM in an isolated standalone BH link can generate and pass sync pulse without GPS timing and not risk that interference will result from the generated sync. In any other type of link, sync should be derived from GPS timing.



NOTE:

The OFDM Series BHMs generate their own sync. For more information about these modules, see the user guides that support them. Titles are listed under [Products Not Covered by This User Guide](#) on Page 34.

Advantage of GPS Sync

Although the embedded timing generation capability of the AP and BHM keeps a precise clock, no trigger exists to start the clock at the same moment in each AP of a cluster. So, the individual AP can synchronize communications between itself and registered SMs, but cannot synchronize itself with other modules, except by GPS timing (shown in [Figure 26](#)).

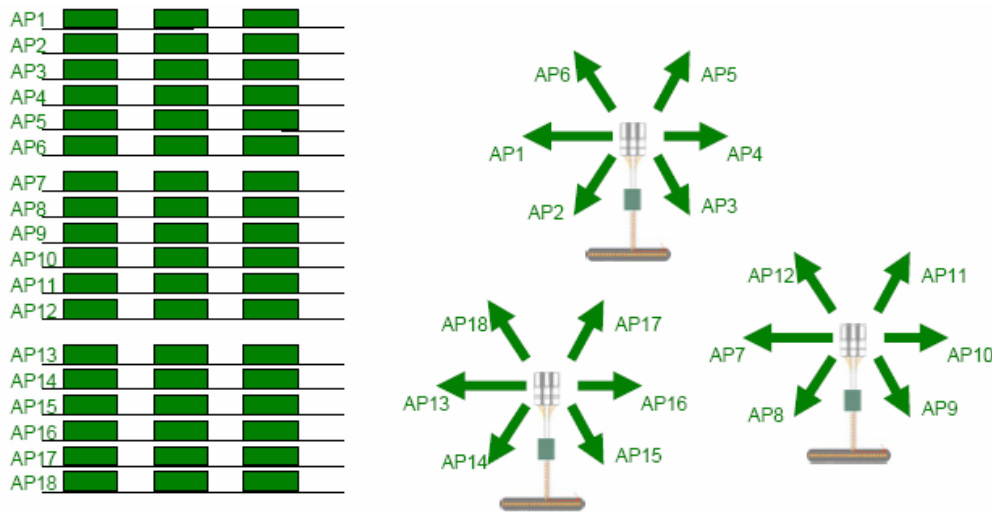


Figure 26: GPS timing throughout the network (FSK shown)

7.2.2 Passing Sync in a Single Hop

Network sync can be passed in a single hop in the following network designs:

- Design 1
 1. A CMM provides sync to a collocated AP.
 2. This AP sends the sync over the air to SMs.
- Design 2
 1. A CMM provides sync to a collocated BH timing master.
 2. This BH timing master sends the sync over the air to a BH timing slave.

7.2.3 Passing Sync in an Additional Hop

Network sync can be extended by one additional link in any of the following network designs:



NOTE:

In each of these following designs, Link 2 is *not* on the same frequency band as Link 4. (For example, Link 2 may be a 5.2-GHz link while Link 4 is a 5.7- or 2.4-GHz link.)

- Design 3
 1. A CMM provides sync to a collocated AP.
 2. This AP sends the sync over the air to an SM.
 3. This SM delivers the sync to a collocated AP.
 4. This AP passes the sync in the additional link over the air to SMs.

This design is illustrated in [Figure 27](#).

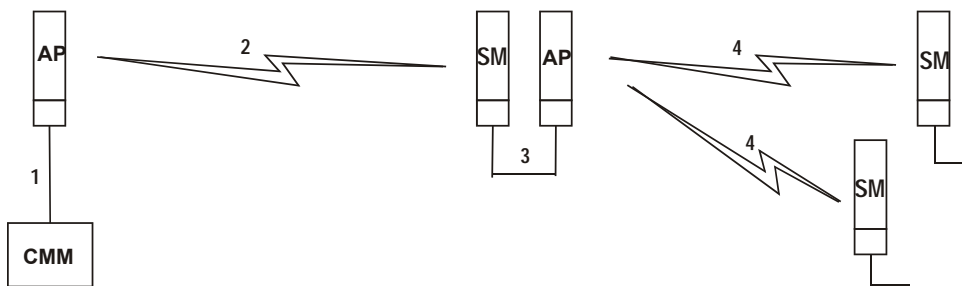


Figure 27: Additional link to extend network sync, Design 3

- Design 4
 1. A CMM provides sync to a collocated AP.
 2. This AP sends the sync over the air to an SM.
 3. This SM delivers the sync to a collocated BHM.
 4. This BHM passes the sync in the additional link over the air to a BHS.

This design is illustrated in [Figure 28](#).

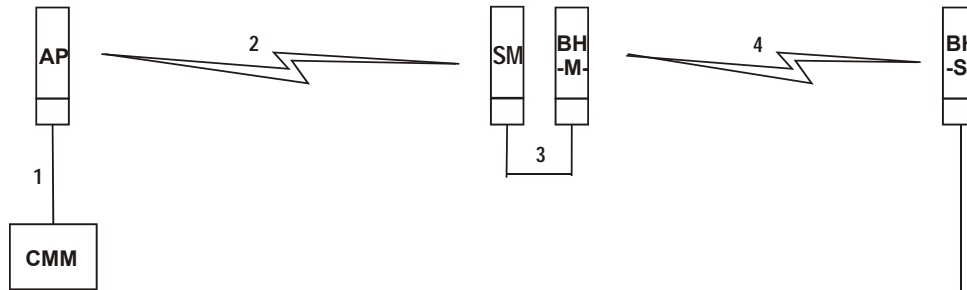


Figure 28: Additional link to extend network sync, Design 4

- Design 5
 1. A CMM provides sync to a collocated BHM or the BHM generates timing.
 2. This BHM sends the sync over the air to a BHS.
 3. This BHS delivers the sync to a collocated AP.
 4. This AP passes the sync in the additional link over the air to SMs.

This design is illustrated in [Figure 29](#).

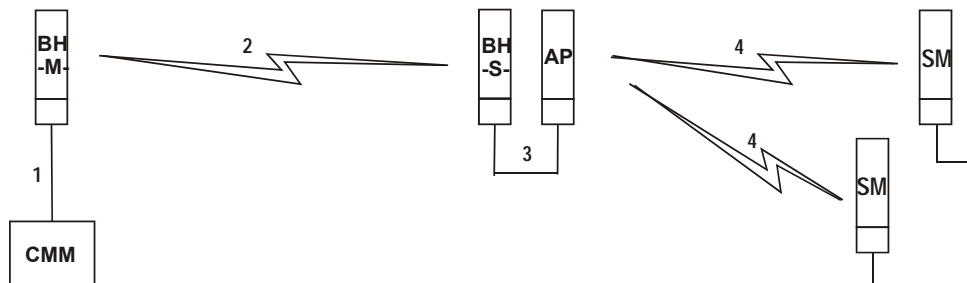


Figure 29: Additional link to extend network sync, Design 5

Wiring and configuration information for this sync extension is described under [Wiring to Extend Network Sync](#) on Page 378.

All radios support the remote AP functionality. The BHS and the SM can reliably pass the sync pulse, and the BHM and AP can reliably receive it. The sync is passed in a cable that connects Pins 1 and 6 of the RJ-11 timing ports of the two modules. (The sync cable is described under [Cables](#) on Page 63.) When you connect modules in this way, you must also adjust configuration parameters to ensure that

- the AP is set to properly receive sync.
- the SM will not propagate sync to the AP if the SM itself ceases to receive sync.

8 MEETING LINK REQUIREMENTS

8.1 AP-SM LINKS

APs communicate with SMs using a point-to-multipoint protocol. An AP-SM link has lower throughput and higher latency than a backhaul link for two reasons:

- Many endpoints are involved.
- The bandwidth request and reservation process consumes bandwidth.

In the 900-MHz frequency band range, round-trip latency is typically 15 msec. In all other frequency band ranges, round-trip latency is typically 6 msec.

At range settings of greater than 40 miles (64 km) in the 900-MHz AP, more time elapses between transmit and receive cycles to compensate for greater air delay. In each frame, this reduces the number of data slots, which slightly reduces the aggregate throughput of the link. However, the throughput is as predictable as in other point-to-multipoint links.

Throughput is a factor of the **Max Range** parameter in the AP and is effective for all SMs, regardless of their distance from the AP. Throughput includes all downlink data to all SMs and all uplink data from all SMs that link to the AP. For throughput, see [Table 15](#) on [Page 68](#).

End user perspective of throughput is based on both bandwidth in the sending direction and the return of TCP acknowledgement packets in the other. Where sufficient downlink bandwidth exists to support downlink traffic and overhead, transient traffic congestion in the uplink can cause some TCP acknowledgement packets to be dropped, and the end user to perceive a reduction in throughput. This can also occur with sufficient uplink bandwidth and dropping acknowledgment packets in the downlink.

However, a network operator can optionally enable the **Prioritize TCP ACK** parameter in the AP and BHM, giving these packets priority over other packet types. This results in fewer of them being dropped.

The effects of changing network conditions on PTMP throughput are indicated in [Table 25](#).

Table 25: Effects of network conditions on PTMP throughput

Changing Network Condition	Effect on AP Aggregate Throughput
Increasing the Max Range parameter setting ¹ in the AP	somewhat decreased ²
Increasing the number of SMs that register in the AP	no effect
Increase in downlink traffic	
Increase in uplink traffic	
Increasing the average bandwidth allotted to the SMs that register in the AP	no effect, even when the additional bandwidth is used.
<p>NOTES:</p> <ol style="list-style-type: none"> 1. For non 900-MHz APs, the AP accepts a Max Range value of up to 30 miles (48 km). See Max Range on Page 235. 2. To avoid a decrease of unnecessary proportion, set to not much further than the distance between the AP and the furthest SM that registers in the AP. 	

A comparison of SM products in link with a CAP 130 is shown in [Table 26](#).

Table 26: Comparison of SM products with CAP 130

Product	Maximum Sustained Aggregate Throughput to a Single SM	Burst	Cap on Committed Information Rate	Upgradability	VoIP Channels Supported
CSM 130	14 Mbps	14 Mb	none	none	multiple
PMP 400 Series SM	21 Mbps	21 Mb	none	none	multiple
CSM 120	7 Mbps	14 Mb	none	to CSM 130 capabilities	multiple
CSM 110 Lite SM as purchased	512 kbps	768 kb	100 kbps	to 1, 2, 4, or 7 Mbps	1
CSM 110 Lite SM upgraded to 1 Mbps	1 Mbps	1.5 Mb	100 kbps	none	1
CSM 110 Lite SM upgraded to 2 Mbps	2 Mbps	3 Mb	100 kbps	none	1
CSM 110 Lite SM upgraded to 4 Mbps	4 Mbps	7 Mb	200 kbps	none	2
CSM 110 Lite SM upgraded to 7 Mbps	7 Mbps	7 Mb	200 kbps	none	2

8.2 BH-BH LINKS

Motorola PTP Bridges communicate with each other using a point-to-point protocol. This point-to-point protocol uses a 2.5-msec frame. A BH link has higher throughput and lower latency (typically 5 msec, 2.5 msec in each direction) for two reasons:

- Only two endpoints are involved.
- No bandwidth request and reservation process is involved.

For 10-Mbps BHs, the aggregate throughput on the channel is 7.5 Mbps. For 20-Mbps BHs, the aggregate throughput on the channel is 14 Mbps. If a BH is set to a downlink ratio of 50%, then the bandwidth in each direction is half of the total BH link bandwidth.

9 PREVIEWING NETWORK CONFIGURATIONS

The following are examples of network layouts. Customer experience case studies are also available.

9.1 VIEWING TYPICAL LAYOUTS

The following layouts are typical of system implementations:

- [Figure 30: Typical network layout with no BH](#)
- [Figure 31: Typical network layout with BH](#)
- [Figure 32: Typical multiple-BH network layout](#)

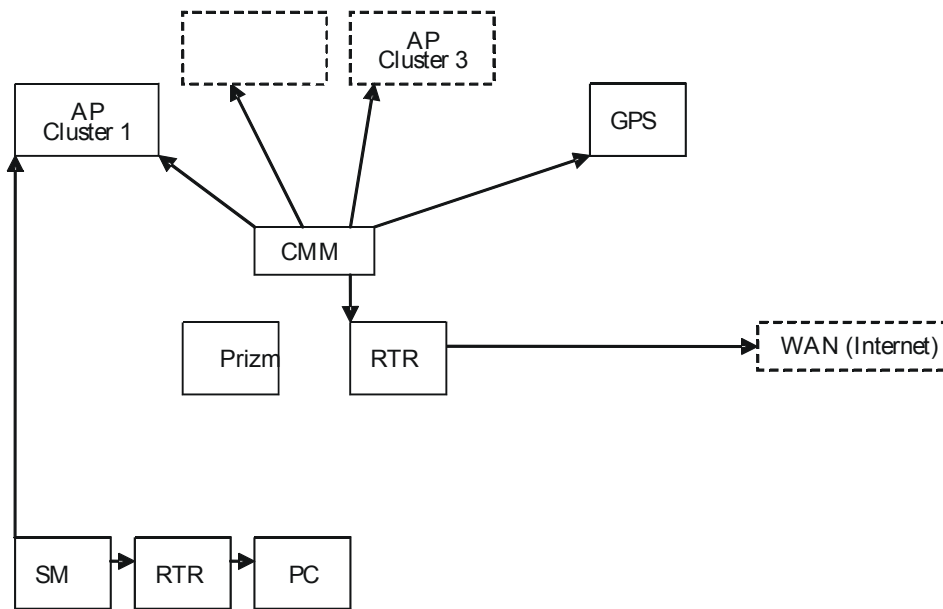


Figure 30: Typical network layout with no BH

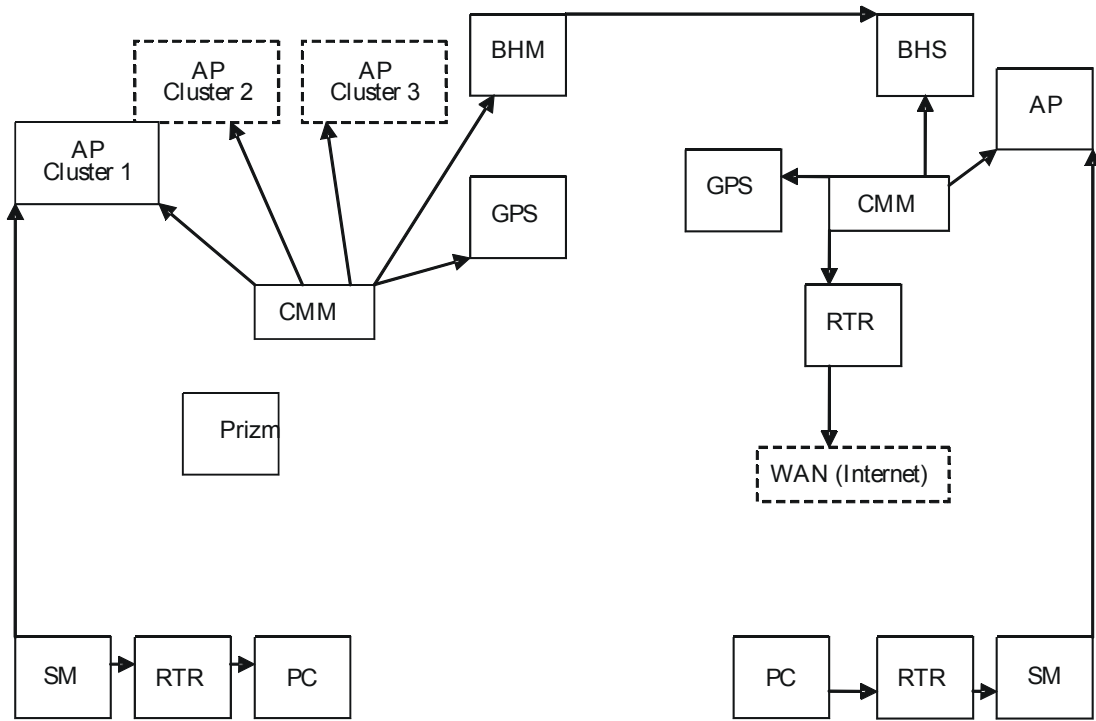


Figure 31: Typical network layout with BH

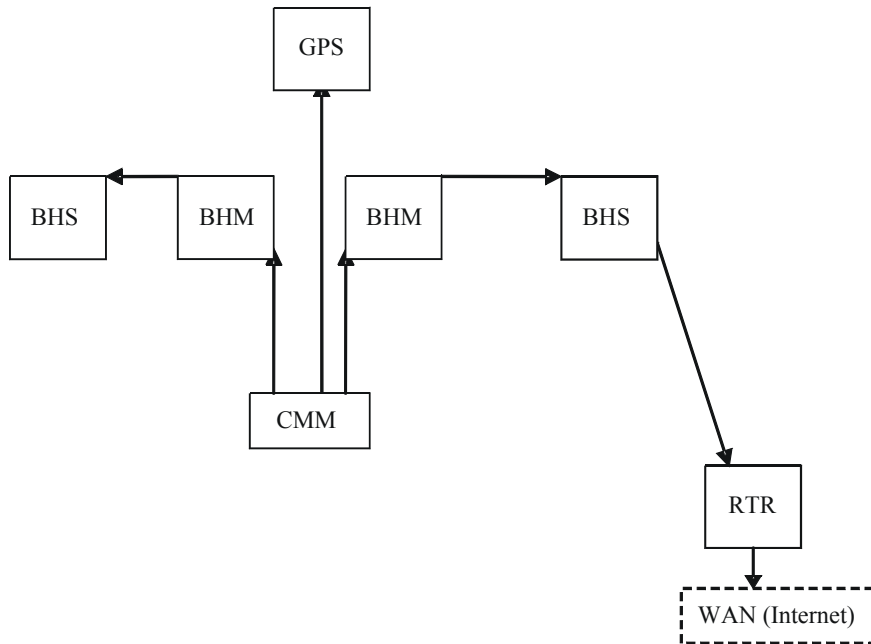


Figure 32: Typical multiple-BH network layout

9.2 VIEWING CASE STUDIES

Case studies of implementations are available as “Feature Articles” for download from <http://www.connectwithcanopy.com/index.cfm?canopy=menu.case>.

10 ACCESSING FEATURES

PMP 100 and 400 and PTP 100 and 200 Series radios support the features that are indicated in [Table 27](#).

Table 27: List of features

Regulatory Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
RoHS compliant (EU “green” mandate)	All modules	no	no
WEEE compliant	All modules	no	no
Complies with Human RF exposure limits (ETSI)	All radios	no	no
Radio Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Time Division Duplex	All radios	no	no
Scalable up to 6 sectors per cell.	AP SM	no	no
200 registered subscribers supported per AP	AP SM	no	no
Fixed/nomadic operation	All radios	no	no
7 ms or less round trip latency (OTA under normal conditions)	All radios	no	no
Transmit frame spreading for geographical area co-existence	AP BHM	Configuration/Radio	yes
Radio statistics (scheduler)	All radios	Statistics/Scheduler	yes
2X rate, enabled per link (requires CAP 130, CAP 09130, or 20 Mbps BH)	SM BHS	Configuration/General	yes
2X rate, enabled per sector (requires CAP 130, CAP 09130, or 20 Mbps BH)	AP BHM	Configuration/General	yes
Manual transmit power control - normal and low (-18 dB)	All radios	Configuration/Radio	yes
Manual transmit power control, 1 dB increments over 25 dB at the AP	AP BHM	Configuration/Radio	yes
6,200 packets per second on P10 or P11 firmware (6,300 in PMP 400 Series modules without VLAN enabled; 5,300 with VLAN enabled; 6,200 in PTP 100 Series wireless Ethernet bridges at 2- and 4-Mbps throughput; 4,600 in CAP 09130 and CSM 09130)	All radios	no	no
Settable downlink broadcast repeat count	AP	Configuration/Radio	yes

RF Configuration Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Configurable center-channel carrier frequency	AP BHM	Configuration/Radio	yes
255 configurable "color codes" to manage SM to AP (or (BHS to BHM) registration	All radios	Configuration/Radio	yes
16 configurable "sector IDs" for administrative convenience	AP BHM	Configuration/Radio	yes
Configurable range settings (determines air turn-around time)	AP	Configuration/Radio	yes
Configurable downlink data % (determines transmit/receive ratio)	AP BHM	Configuration/Radio	yes
Configurable number of reserved control slots (manages contention for uplink requests)	AP	Configuration/Radio	yes
Configurable frequency scan list at SM	SM BHS	Configuration/Radio	yes
Packet stats - RF interface	All radios	Statistics/Radio	yes
Timing Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Configurable AP/BHM sync source - Sync over Power over Ethernet, self-sync, or sync cable	AP BHM	Configuration/General	yes
"Remote AP" support, including timing pulse propagation through SM/BHS	SM BHS	Configuration/General	yes
Ethernet Interface Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Selectable link speeds - 10/100 Base T, half, full-duplex	All modules	Configuration/General	yes
Ethernet link auto-negotiation	All modules	Configuration/General	no
Accepts straight-through or crossover Ethernet cable wiring (Auto-MDX)	All modules	no	no
Wire line Interface: Ethernet cable with proprietary PoE	All modules	no	no
Disable SM Ethernet link	SM	Configuration/General	yes
Packet stats - Ethernet interface	All radios	Statistics/Ethernet	yes

IP Interface Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Configurable LAN settings (IP address, mask, gateway)	All radios	Configuration/IP	yes
Module's management IP address assignable via DHCP	All radios	Configuration/IP	yes
Private LAN to support AP to SM (or BHM to BHS) communications	All radios	Configuration/IP	yes
Configurable SM mgmt accessibility (Local/Ethernet only, or Public/RF and Local/Ethernet)	SM	Configuration/IP	yes
Security Features (Authentication, Encryption, and Access Control)	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Configurable SM authentication using BAM/PrizmEMS	AP SM	Configuration/Security	yes
Configurable BH authentication, standalone	BHM BHS	Configuration/Security	no
DES encryption on standard product	All radios	no	yes
AES encryption on AES product	All radios	no	yes
Configurable whether SM/BHS displays AP/BHM beacon information	AP BHM	Configuration/Security	yes
Configurable web, telnet, and ftp session timeout	All radios	Configuration/Security	yes
Configurable access to radio management - up to 3 source IP addresses	All radios	Configuration/Security	yes
User/account names (up to 4) and passwords on modules	All radios	Account	yes
Permission levels control ability to add/delete users/passwords	All radios	Account	yes
Override plug to override lost IP address or user/password	All radios	no	no
Override plug configurable as a default plug - reset to factory defaults	AP SM BHM BHS	Configuration/Unit Settings	yes
Override switch to override lost IP address or user/password on CMM	CMMmicro CMM4	no	no
Capability to disable refresh of the encryption key every 24 hours	BHM	Configuration/Security	yes
Read only community string configurable	AP	Configuration/SNMP	yes

Monitoring Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
List of registered SMs/BHSs with full data, with hot links to SMs/BHSs	AP BHM	Configuration/General	multiple objects
Abbreviated list of SMs/BHSs, with hot links to SMs/BHSs	AP BHM	Configuration/General	multiple objects
Received power level indication	All radios	Home/Session Status (in master)	yes
LEDs on modules to display states and activity	All modules	no	no
Received interference level indication (jitter)	All radios	Configuration/General	yes
Configurable web-page auto-refresh	All modules	Configuration/General	yes
SM registration failures	AP BHM	Statistics/Reg Failures	yes
Event log	All modules	Home/Event Log	no
Operator can use own logo on GUI pages	All modules	no	yes
Operator can use own style sheets for GUI	All modules	no	yes
Jitter consistent regardless of operation (1X or 2X)	All radios	no	no
Link status table with bidirectional data for all links	AP	Tools/Link Status	no
Point-to-Point Protocol over Ethernet (PPPoE) client	SM	Configuration/PPPoE	yes
Maximum number of SMs registered since last reboot displayed	AP	Home/General Status	no
Per-SM query (instead of Link Status table)	AP	Tools/Link Status	no
Bridge Management Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Configurable bridge entry timeout	All radios	Configuration/General	yes
Bridging table statistics (up to 4096 entries)	All radios	Statistics/Bridging Table	yes
Disable bridging on BHs	BHM BHS	Configuration/General	yes
SM Isolation Features (preventing communication between SMs)	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
SM isolation at AP	AP	Configuration/General	yes
SM isolation at CMM	CMMmicro CMM4	Configuration/General	yes
SM Isolation Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Translation bridging (replace customer MAC with SM MAC address)	AP	Configuration/General	yes
With Translation bridging, choice of sending untranslated ARP	AP	Configuration/General	yes
Translation table statistics	All radios	Statistics/Translation Table	yes

Quick Start Feature	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
AP configuration quick-start wizard	AP BHM	Quick Start	
Bandwidth Management Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
AP Maximum Information Rate (MIR) default settings	AP	Configuration/QoS	yes
Per SM Maximum Information Rate (MIR)	SM	Configuration/QoS	yes
Per SM Committed Information Rate (CIR) for high and low channels	SM	Configuration/QoS	yes
"Configuration Source" for MIR/CIR/HP/VLAN can be either SM or BAM/Prizm	AP	Configuration/General	yes
CIR for low priority channel on BH	BHS	Configuration/QoS	yes
Configurable priority for TCP Acks, to optimize bandwidth use	AP BHM	Configuration/General	yes
Settable broadcast downlink CIR	AP	Configuration/QoS	yes
Bandwidth Management Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Configurable High Priority channel with configurable DiffServ mappings on AP, SM (2 classes of service)	AP SM	Configuration/DiffServe	yes
Permanent BH High Priority Channel with configurable DiffServ mappings on BH (2 classes of service)	BHM BHS	Configuration/DiffServe	yes
Virtual channel (high/low priority) statistics	All radios	Statistics/Data VC	yes
Network Address Translation (NAT) Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
NAT	SM	Configuration/NAT	yes
NAT DMZ	SM	Configuration/NAT	yes
NAT DHCP server on LAN with up to 254 IP addresses in pool	SM	Configuration/NAT	yes
NAT DHCP client on WAN (obtains NAT address from a DHCP server)	SM	Configuration/NAT	yes
NAT port mapping	SM	Configuration/NAT	yes
VPN "pass through" for L2TP over IPSec (but not PPTP)	SM	no	no
NAT statistics	SM	Statistics/NAT Stats	yes
NAT DHCP statistics	SM	Statistics/NAT DHCP Statistics	yes
NAT table	SM	Logs/NAT Table	no

Filtering Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Protocol filtering based on protocol	SM	Configuration/Protocol Filtering	yes
Operator-defined port filtering (3 ports)	SM	Configuration/Protocol Filtering	yes
Packet filter statistics	All radios	Statistics/Filter	yes
VLAN Management Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Configurable VLAN	AP SM CMMmicro CMM4	Configuration/VLAN	yes
Highly configurable VLAN (802.1Q)	AP SM	Configuration/VLAN	yes
Use of VLAN priorities (802.1p) with high priority channel	AP SM	no	yes
Port-based VLAN switching on CMM	CMMmicro CMM4	Configuration	yes
VLAN statistics	AP SM	Statistics/VLAN	yes
Dynamic Frequency Selection (DFS) Feature	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
DFS v1.2.3	All radios	no	yes
DFS v1.3.1	All radios	no	yes
DFS v1.4.1	All radios	no	yes
Time Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Time and Date from CMM via Network Time Protocol (NTP) server	AP BHM	Configuration/Time	yes
Time and Date manually settable	AP BHM	Configuration/Time	yes
CMM provides NTP server	CMMmicro CMM4	no	no
Spectrum Analyzer Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Spectrum analyzer	SM BHS	Tools/Spectrum Analyzer	no
Ability to switch an AP to an SM (or BHS to BHM)	AP BHM	Configuration/General	yes
Remote Spectrum Analysis	AP	Tools/Remote Spectrum Analyzer	no

Aim/Link Quality Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Alignment tone for using during aiming/alignment	SM BHS	no	no
Aiming support page when not using alignment tone	SM BHS	Tools/Alignment	multiple objects
LED for alignment	SM BHS	no	no
Configure SM power-up state - aiming or operational	SM BHS	Configuration/General	yes
Link capacity test, with configurable packet length	All radios	Tools/Link Capacity Test	yes
Display of SM configuration information at AP	AP BHM	Home/Session Status	yes
Display/evaluation of AP beacon data from all receivable APs	SM BHS	Tools/AP Evaluation	yes
Over-the-air radio Bit Error Rate (BER) indicator	All radios	Tools/BER Results	yes
Graphical alignment tool with near-real time jitter and received power level	SM	Tools/Alignment Tool	no
Optional selection of Revised or Legacy LED indicator scheme	SM	Configuration/Unit Settings	no
Frame Tool Feature	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Frame calculator for supporting collocation	All radios	Tools/Frame Calculator	no
Personal Digital Assistant (PDA) Interface Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
GUI automatically sized/styled for PDA when displayed on a PDA	All radios	all	no
Spectrum analyzer display for PDA	All radios	PDA/Spectrum Results (PDA)	no
Specific pages for PDA display	All radios	PDA	no
SNMP Interface Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Support of SNMP v2	All modules	no	no
Canopy Enterprise MIB	All modules	no	no
Configurable SNMP community string	All radios	Configuration/SNMP	yes
Configurable SNMP accessing subnet	All radios	Configuration/SNMP	yes
10 configurable SNMP trap addresses	All radios	Configuration/SNMP	yes
Configurable traps (sync and session)	All radios	Configuration/SNMP	yes
Configurable SNMP permissions (read, read/write)	All radios	Configuration/SNMP	yes
Configurable site information, including site name	All modules	Configuration/SNMP	yes

Upgrade Process Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
Upgrading using CNUT and SM Auto-update for SMs	All modules	no	no
Configurable update address to support distributed software upgrades	AP	Configuration/General	yes
AP Cluster Management Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
CMM port power control	CMMmicro CMM4	Configuration	yes
CMM port reset	CMMmicro CMM4	Configuration	yes
CMM: Sufficient ports for at least 4 AP, 2 BH, plus management	CMMmicro CMM4	no	no
CMM: Sufficient power for at least 4 AP plus 2 BH	CMMmicro CMM4	no	no
Powered from 90-264 VAC, 50/60 Hz; 55 V DC power output	AP BH	no	no
Physical Features	Module Type(s)	Controlled in GUI Page/Tab	SNMP Control
MTBF > 45 years (~400 000 hours)	All modules	no	no
neg 40 C to + 55 C (Ambient) operation	All modules	no	no
Temperature indication	All radios	Home/General	no
Non-condensing (Indoor/outdoor), weather protected form factor/packaging	All modules	no	no
Element Management System (Prizm) Features			
Current Prizm to manage all elements of the system (including Mot Backhaul)			
Up to 1000 APs, plus 100 devices/AP); minimal storage / minimal polling			
Redundant configuration for additional storage/reporting capability			
Commercial Off the Shelf (COTS) Platform and OS support (e.g. Intel, Linux, Windows)			
COTS Database support (e.g. MySQL, PostgreSQL, MS SQL Server, etc.); Oracle optional			

10.1 ACTIVATING FEATURES

A feature is *active* if the software that allows the feature to be turned on or off (enabled or disabled) is present.

10.1.1 Fixed License Keys

Some features are activated by loading a fixed license key into the radio. Such a key arrives from Motorola as a *filename.url* file. When you double-click on this file, your browser opens and the location bar is populated by a lengthy string. This URL string begins with `http://<ModuleIPAddress>/`. If you need to load a key into a module whose IP address has changed since Motorola issued the key, perform the following steps.

Procedure 1: Modifying a fixed license key for a module IP address

4. Right-click on the license key filename.
5. Select **Properties**.
6. Select the **Web Document** tab.
7. At **URL**, substitute the current IP address for the original IP address in the URL.
8. Click **OK**.
9. Double-click on the license key filename.
RESULT: The key loads into the module.
10. Open the Configuration web page of the module.
11. Review parameter settings and enable the feature if you wish to do so at this time (see next section).

===== end of procedure =====

10.2 ENABLING FEATURES

A feature is *enabled* (functioning) if the feature is both active and enabled. For example, Transmit Frame Spreading is active (*can be enabled*) in any AP or BHM, except 900-MHz radios. However, Transmit Frame Spreading functions only if the **Enable** selection for the **Transmit Frame Spreading** parameter is checked in the Radio tab of the Configuration web page in the module.

11 ACQUIRING PROFICIENCIES

Designing and operating a network requires fundamental knowledge of radio frequency transmission and reception, Internet Protocol addressing schemes, experimentation with equipment, and for most operators participation in some forms of product training.

11.1 UNDERSTANDING RF FUNDAMENTALS

Product training and user interfaces presume an understanding of RF fundamentals. Excellent written sources for these fundamentals are available. One such source is *Deploying License-Free Wireless Wide-Area Networks* by Jack Unger (ISBN 1-58705-069-2), published by Cisco Press.

11.2 UNDERSTANDING IP FUNDAMENTALS

Product training and user interfaces also presume an understanding of Internet Protocol (IP) fundamentals. Excellent written sources for these fundamentals are available. One such source is *Sams Teach Yourself TCP/IP in 24 Hours* by Joe Casad (ISBN 0-672-32085-1), published by Sams Publishing.



NOTE:

The default IP address of each component is 169.254.1.1.

11.3 ACQUIRING A DEMONSTRATION KIT

Demonstration Kits are available through your Motorola representative.

11.3.1 900-MHz with Integrated Antenna and Band-pass Filter Demonstration Kit

Each 900-MHz with integrated antenna and band-pass filter Demonstration Kit contains

- 2 9000SM SMs
- 1 9000APF AP
- 1 600SS Surge Suppressor
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in [Table 28](#).

11.3.2 900-MHz with Connectorized Antenna Demonstration Kit

Each 900-MHz with connectorized (external) antenna Demonstration Kit contains

- 2 9000SMC CSM 09130s
- 1 9000APC CAP 09130
- 3 AN900 60° 9-dBi Antennas
- 1 600SS Surge Suppressor
- 1 SMMB2 Universal Heavy Duty Mounting Bracket
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in [Table 28](#).

11.3.3 2.4-GHz with Adjustable Power Set to High Demonstration Kit

Each 2.4-GHz with adjustable power set to high Demonstration Kit contains

- 1 2400SM SM
- 1 2450SM CSM 130
- 1 2450AP CAP 130
- 1 600SS Surge Suppressor
- 1 SMMB1 Universal Mounting Bracket
- 3 ACPSSW-02 90- to 230-V AC 50- to 60-Hz Power Supplies
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in [Table 28](#).

11.3.4 5.2-GHz Demonstration Kit

Each 5.2-GHz Demonstration Kit contains

- 1 5200SM SM
- 1 5250SM CSM 130
- 1 5250AP CAP 130
- 1 600SS Surge Suppressor
- 1 SMMB1 Universal Mounting Bracket
- 3 ACPSSW-02 90- to 230-V AC 50- to 60-Hz Power Supplies
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in [Table 28](#).

11.3.5 5.4-GHz Demonstration Kit

Each 5.4-GHz Demonstration Kit contains

- 1 5400SM SM
- 1 5450SM CSM 130
- 1 5450AP CAP 130
- 1 600SS Surge Suppressor
- 1 SMMB1 Universal Mounting Bracket
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 Cross-over Category 5 Cable
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in [Table 28](#).

11.3.6 5.7-GHz with Connectorized Antenna and Adjustable Power Set to Low Demonstration Kit

Each 5.7-GHz with connectorized antenna and adjustable power set to low Demonstration Kit contains

- 1 5700SMC SM
- 1 5750SMC CSM 130
- 1 5750APC CAP 130
- 1 600SS Surge Suppressor
- 1 SMMB2 Universal Heavy Duty Mounting Bracket
- 3 ACPSSW-02 90- to 230-V AC 50- to 60-Hz Power Supplies
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 Cross-over Category 5 Cable
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD03EN Technical Overview on CD
- 1 User Guide on CD

Part numbers for Demonstration Kits are provided in [Table 28](#).

11.3.7 Demonstration Kit Part Numbers

The part numbers for ordering demonstration kits are provided in [Table 28](#).

Table 28: Demonstration Kit part numbers

Frequency Band Range and Feature	Current Part Number	Previous Part Number
900 MHz integrated antenna with band-pass filter	HK1267B	TK10290
900 MHz connectorized antenna	HK1244B	TK10290C
2.4 GHz adjustable power set to low		TK10250
2.4 GHz adjustable power set to high	HK1135B	TK10251
5.2 GHz	HK1133B	TK10252
5.4 GHz	HK1282A	TK10254
5.7 GHz		TK10257
5.7 GHz connectorized adjustable power set to low	HK1132B	TK10257C

11.4 ACQUIRING A STARTER KIT

Starter Kits are also available through your Motorola representative.

11.4.1 900-MHz with Integrated Antenna and Band-pass Filter Starter Kit

Each 900-MHz with integrated antenna and band-pass filters Starter Kit contains

- 20 9000SM CSM 09130s
- 3 9000APF CAP 09130s
- 1 1070CK CMMmicro
- 21 600SS Surge Suppressors
- 1 User Guide on CD

Power supplies and SM mounting brackets *are not* included in this kit. Part numbers for Starter Kits are provided in [Table 29](#).

11.4.2 900-MHz with Connectorized Antenna Starter Kit

Each 900-MHz with connectorized (external) antenna Starter Kit contains

- 20 9000SMC CSM 09130s
- 3 9000APC CAP 09130s
- 1 1070CK CMMmicro
- 21 600SS Surge Suppressors
- 20 SMMB2 Universal Heavy Duty Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in [Table 29](#).

11.4.3 2.4-GHz with Adjustable Power Set to High Starter Kit

Each 2.4-GHz adjustable power set to high Starter Kit contains

- 30 2400SM CSM 120s
- 6 2450AP CAP 130s
- 1 1070CK CMMmicro
- 31 600SS Surge Suppressors
- 30 SMMB1 Universal Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in [Table 29](#).

11.4.4 5.2-GHz Starter Kit

Each 5.2-GHz Starter Kit contains

- 30 5200SM CSM 120s
- 6 5250AP CAP 130s
- 1 1070CK CMMmicro
- 31 600SS Surge Suppressors
- 30 SMMB1 Universal Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in [Table 29](#).

11.4.5 5.4-GHz FSK Starter Kit

Each 5.4-GHz Starter Kit contains

- 30 5400SM CSM 120s
- 6 5450AP CAP 130s
- 1 1070CK CMMmicro
- 31 600SS Surge Suppressors
- 30 SMMB1 Universal Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in [Table 29](#).

11.4.6 5.4-GHz OFDM Starter Kits

Starter kits for PMP 54400 series network equipment are available in three sizes. Each HK1820A Starter Kit contains

- 2 5440 SMs
- 1 5440 AP
- 3 ACPSSW-13B Power Supplies
- 3 600SS Surge Suppressors
- 2 SMMB2A Mounting Brackets

Each HK1819A Starter Kit contains

- 5 5440 SMs
- 2 5440 APs
- 6 ACPSSW-13B Power Supplies
- 6 600SS Surge Suppressors
- 5 SMMB2A Mounting Brackets

Each HK1818A Starter Kit contains

- 20 5440 SMs
- 2 5440 APs
- 20 ACPSSW-13B Power Supplies
- 22 600SS Surge Suppressors
- 20 SMMB2A Mounting Brackets

Part numbers for Starter Kits are provided in [Table 29](#).

11.4.7 5.7-GHz with Integrated Antenna Starter Kit

Each 5.7-GHz with integrated antenna Starter Kit contains

- 30 5700SM CSM 120s
- 6 5750AP CAP 130s
- 1 1070CK CMMmicro
- 31 600SS Surge Suppressors
- 30 SMMB1 Universal Mounting Brackets
- 1 User Guide on CD

Power supplies *are not* included in this kit. Part numbers for Starter Kits are provided in [Table 29](#).

11.4.8 Starter Kit Part Numbers

The part numbers for ordering Starter kits are provided in [Table 29](#).

Table 29: Starter Kit part numbers

Frequency Band Range	Current Part Number	Previous Part Number
900 MHz integrated antenna with band-pass filter	HK1266B	TK10190
900 MHz connectorized	HK1243B	TK10190C
2.4 GHz adjustable power set to low		TK10150
2.4 GHz adjustable power set to high	HK1139B	TK10151
5.2 GHz	HK1140B	TK10152
5.4 GHz FSK	HK1283A	TK10154
5.4 GHz OFDM	HK1118A	
	HK1119A	
	HK1120A	
5.7 GHz	HK1141B	TK10157
5.7 GHz connectorized adjustable power set to low		TK10157C

11.5 EVALUATING TRAINING OPTIONS

Motorola and its distributors make technical training available to customers. For information on this training, either

- send email inquiries to training@canopywireless.com.
- visit <http://motorola.wirelessbroadbandsupport.com/support>. Click the **Canopy Training** link.

11.6 ATTENDING ON-LINE KNOWLEDGE SESSIONS

Irregularly but often, Motorola presents a knowledge session over the Internet about a new product offering. Some of these knowledge sessions provide the opportunity for participants to interact in real time with the leader of the session.

The knowledge session

- provides a high-level understanding of the technology that the new product introduces.
- announces any subtleties and caveats.
- typically includes a demonstration of the product.
- is usually recorded for later viewing by those who could not attend in real time.

To participate in upcoming knowledge sessions, ask your Motorola representative to ensure that you receive email notifications.

PLANNING GUIDE

12 ENGINEERING YOUR RF COMMUNICATIONS

Before diagramming network layouts, the wise course is to

- anticipate the correct amount of signal loss for your fade margin calculation (as defined below).
- recognize all permanent and transient RF signals in the environment.
- identify obstructions to line of sight reception.

12.1 ANTICIPATING RF SIGNAL LOSS

The C/I (Carrier-to-Interference) ratio defines the strength of the intended signal relative to the collective strength of all other signals. Standard modules typically do not require a C/I ratio greater than

- 3 dB or less at 10-Mbps modulation and -65 dBm for 1X operation. The C/I ratio that you achieve must be even greater as the received power approaches the nominal sensitivity (-85 dBm for 1X operation).
- 10 dB or less at 10-Mbps modulation and -65 dBm for 2X operation. The C/I ratio that you achieve must be even greater as the received power approaches the nominal sensitivity (-79 dBm for 2X operation).
- 10 dB or less at 20-Mbps modulation.

Nominal receive sensitivity in PMP 400 Series modules is as follows:

- -89 dBm for 1X operation
- -78 dBm for 2X operation
- -70 dBm for 3X operation

12.1.1 Understanding Attenuation

An RF signal in space is attenuated by atmospheric and other effects as a function of the distance from the initial transmission point. The further a reception point is placed from the transmission point, the weaker is the received RF signal.

12.1.2 Calculating Free Space Path Loss

The attenuation that distance imposes on a signal is the free space path loss. [PathLossCalcPage.xls](#) calculates free space path loss.

12.1.3 Calculating Rx Signal Level

The Rx sensitivity of each module is provided at http://motorola.canopywireless.com/prod_specs.php. The determinants in Rx signal level are illustrated in [Figure 33](#).

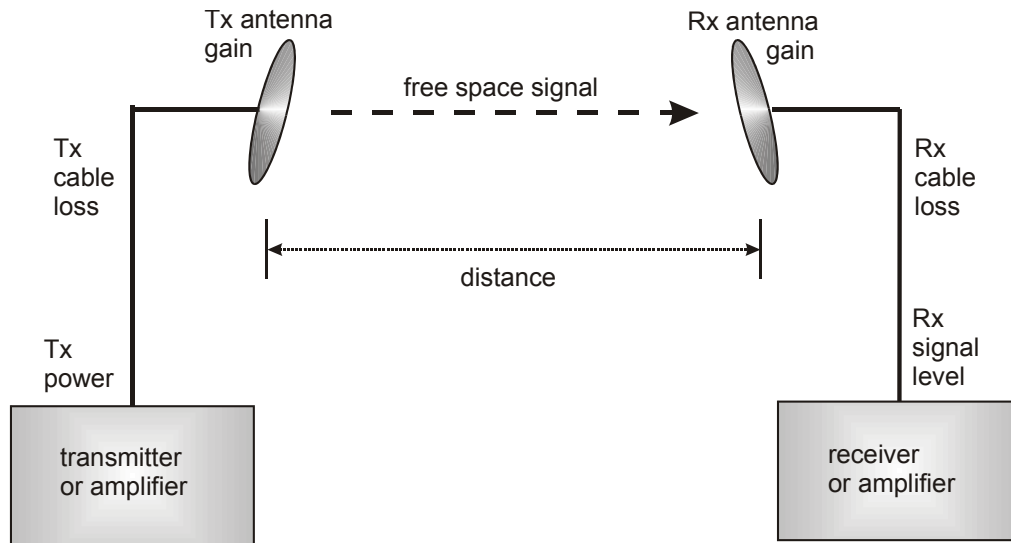


Figure 33: Determinants in Rx signal level

Rx signal level is calculated as follows:

$$\text{Rx signal level dB} = \text{Tx power} - \text{Tx cable loss} + \text{Tx antenna gain} - \text{free space path loss} + \text{Rx antenna gain} - \text{Rx cable loss}$$



NOTE:

This Rx signal level calculation presumes that a clear line of sight is established between the transmitter and receiver and that no objects encroach in the Fresnel zone.

12.1.4 Calculating Fade Margin

Free space path loss is a major determinant in Rx (received) signal level. Rx signal level, in turn, is a major factor in the system operating margin (fade margin), which is calculated as follows:

$$\text{system operating margin (fade margin) dB} = \text{Rx signal level dB} - \text{Rx sensitivity dB}$$

Thus, fade margin is the difference between strength of the received signal and the strength that the receiver requires for maintaining a reliable link. A higher fade margin is characteristic of a more reliable link.

12.2 ANALYZING THE RF ENVIRONMENT

An essential element in RF network planning is the analysis of spectrum usage and the strength of the signals that occupy the spectrum you are planning to use. Regardless of how you measure and log or chart the results you find (through the Spectrum Analyzer in SM and BHS feature or by using a spectrum analyzer), you should do so

- at various times of day.
- on various days of the week.
- periodically into the future.

As new RF neighbors move in or consumer devices in your spectrum proliferate, this will keep you aware of the dynamic possibilities for interference with your network.

12.2.1 Mapping RF Neighbor Frequencies

These modules allow you to

- use an SM or BHS (or a BHM reset to a BHS), or an AP that is temporarily transformed into an SM, as a spectrum analyzer.
- view a graphical display that shows power level in RSSI and dBm at 5-MHz increments throughout the frequency band range, regardless of limited selections in the **Custom Radio Frequency Scan Selection List** parameter of the SM.
- select an AP channel that minimizes interference from other RF equipment.

The SM measures only the spectrum of its manufacture. So if, for example, you wish to analyze an area for both 2.4- and 5.7-GHz activity, take both a 2.4- and 5.7-GHz SM to the area. To enable this functionality, perform the following steps:



CAUTION!

The following procedure causes the SM to drop any active RF link. If a link is dropped when the spectrum analysis begins, the link can be re-established when either a 15-minute interval has elapsed or the spectrum analyzer feature is disabled.


Procedure 2: Analyzing the spectrum

1. Predetermine a power source and interface that will work for the SM or BHS in the area you want to analyze.
2. Take the SM or BHS, power source, and interface device to the area.
3. Access the Tools web page of the SM or BHS.
RESULT: The Tools page opens to its Spectrum Analyzer tab. An example of this tab is shown in [Figure 147](#).
4. Click **Enable**.
RESULT: The feature is enabled.
5. Click **Enable** again.
RESULT: The system measures RSSI and dBm for each frequency in the spectrum.

6. Travel to another location in the area.
7. Click **Enable** again.
RESULT: The system provides a new measurement of RSSI and dBm for each frequency in the spectrum.
NOTE: Spectrum analysis mode times out 15 minutes after the mode was invoked.
8. Repeat Steps 6 and 7 until the area has been adequately scanned and logged.

===== **end of procedure** =====

As with any other data that pertains to your business, a decision today to put the data into a retrievable database may grow in value to you over time.



RECOMMENDATION:
 Wherever you find the measured noise level is greater than the sensitivity of the radio that you plan to deploy, use the noise level (rather than the link budget) for your link feasibility calculations.

12.2.2 Anticipating Reflection of Radio Waves

In the signal path, any object that is larger than the wavelength of the signal can reflect the signal. Such an object can even be the surface of the earth or of a river, bay, or lake. The wavelength of the signal is approximately

- 2 inches for 5.2- and 5.7-GHz signals.
- 5 inches for 2.4-GHz signals.
- 12 inches for 900-MHz signals.

A reflected signal can arrive at the antenna of the receiver later than the non-reflected signal arrives. These two or more signals cause the condition known as multipath. When multipath occurs, the reflected signal cancels part of the effect of the non-reflected signal so, overall, attenuation beyond that caused by link distance occurs. This is problematic at the margin of the link budget, where the standard operating margin (fade margin) may be compromised.

12.2.3 Noting Possible Obstructions in the Fresnel Zone

The Fresnel (pronounced *fre-NEL*) Zone is a theoretical three-dimensional area around the line of sight of an antenna transmission. Objects that penetrate this area can cause the received strength of the transmitted signal to fade. Out-of-phase reflections and absorption of the signal result in signal cancellation.

The foliage of trees and plants in the Fresnel Zone can cause signal loss. Seasonal density, moisture content of the foliage, and other factors such as wind may change the amount of loss. Plan to perform frequent and regular link tests if you must transmit through foliage.

12.2.4 Radar Signature Detection and Shutdown

With Release 8.1, Motorola met *ETSI EN 301 893 v1.2.3* for Dynamic Frequency Selection (DFS) in slave as well as master radios. DFS is a requirement in certain countries and regions for systems to detect interference from other systems, notably radar systems, and to avoid co-channel operation with these systems. With Release 8.1, all 5.7-GHz connectorized modules and all 5.4-GHz modules were ETSI DFS capable. These two products were sold only outside the U.S.A. and Canada. No other products had a DFS option.

The Configuration => Radio web page in Release 8.1 allowed the operator to enable or disable DFS. Operators in countries with regulatory requirements for DFS *must not* disable the feature and *must* ensure that it is enabled after a module is reset to factory defaults. Operators in countries without regulatory requirements for DFS should disable DFS to avoid the additional minute of connection time for APs, BHMs, and SMs, and avoid the additional two minutes for BHSs.

With Release 8.2 and later, all of the 5.2-, 5.4-, and 5.7-GHz master and slave radios satisfy the requirements that the *FCC Report and Order 03-287*, Industry Canada, and *ETSI EN 301 893 v1.3.1* impose for DFS. These regulations differ on

- which radio frequency band(s) have DFS required.
- whether older radios must have DFS enabled.
- whether SMs and BHSs, in addition to APs and BHMs, must have DFS enabled.

Moreover in Release 8.2 and later, 5.4-GHz radios that are set for Canada or Australia omit center channel frequencies from 5580 to 5670 MHz, inclusive, from their GUIs and cannot operate in that range. This satisfies Canadian and Australian requirements that protect weather radio from interference by co-channel operation. This leaves 6 instead of 9 channels at 25-MHz center spacing³ (or 7 instead of 11 at 20-MHz center spacing). Operators in the U.S.A. should avoid the weather channels as well, but may be able to temporarily use them after spectrum analysis reveals that no competition exists.

The master radios properly implement the regionally-imposed DFS conditions after reading the value of the **Region Code** parameter, which Release 8.2 introduced. The effect of the DFS feature, based on the **Region Code** value (if this parameter is present), is shown in [Table 30](#).

³ 25-MHz center channel spacing is recommended for CAP 130 (Advantage AP) and 20-Mbps BH.

Table 30: Effect of DFS feature

Region Code ¹ Value	Effect of DFS Feature							
	900 MHz	2.4 GHz	5.2 GHz		5.4 GHz		5.7 GHz	
	AP SM	AP SM BH	AP BHM	SM BHS	AP BHM	SM BHS	AP BHM	SM BHS
Australia	No effect	No effect			FCC/IC DFS with notch ²	No effect	No effect	No effect
Brazil					ETSI DFS	ETSI DFS	No effect	No effect
Canada	No effect	No effect	FCC/IC DFS ³	No effect	FCC/IC DFS with notch ²	No effect	No effect	No effect
Europe		No effect			ETSI DFS	ETSI DFS	ETSI DFS	ETSI DFS
Russia			No effect	No effect			No effect	No effect
United States	No effect	No effect	FCC/IC DFS ³	No effect	FCC/IC DFS	No effect	No effect	No effect
Other	No effect on radio operation							
None	AP or BHM will not transmit							

NOTES:

1. In all cases, set the **Region Code** parameter to the appropriate region. Then the software will determine the correct use of DFS.
2. Center channel frequencies from 5580 to 5670 MHz, inclusive, are omitted (notched out of the otherwise continuous band) from the GUIs and these radios cannot operate in that range.
3. Newly manufactured P10 5.2-GHz radios use DFS. Radios that were purchased without DFS are not required to use DFS.

When an AP or BHM boots, it performs a channel availability check (CAC) for one minute on its main carrier frequency, without transmitting, as it monitors the channel for radar. If it detects no radar signature during this minute, the radio then proceeds to normal beacon transmit mode. If it does detect a radar signature, it locks that frequency carrier out for 30 minutes, and switches to the **Alternate Frequency Carrier 1**, which is set in the Configuration => Radio web page.

For the next minute, the radio monitors this new frequency for radar and, if it detects no radar, it proceeds to beacon transmit mode. If it does detect radar, it locks that frequency carrier out for 30 minutes, and switches to **Alternate Frequency Carrier 2**. For the minute that follows, the radio monitors this second alternate frequency and responds as described above to the presence or absence of radar on its current channel, switching if necessary to the next channel in line.

The ETSI EN 301 893 v1.3.1 specification requires DFS on a slave radio (SM or BHS) also. A slave radio transmits only if it receives a beacon from the master radio (AP or BHM). When the slave radio with DFS boots, it scans to distinguish whether a master radio beacon is present. If it finds a master, the slave receives on that frequency for

one minute without transmitting, as it monitors for a radar signature. Then the slave proceeds as follows:

- If an SM detects no radar during this minute, it attempts to register in the AP. If it does detect radar, it locks out that frequency for 30 minutes and continues scanning other frequencies in its scan list.
- If a BHS detects no radar during this minute, it registers in the BHM. While registering and ranging, it continues *for another full minute* to scan for radar. If it detects radar, it locks out that frequency for 30 minutes and continues scanning other frequencies in its scan list.

The possibility exists for a slave to attempt to register in a different master at this point and to even succeed. This would depend on both of the following conditions:

- matching color code values in the slave and master
- matching transmission frequency of the master to one that the slave is set in the scan list of the slave.

The slave automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), the operator should always set the value that corresponds to the local region.

The Home => General Status web page in any module with DFS displays one of the following status statements in its read-only field **DFS** field under Device Information:

- Normal Transmit
- Radar Detected Stop Transmitting for *n* minutes, where *n* counts down from 30 to 1.
- Checking Channel Availability Remaining time *n* seconds, where *n* counts down from 60 to 1.
- Idle, which indicates that the slave radio is scanning but has failed to detect a beacon from a master radio. When it has detected a beacon, the slave initiates a channel availability check (CAC) on that frequency.



RECOMMENDATION:

Where regulations require that radar sensing and radio shutdown is enabled, you can most effectively share the spectrum with satellite services if you perform spectrum analysis and select channels that are distributed evenly across the frequency band range.

A connectorized 5.7-GHz module provides an **Antenna Gain** parameter. When you indicate the gain of your antenna in this field, the algorithm calculates the appropriate sensitivity to radar signals, and this reduces the occurrence of false positives (wherever the antenna gain is less than the maximum).

Release 9 introduces support for Dynamic Frequency Selection (DFS) ETSI v1.4.1.

12.3 USING JITTER TO CHECK RECEIVED SIGNAL QUALITY (FSK ONLY)

The General Status tab in the Home page of the SM and BHS displays current values for **Jitter**, which is essentially a measure of interference. Interpret the jitter value as indicated in [Table 31](#).

Table 31: Signal quality levels indicated by jitter

Signal Modulation	Correlation of Highest Seen Jitter to Signal Quality		
	High Quality	Questionable Quality	Poor Quality
1X operation (2-level FSK)	0 to 4	5 to 14	15
2X operation (4-level FSK)	0 to 9	10 to 14	15

In your lab, an SM whose jitter value is constant at 14 may have an incoming packet efficiency of 100%. However, a deployed SM whose jitter value is 14 is likely to have even higher jitter values as interfering signals fluctuate in strength over time. So, *do not* consider 14 to be acceptable. Avoiding a jitter value of 15 should be the highest priority in establishing a link. At 15, jitter causes fragments to be dropped and link efficiency to suffer.

Modules calculate jitter based on both interference and the modulation scheme. For this reason, values on the low end of the jitter range that are significantly higher in 2X operation can still be indications of a high quality signal. For example, where the amount of interference remains constant, an SM with a jitter value of 3 in 1X operation can display a jitter value of 7 when enabled for 2X operation.

However, on the high end of the jitter range, *do not* consider the higher values in 2X operation to be acceptable. This is because 2X operation is much more susceptible to problems from interference than is 1X. For example, where the amount of interference remains constant, an SM with a jitter value of 6 in 1X operation can display a jitter value of 14 when enabled for 2X operation. As indicated in [Table 31](#), these values are unacceptable.

OFDM uses a different modulation scheme and does not display a jitter value.

12.4 USING LINK EFFICIENCY TO CHECK FSK RECEIVED SIGNAL QUALITY

A link test, available in the Link Capacity Test tab of the Tools web page in an AP or BH, provides a more reliable indication of received signal quality, particularly if you launch tests of varying duration. However, a link test interrupts traffic and consumes system capacity, so *do not* routinely launch link tests across your networks.

12.4.1 Comparing Efficiency in 1X Operation to Efficiency in 2X Operation

Efficiency of at least 98 to 100% indicates a high quality signal. Check the signal quality numerous times, at various times of day and on various days of the week (as you checked the RF environment a variety of times by spectrum analysis before placing

radios in the area). Efficiency less than 90% in 1X operation or less than 60% in 2X operation indicates a link with problems that require action.

12.4.2 When to Switch from 2X to 1X Operation Based on 60% Link Efficiency

In the above latter case (60% in 2X operation), the link experiences worse latency (from packet resends) than it would in 1X operation, but still greater capacity, if the link remains stable at 60% Efficiency. Downlink Efficiency and Uplink Efficiency are measurements produced by running a link test from either the SM or the AP. Examples of what action should be taken based on Efficiency in 2X operation are provided in [Table 32](#).

Table 32: Recommended courses of action based on Efficiency in 2X operation

Module Types	Further Investigation	Result	Recommended Action
CAP 130 with CSM 130	Check the General Status tab of the CSM 130. ¹ See Checking the Status of 2X Operation on Page 94.	Uplink and downlink are both $\geq 60\%$ Efficiency. ²	Rerun link tests.
	Rerun link tests.	Uplink and downlink are both $\geq 60\%$ Efficiency.	Optionally, re-aim SM, add a reflector, or otherwise mitigate interference. In any case, continue 2X operation up and down.
CAP 130 with CSM 120	Check the General Status tab of the CSM 120. ¹ See Checking the Status of 2X Operation on Page 94.	Uplink and downlink are both $\geq 60\%$ Efficiency. ²	Rerun link tests.
	Rerun link tests.	Uplink and downlink are both $\geq 60\%$ Efficiency.	Optionally, re-aim SM, add a reflector, or otherwise mitigate interference. In any case, continue 2X operation up and down.
		Results are inconsistent and range from 20% to 80% Efficiency.	Monitor the Session Status tab in the CAP 130.
	Monitor the Session Status tab in the CAP 130.	Link fluctuates between 2X and 1X operation. ³	Optionally, re-aim SM, add a reflector, or otherwise mitigate interference. Then rerun link tests.
	Rerun link tests.	No substantial improvement with consistency is seen.	On the General tab of the SM, disable 2X operation. Then rerun link tests.
	Rerun link tests.	Uplink and downlink are both $\geq 90\%$ Efficiency.	Continue 1X operation up and down.
NOTES:			
1. Or check Session Status page of the CAP 130, where a sum of greater than 7,000,000 bps for the up- and downlink indicates 2X operation up and down (for 2.4- or 5.x-GHz modules).			
2. For throughput to the SM, this is equivalent to 120% Efficiency in 1X operation, with less capacity used at the AP.			
3. This link is problematic.			

12.5 CONSIDERING FREQUENCY BAND ALTERNATIVES

For 5.2-, 5.4-, and 5.7-GHz modules, 20-MHz wide channels are centered every 5 MHz. For 2.4-GHz modules, 20-MHz wide channels are centered every 2.5 MHz. For OFDM, the operator can configure center channel frequencies of the 10 MHz channels with a granularity of 0.5 MHz. This allows the operator to customize the channel layout for interoperability where other equipment is collocated.

Cross-band deployment of APs and BH is the recommended alternative (for example, a 5.2-GHz AP collocated with 5.7-GHz BH).



IMPORTANT!

In all cases, channel center separation between collocated FSK modules should be at least 20 MHz for 1X operation and 25 MHz for 2X. For OFDM, channel center separation between collocated modules should be at least 10 MHz.

12.5.1 900-MHz Channels

900-MHz AP Available Channels

A 900-MHz AP can operate with its 8-MHz wide channel centered on any of the following frequencies:

(All Frequencies in MHz)

906	909	912	915	918	922
907	910	913	916	919	923
908	911	914	917	920	924

900-MHz AP Cluster Recommended Channels

Three non-overlapping channels are recommended for use in a 900-MHz AP cluster:

(All Frequencies in MHz)

906	915	924
-----	-----	-----

This recommendation allows 9 MHz of separation between channel centers. You can use the Spectrum Analysis feature in an SM, or use a standalone spectrum analyzer, to evaluate the RF environment. In any case, ensure that the 8-MHz wide channels you select *do not* overlap.

12.5.2 2.4-GHz Channels

2.4-GHz BHM and AP Available Channels

A 2.4-GHz BHM or AP can operate with its 20-MHz wide channel centered on any of the following channels, which are separated by only 2.5-MHz increments.

(All Frequencies in GHz)

2.4150	2.4275	2.4400	2.4525
2.4175	2.4300	2.4425	2.4550
2.4200	2.4325	2.4450	2.4575
2.4225	2.4350	2.4475	
2.4250	2.4375	2.4500	

The center channels of *adjacent* 2.4-GHz APs should be separated by at least 20 MHz.

2.4-GHz AP Cluster Recommended Channels

Three non-overlapping channels are recommended for use in a 2.4-GHz AP cluster:

(All Frequencies in GHz)
2.4150 2.4350 2.4575

This recommendation allows 20 MHz of separation between one pair of channels and 22.5 MHz between the other pair. You can use the Spectrum Analysis feature in an SM or BHS, or use a standalone spectrum analyzer, to evaluate the RF environment. Where spectrum analysis identifies risk of interference for any of these channels, you can compromise this recommendation as follows:

- Select 2.4375 GHz for the middle channel
- Select 2.455 GHz for the top channel
- Select 2.4175 GHz for the bottom channel

In any case, ensure that your plan allows at least 20 MHz of separation between channels.

12.5.3 4.9-GHz OFDM Channels

Channel selections for the OFDM AP in the 4.9-GHz frequency band range are 4.945 through 4.985 GHz on 5-MHz centers, with not more than five non-overlapping channels.

12.5.4 5.2-GHz Channels

Channel selections for the AP in the 5.2-GHz frequency band range depend on whether the AP is deployed in cluster.

5.2-GHz BH and Single AP Available Channels

A BH or a single 5.2-GHz AP can operate in the following channels, which are separated by 5-MHz increments.

(All Frequencies in GHz)
5.275 5.290 5.305 5.320
5.280 5.295 5.310 5.325
5.285 5.300 5.315

The center channels of *adjacent* APs should be separated by at least 20 MHz. However, 25 MHz of separation is advised, especially for CAP 130s to take advantage of 2X operation.

5.2-GHz AP Cluster Recommended Channels

Three non-overlapping channels are recommended for use in a 5.2-GHz AP cluster:

(All Frequencies in GHz)
5.275 5.300 5.325

12.5.5 5.4-GHz FSK Channels

Channel selections for the AP in the 5.4-GHz FSK frequency band range depend on whether the AP is deployed in cluster.

5.4-GHz BH and Single AP Available

A BH or single 5.4-GHz FSK AP can operate in the following channels, which are separated by 5-MHz.

(All Frequencies in GHz)

5495	5515	5535	5555	5575	5595	5615	5635	5655	5675	5695
5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700
5505	5525	5545	5565	5585	5605	5625	5645	5665	5685	5705
5510	5530	5550	5570	5590	5610	5630	5650	5670	5690	

The channels of *adjacent* APs should be separated by at least 20 MHz, especially for CAP 130s to take advantage of 2X operation.


5.4-GHz AP Cluster Recommended Channels

The fully populated cluster requires only three channels, each reused by the module that is mounted 180° opposed. In this frequency band range, the possible sets of three non-overlapping channels are numerous. As many as 11 non-overlapping 20-MHz wide channels are available for 1X operation. Fewer 25-MHz wide channels are available for 2X operation, where this greater separation is recommended for interference avoidance.

5.4-GHz AP Cluster Limit Case

In the limit, the 11 channels could support all of the following, vertically stacked on the same mast:

- 3 full clusters, each cluster using 3 channels
- a set of 4 APs, the set using the 2 channels that no AP in any of the 3 full clusters is using



IMPORTANT!
Where regulations require you to have Dynamic Frequency Selection (DFS) enabled, analyze the spectrum, then spread your channel selections as evenly as possible throughout this frequency band range, appropriately sharing it with satellite services.

12.5.6 5.4-GHz OFDM Channels

Channel selections for the PMP 400 Series AP in the 5.4-GHz frequency band range depend on whether the AP is deployed.

5.4-GHz Single OFDM AP Available Channels

Operators configure the channels of OFDM modules on their Configuration => Custom Frequencies web pages. The available center channels for an individual OFDM AP (not in cluster) depends on the region where the AP is deployed and are in the ranges quoted in [Table 33](#).

Table 33: Available center channels for single OFDM AP

Region	Range(s) For Center Channels ¹
U.S.A.	5480 to 5710
Canada	5480 to 5595 5655 to 5710
Europe	5475 to 5595 5655 to 5715
NOTES:	
1. Selectable in 5-MHz increments.	

5.4-GHz OFDM AP Cluster Recommended Channels

No guard band is required between 10-MHz channels. However, to use the 3X operation feature of these OFDM modules, you should separate the channels of clustered APs by at least 10 MHz. The fully populated cluster may be configured for two channels—each reused by the module that is mounted 180° opposed—or four channels.

Channels are preconfigured to help in your decision on the two or four to use in a four-AP cluster. These modules *do not* include a spectrum analyzer for you to read the strength of neighboring frequencies. The ranges of available center channels for clustered APs are those shown in [Table 33](#) above.

However, where 5.4-GHz OFDM APs are collocated with 5.4-GHz FSK APs, you should allow 25 MHz channel center spacing to prevent either of the sectors from experiencing interference from the other.

12.5.7 5.7-GHz Channels

Channel selections for the AP in the 5.7-GHz frequency band range depend on whether the AP is deployed in cluster.

5.7-GHz BH and Single AP Available Channels

A BH or a single 5.7-GHz AP enabled for frequencies can operate in the following channels, which are separated by 5-MHz increments.

(All Frequencies in GHz)

5.735	5.765	5.795	5.825
5.740	5.770	5.800	5.830
5.745	5.775	5.805	5.835
5.750	5.780	5.810	5.840
5.755	5.785	5.815	
5.760	5.790	5.820	

The channels of *adjacent* APs should be separated by at least 20 MHz. However, 25 MHz of separation is advised, especially for CAP 130s to take advantage of 2X operation.

5.7-GHz AP Cluster Recommended Channels

Six non-overlapping channels are recommended for use in 5.7-GHz AP clusters:

(All Frequencies in GHz)
 5.735 5.775 5.815
 5.755 5.795 5.835

The fully populated cluster requires only three channels, each reused by the module that is mounted 180° offset. The six channels above are also used for backhaul point-to-point links.

As noted above, a 5.7-GHz AP can operate on a frequency as high as 5.840 GHz. Where engineering plans allow, this frequency can be used to provide an additional 5-MHz separation between AP and BH channels.

12.5.8 Channels Available for PTP 400 and PTP 600 Radios

Channel selections for radios in the PTP400 and PTP 600 series are quoted in the user guides that are dedicated to those products. However, these units dynamically change channels when the signal substantially degrades. Since the available channels are in the 5.4- and 5.7-GHz frequency band ranges, carefully consider the potential effects of deploying these products into an environment where traffic in this range pre-exists.

12.5.9 Example Channel Plans for FSK AP Clusters

Examples for assignment of frequency channels and sector IDs are provided in the following tables. Each frequency is reused on the sector that is at a 180° offset. The entry in the Symbol column of each table refers to the layout in [Figure 34](#) on Page 144.



NOTE:

The operator specifies the sector ID for the module as described under [Sector ID](#) on Page 445.

Table 34: Example 900-MHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	906 MHz	0	A
Northeast (60°)	915 MHz	1	B
Southeast (120°)	924 MHz	2	C
South (180°)	906 MHz	3	A
Southwest (240°)	915 MHz	4	B
Northwest (300°)	924 MHz	5	C

Table 35: Example 2.4-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	2.4150 GHz	0	A
Northeast (60°)	2.4350 GHz	1	B
Southeast (120°)	2.4575 GHz	2	C
South (180°)	2.4150 GHz	3	A
Southwest (240°)	2.4350 GHz	4	B
Northwest (300°)	2.4575 GHz	5	C

Table 36: Example 5.2-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.275 GHz	0	A
Northeast (60°)	5.300 GHz	1	B
Southeast (120°)	5.325 GHz	2	C
South (180°)	5.275 GHz	3	A
Southwest (240°)	5.300 GHz	4	B
Northwest (300°)	5.325 GHz	5	C

Table 37: Example 5.4-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.580 GHz	0	A
Northeast (60°)	5.620 GHz	1	B
Southeast (120°)	5.660 GHz	2	C
South (180°)	5.580 GHz	3	A
Southwest (240°)	5.620 GHz	4	B
Northwest (300°)	5.660 GHz	5	C

Table 38: Example 5.7-GHz FSK channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.735 GHz	0	A
Northeast (60°)	5.755 GHz	1	B
Southeast (120°)	5.775 GHz	2	C
South (180°)	5.735 GHz	3	A
Southwest (240°)	5.755 GHz	4	B
Northwest (300°)	5.775 GHz	5	C

12.5.10 Multiple FSK Access Point Clusters

When deploying multiple AP clusters in a dense area, consider aligning the clusters as shown in [Figure 34](#). However, this is only a recommendation. An installation may dictate a different pattern of channel assignments.

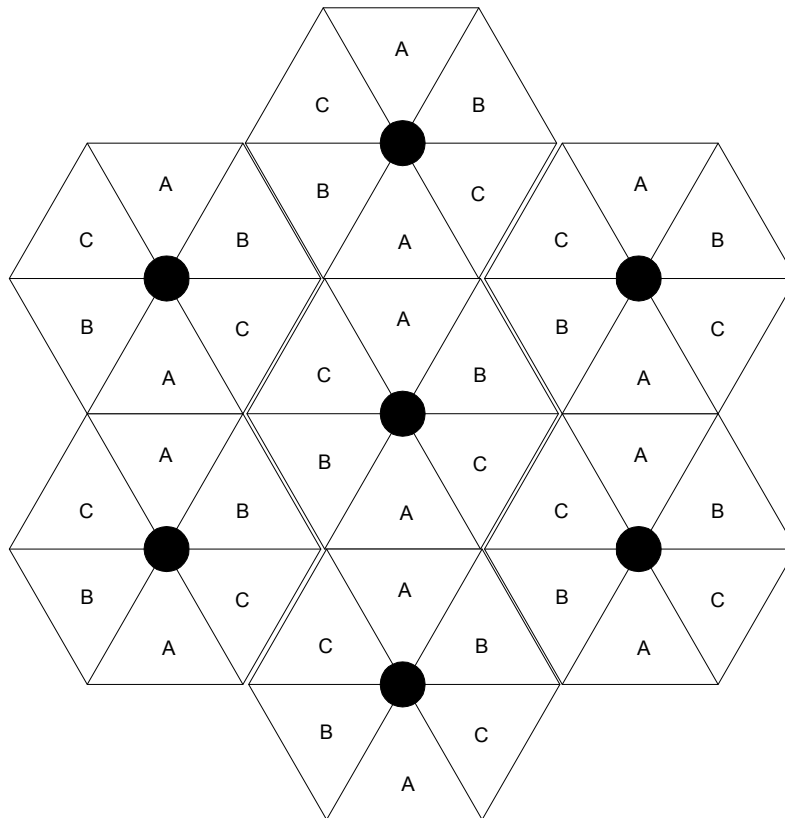


Figure 34: Example layout of 7 FSK Access Point clusters

12.5.11 Example Channel Plan for OFDM AP Cluster

An example for assignment of frequency channels and sector IDs is provided in the following table. Each frequency is reused on the sector that is at a 180° offset. The entry in the Symbol column of each table refers to the layout in [Figure 35](#) on Page 146.



NOTE:

The operator specifies the sector ID for the module as described under [Sector ID](#) on Page 445.

Table 39: Example 4.9-GHz OFDM channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	4.955 GHz	0	A
East (90°)	4.973 GHz	1	B
South (180°)	4.955 GHz	2	A
West (270°)	4.973 GHz	3	B

Table 40: Example 5.4-GHz OFDM channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.475 GHz	0	A
East (90°)	5.715 GHz	1	B
South (180°)	5.475 GHz	2	A
West (270°)	5.715 GHz	3	B

NOTE:

The guard band for access by weather information transmissions spans 5.480 to 5.710 GHz. The example frequencies listed above avoid this guard band.

12.5.12 Multiple OFDM Access Point Clusters

When deploying multiple AP clusters in a dense area, consider aligning the clusters as shown in [Figure 35](#). However, this is only a recommendation. An installation may dictate a different pattern of channel assignments.

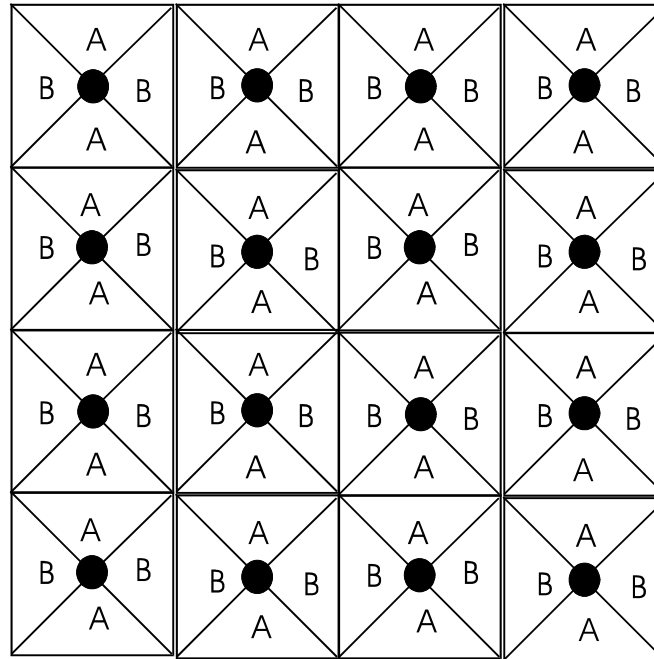


Figure 35: Example layout of 16 OFDM Access Point sectors

12.6 SELECTING SITES FOR NETWORK ELEMENTS

The APs must be positioned

- with hardware that the wind and ambient vibrations cannot flex or move.
- where a tower or rooftop is available or can be erected.
- where a grounding system is available.
- with lightning arrestors to transport lightning strikes away from equipment.
- at a proper height:
 - higher than the tallest points of objects immediately around them (such as trees, buildings, and tower legs).
 - at least 2 feet (0.6 meters) below the tallest point on the tower, pole, or roof (for lightning protection).
- away from high-RF energy sites (such as AM or FM stations, high-powered antennas, and live AM radio towers).
- in line-of-sight paths
 - to the SMs and BH.
 - that will not be obstructed by trees as they grow or structures that are later built.



NOTE:

Visual line of sight does not guarantee radio line of sight.

12.6.1 Resources for Maps and Topographic Images

Mapping software is available from sources such as the following:

- <http://www.microsoft.com/streets/default.asp>
 - Microsoft Streets & Trips (with Pocket Streets)
- <http://www.delorme.com/software.htm>
 - DeLorme Street Atlas USA
 - DeLorme Street Atlas USA Plus
 - DeLorme Street Atlas Handheld

Topographic maps are available from sources such as the following:

- <http://www.delorme.com/software.htm>
 - DeLorme Topo USA
 - DeLorme 3-D TopoQuads
- <http://www.usgstopomaps.com>
 - Timely Discount Topos, Inc. authorized maps

Topographic maps with waypoints are available from sources such as the following:

- <http://www.topografix.com>
 - TopoGrafix EasyGPS
 - TopoGrafix Panterra
 - TopoGrafix ExpertGPS

Topographic images are available from sources such as the following:

- <http://www.keyhole.com/body.php?h=products&t=keyholePro>
 - keyhole PRO
- <http://www.digitalglobe.com>
 - various imagery

12.6.2 Surveying Sites

Factors to survey at potential sites include

- what pre-existing wireless equipment exists at the site. (Perform spectrum analysis.)
- whether available mounting positions exist near the lowest elevation that satisfies line of site, coverage, and other link criteria.
- whether you will always have the right to decide who climbs the tower to install and maintain your equipment, and whether that person or company can climb at any hour of any day.
- whether you will have collaborative rights and veto power to prevent interference to your equipment from wireless equipment that is installed at the site in the future.
- whether a pre-existing grounding system (path to Protective Earth ↓) exists, and what is required to establish a path to it.
- who is permitted to run any indoor lengths of cable.

12.6.3 Assuring the Essentials

In the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency band ranges, an unobstructed line of sight (LOS) must exist and be maintainable between the radios that are involved in each link.

Line of Sight (LOS) Link

In these ranges, a line of sight link is both

- an unobstructed straight line from radio to radio.
- an unobstructed zone surrounding that straight line.

Fresnel Zone Clearance

An unobstructed line of sight is important, but is not the *only* determinant of adequate placement. Even where the path has a clear line of sight, obstructions such as terrain, vegetation, metal roofs, or cars may penetrate the Fresnel zone and cause signal loss. [Figure 36](#) illustrates an ideal Fresnel zone.

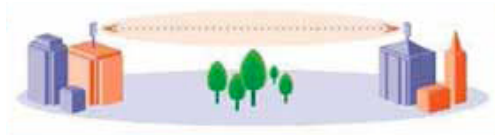


Figure 36: Fresnel zone in line of sight link

[FresnelZoneCalcPage.xls](#) calculates the Fresnel zone clearance that is required between the visual line of sight and the top of an obstruction that would protrude into the link path.

Near Line of Sight (nLOS) Link

The 900-MHz and OFDM modules have a greater near line of sight (nLOS) range than modules of other frequency bands. NLOS range depends on RF considerations such as foliage, topography, obstructions. A depiction of an nLOS link is shown in [Figure 37](#).



Figure 37: Fresnel zone in near line of sight link

Non-Line of Sight (NLOS) Link

The 900-MHz and OFDM modules have a greater non-line of sight (NLOS) range than modules of other frequency bands. NLOS range depends on RF considerations such as foliage, topography, obstructions. A depiction of an NLOS link is shown in [Figure 38](#).



Figure 38: Fresnel zone in non-line of sight link

12.6.4 Finding the Expected Coverage Area

The transmitted beam in the vertical dimension covers more area beyond than in front of the beam center. [BeamwidthRadiiCalcPage.xls](#) calculates the radii of the beam coverage area for PMP 100 Series APs.

12.6.5 Clearing the Radio Horizon

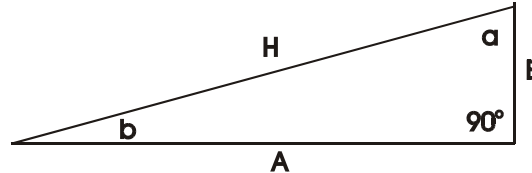
Because the surface of the earth is curved, higher module elevations are required for greater link distances. This effect can be critical to link connectivity in link spans that are greater than 8 miles (12 km). [AntennaElevationCalcPage.xls](#) calculates the minimum antenna elevation for these cases, presuming no landscape elevation difference from one end of the link to the other.

12.6.6 Calculating the Aim Angles

The appropriate angle of AP downward tilt is derived from both the distance between transmitter and receiver and the difference in their elevations. [DowntiltCalcPage.xls](#) calculates this angle.

The proper angle of tilt can be calculated as a factor of both the difference in elevation and the distance that the link spans. Even in this case, a plumb line and a protractor can be helpful to ensure the proper tilt. This tilt is typically minimal.

The number of degrees to offset (from vertical) the mounting hardware leg of the support tube is equal to the angle of elevation from the lower module to the higher module (<B in the example provided in [Figure 39](#)).



LEGEND

b Angle of elevation.

B Vertical difference in elevation.

A Horizontal distance between modules.

Figure 39: Variables for calculating angle of elevation (and depression)

Calculating the Angle of Elevation

To use metric units to find the angle of elevation, use the following formula:

$$\tan b = \frac{B}{1000A}$$

where

B is expressed in meters

A is expressed in kilometers.

To use English standard units to find the angle of elevation, use the following formula:

$$\tan b = \frac{B}{5280A}$$

where
 B is expressed in feet
 A is expressed in miles.

The angle of depression from the higher module is identical to the angle of elevation from the lower module.

12.7 COLLOCATING MODULES

A BH and an AP or AP cluster on the same tower require a CMM. The CMM properly synchronizes the *transmit start* times of all modules to prevent interference and desensing of the modules. At closer distances without sync from a CMM, the frame structures cause self interference.

Furthermore, a BH and an AP on the same tower require that the effects of their differing *receive start* times be mitigated by either

- 100 vertical feet (30 meters) or more and as much spectral separation as possible within the same frequency band range.
- the use of the frame calculator to tune the **Downlink Data** parameter in each, so that the receive start time in each is the same. See [Using the Frame Calculator Tool \(All\)](#) on Page 446.

APs and a BHS can be collocated at the same site only if they operate in different frequency band ranges.

Where a single BH air link is insufficient to cover the distance from an AP cluster to your point of presence (POP), you can deploy two BHSs, connected to one another by Ethernet, on a tower that is between a BHM collocated with the AP cluster and another BHM collocated with the POP. This deployment is illustrated in [Figure 40](#).

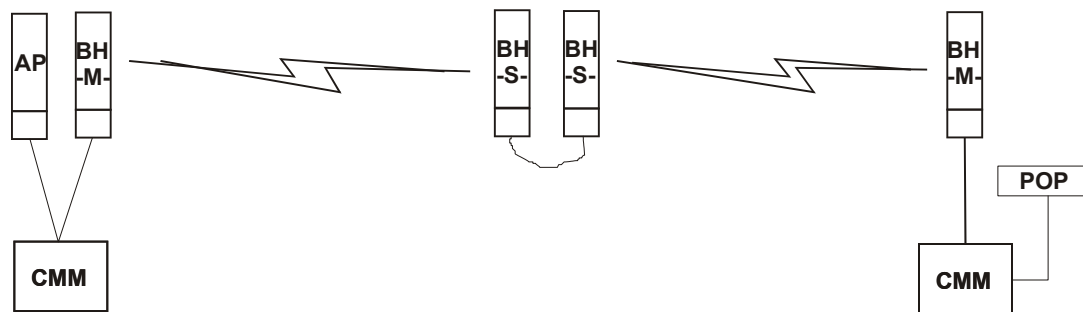


Figure 40: Double-hop backhaul links

However, the BHSs can be collocated at the same site *only if* one is on a different frequency band range from that of the other or one of the following conditions applies:

- They are vertically separated on a structure by at least 100 feet (30 m).
- They are vertically separated on a structure by less distance, but either
 - an RF shield isolates them from each other.
 - the uplink and downlink data parameters and control channels match (the **Downlink Data** parameter is set to **50%**).

The constraints for collocated modules in the same frequency band range are to avoid self-interference that would occur between them. Specifically, unless the uplink and downlink data percentages match, intervals exist when one is transmitting while the other is receiving, such that the receiving module cannot receive the signal from the far end.

The interference is less a problem during low throughput periods and intolerable during high. Typically, during low throughput periods, sufficient time exists for the far end to retransmit packets lost because of interference from the collocated module.

12.8 DEPLOYING A REMOTE AP

In cases where the subscriber population is widely distributed, or conditions such as geography restrict network deployment, you can add a Remote AP to

- provide high-throughput service to near LoS business subscribers.
- reach around obstructions or penetrate foliage with non-LoS throughput.
- reach new, especially widely distributed, residential subscribers with broadband service.
- pass sync to an additional RF hop.

In the remote AP configuration, a remote AP is collocated with an SM. The remote AP distributes the signal over the last mile to SMs that are logically behind the collocated SM. A remote AP deployment is illustrated in [Figure 41](#).

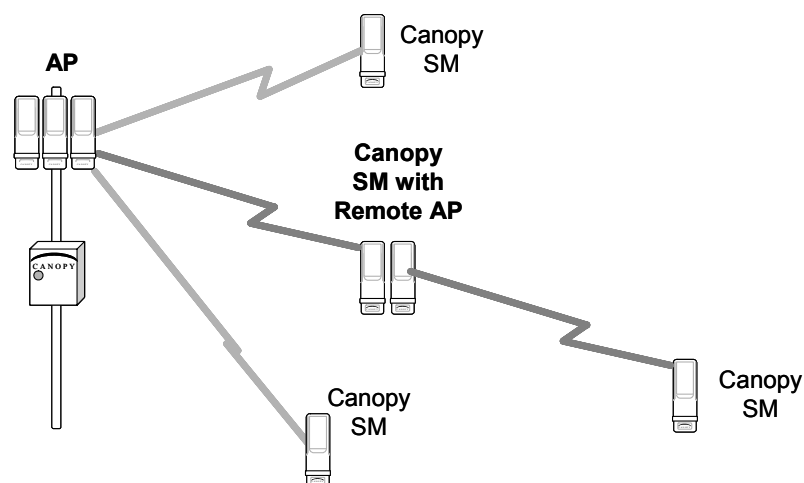


Figure 41: Remote AP deployment

The collocated SM receives data in one frequency band, and the remote AP must redistribute the data in a different frequency band. Base your selection of frequency band ranges on regulatory restrictions, environmental conditions, and throughput requirements.

**IMPORTANT!**

Each relay hop (additional daisy-chained remote AP) adds approximately 6 msec latency.

12.8.1 Remote AP Performance

The performance of a remote AP is identical to the AP performance in cluster. Throughputs, ranges, and patch antenna coverage are identical. CAP 130s and CSM 130s (or CAP 09130s and CSM 09130s) can be deployed in tandem in the same sector to meet customer bandwidth demands.

As with all equipment operating in the unlicensed spectrum, Motorola *strongly* recommends that you perform site surveys before you add network elements. These will indicate that spectrum is available in the area where you want to grow. Keep in mind that

- non-LoS ranges heavily depend on environmental conditions.
- in most regions, not all frequencies are available.
- your deployments must be consistent with local regulatory restrictions.

12.8.2 Example Use Case for RF Obstructions

A remote AP can be used to provide last-mile access to a community where RF obstructions prevent SMs from communicating with the higher-level AP in cluster. For example, you may be able to use 900 MHz for the last mile between a remote AP and the outlying SMs where these subscribers cannot form good links to a higher-level 2.4-GHz AP. In this case, the short range of the 900-MHz remote AP is sufficient, and the ability of the 900-MHz wavelength to be effective around foliage at short range solves the foliage penetration problem.

An example of this use case is shown in [Figure 42](#).

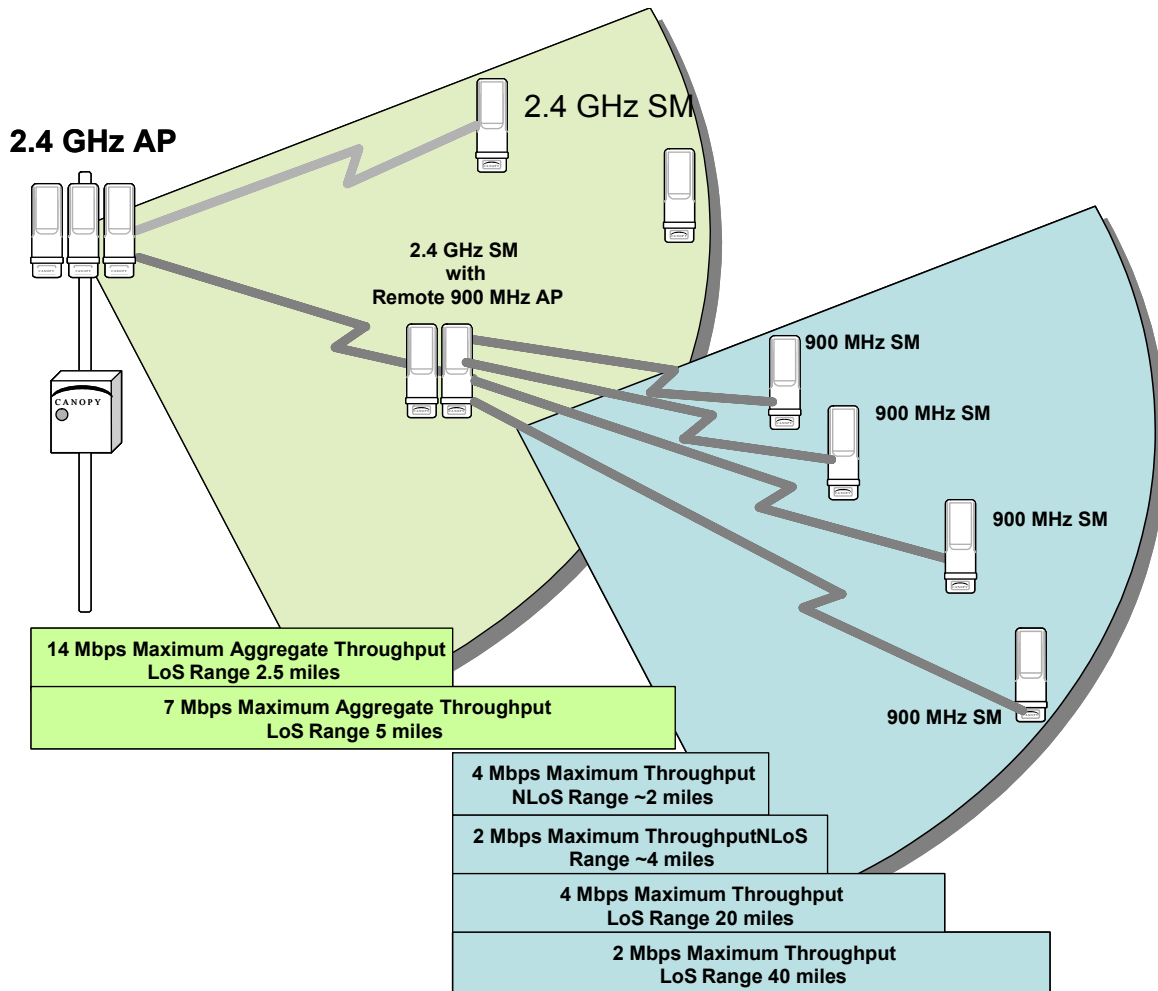


Figure 42: Example 900-MHz remote AP behind 2.4-GHz SM

The 2.4 GHz modules provide a sustained aggregate throughput of up to 14 Mbps to the sector. One of the SMs in the sector is wired to a 900-MHz remote AP, which provides NLoS sustained aggregate throughput⁴ of

- 4 Mbps to 900-MHz SMs up to 2 miles away in the sector.
- 2 Mbps to 900-MHz SMs between 2 and 4 miles away in the sector.

12.8.3 Example Use Case for Passing Sync

All radios support the remote AP functionality. The BHS and the SM can reliably pass the sync pulse, and the BHM and AP can reliably receive it. Examples of passing sync over cable are shown under [Passing Sync in an Additional Hop](#) on Page 99. The sync cable is described under [Cables](#) on Page 63.

⁴ NLoS ranges depend on environmental conditions. Your results may vary from these.

The sync is passed in a cable that connects Pins 1 and 6 of the RJ-11 timing ports of the two modules. When you connect modules in this way, you must also adjust configuration parameters to ensure that

- the AP is set to properly receive sync.
- the SM will not propagate sync to the AP if the SM itself ceases to receive sync.

Perform [Procedure 32: Extending network sync](#) on Page 378.

12.8.4 Physical Connections Involving the Remote AP

The SM to which you wire a remote AP can be either an SM that serves a customer or an SM that simply serves as a relay. Where the SM serves a customer, wire the remote AP to the SM as shown in [Figure 43](#).

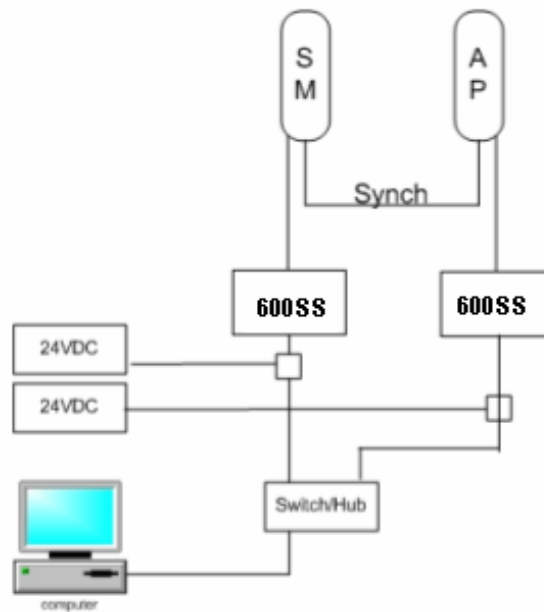


Figure 43: Remote AP wired to SM that also serves a customer

Where the SM simply serves as a relay, you must use a straight-through RJ-45 female-to-female coupler, and wire the SM to the remote AP as shown in [Figure 44](#).

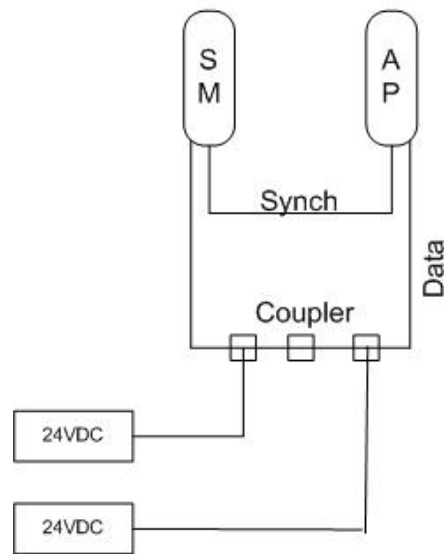


Figure 44: Remote AP wired to SM that serves as a relay

12.9 DIAGRAMMING NETWORK LAYOUTS

12.9.1 Accounting for Link Ranges and Data Handling Requirements

For aggregate throughput correlation to link distance in both point-to-multipoint and point-to-point links, see

- [Link Performance and Encryption Comparisons](#) on Page 67.
- all regulations that apply in your region and nation(s).

12.9.2 Avoiding Self Interference

For 5.2-, 5.4-, and 5.7-GHz modules, 20-MHz wide channels are centered every 5 MHz. For 2.4-GHz modules, 20-MHz wide channels are centered every 2.5 MHz. For 5.4-GHz OFDM modules, 10-MHz wide channels can be centered every 0.5 MHz. This allows you to customize the channel layout for interoperability where other equipment is collocated, as well as select channels with the least background interference level.



CAUTION!

Regardless of whether 2.4-, 5.2-, 5.4-, or 5.7-GHz modules are deployed, channel separation between modules should be at least 20 MHz for 1X operation or 25 MHz for 2X.

Physical Proximity

A BH and an AP on the same tower require a CMM. The CMM properly synchronizes the *transmit start* times of all modules to prevent interference and desensing of the modules. At closer distances without sync from a CMM, the frame structures cause self interference.

Furthermore, a BH and an AP on the same tower require that the effects of their differing *receive start* times be mitigated by either

- 100 vertical feet (30 meters) or more and as much spectral separation as possible within the same frequency band range.
- the use of the frame calculator to tune the Downlink Data % parameter in each, so that the receive start time in each is the same. See [Using the Frame Calculator Tool \(All\)](#) on Page 446.

Spectrum Analysis

You can use an SM or BHS as a spectrum analyzer. See [Mapping RF Neighbor Frequencies](#) on Page 131. Through a toggle of the **Device Type** parameter, you can temporarily transform an AP into an SM to use it as a spectrum analyzer.

Power Reduction to Mitigate Interference

Where any module (SM, AP, BH timing master, or BH timing slave) is close enough to another module that self-interference is possible, you can set the SM to operate at less than full power. To do so, perform the following steps.



CAUTION!

Too low a setting of the **Transmitter Output Power** parameter can cause a link to a distant module to drop. A link that drops for this reason requires Ethernet access to the GUI to re-establish the link.

Procedure 3: Reducing transmitter output power

1. Access the Radio tab of the module.
2. In the **Transmitter Output Power** parameter, reduce the setting.
3. Click **Save Changes**.
4. Click **Reboot**.
5. Access the Session Status tab in the Home web page of the SM.
6. Assess whether the link achieves good **Power Level** and **Jitter** values.
NOTE: The received **Power Level** is shown in dBm and should be maximized. **Jitter**, where a value is present, should be minimized. However, better/lower jitter should be favored over better/higher dBm. For historical reasons, **RSSI** is also shown and is the unitless measure of power. The best practice is to use **Power Level** and ignore **RSSI**, which implies more accuracy and precision than is inherent in its measurement.
7. Access the Link Capacity Test tab in the Tools web page of the module.
8. Assess whether the desired links for this module achieve
 - uplink efficiency greater than 90%.
 - downlink efficiency greater than 90%.
9. If the desired links fail to achieve any of the above measurement thresholds, then
 - a. access the module by direct Ethernet connection.
 - b. access the Radio tab in the Configuration web page of the module.
10. In the **Transmitter Output Power** parameter, increase the setting.

11. Click **Save Changes**.

12. Click **Reboot**.

===== end of procedure =====

12.9.3 Avoiding Other Interference

Where signal strength cannot dominate noise levels, the network experiences

- bit error corrections.
- packet errors and retransmissions.
- lower throughput (because bandwidth is consumed by retransmissions) and high latency (due to resends).

Be especially cognitive of these symptoms for 900-MHz links. Where you see these symptoms, attempt the following remedies:

- Adjust the position of the SM.
- Deploy a band-pass filter at the AP.
- Consider adding a remote AP closer to the affected SMs. (See [Deploying a Remote AP](#) on Page 151.)

Certain other actions, which may seem to be potential remedies, *do not* resolve high noise level problems:

- *Do not* deploy an omnidirectional antenna.
- *Do not* set the antenna gain above the regulated level.
- *Do not* deploy a band-pass filter in the expectation that this can mitigate co-channel interference.

13 ENGINEERING YOUR IP COMMUNICATIONS

13.1 UNDERSTANDING ADDRESSES

A basic understanding of Internet Protocol (IP) address and subnet mask concepts is required for engineering your IP network.

13.1.1 IP Address

The IP address is a 32-bit binary number that has four parts (octets). This set of four octets has two segments, depending on the class of IP address. The first segment identifies the network. The second identifies the hosts or devices on the network. The subnet mask marks a boundary between these two sub-addresses.

13.2 DYNAMIC OR STATIC ADDRESSING

For any computer to communicate with a module, the computer must be configured to either

- use DHCP (Dynamic Host Configuration Protocol). In this case, when not connected to the network, the computer derives an IP address on the 169.254 network within two minutes.
- have an assigned static IP address (for example, 169.254.1.5) on the 169.254 network.



IMPORTANT!

If an IP address that is set in the module is not the 169.254.x.x network address, then the network operator must assign the computer a static IP address in the same subnet.

13.2.1 When a DHCP Server is Not Found

To operate on a network, a computer requires an IP address, a subnet mask, and possibly a gateway address. Either a DHCP server automatically assigns this configuration information to a computer on a network or an operator must input these items.

When a computer is brought on line and a DHCP server is not accessible (such as when the server is down or the computer is not plugged into the network), Microsoft and Apple operating systems default to an IP address of 169.254.x.x and a subnet mask of 255.255.0.0 (169.254/16, where /16 indicates that the first 16 bits of the address range are identical among all members of the subnet).

13.3 NETWORK ADDRESS TRANSLATION (NAT)

13.3.1 NAT, DHCP Server, DHCP Client, and DMZ in SM

The system provides NAT (network address translation) for SMs in the following combinations of NAT and DHCP (Dynamic Host Configuration Protocol):

- NAT Disabled (as in earlier releases)
- NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface) and DHCP Server
- NAT with DHCP Client(**DHCP** selected as the **Connection Type** of the WAN interface)
- NAT with DHCP Server
- NAT without DHCP

NAT

NAT isolates devices connected to the Ethernet/wired side of an SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic (separate from its address for management), terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet/wired side of the SM.

In the Motorola system, NAT supports many protocols, including HTTP, ICMP (Internet Control Message Protocols), and FTP (File Transfer Protocol). For virtual private network (VPN) implementation, L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) and PPTP (Point to Point Tunneling Protocol) are supported. See [NAT and VPNs](#) on Page 165.

DHCP

DHCP enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the Motorola system.

In conjunction with the NAT features, each SM provides

- a DHCP server that assigns IP addresses to computers connected to the SM by Ethernet protocol.
- a DHCP client that receives an IP address for the SM from a network DHCP server.

DMZ

In conjunction with the NAT features, a DMZ (demilitarized zone) allows the assignment of one IP address behind the SM for a device to logically exist outside the firewall and receive network traffic. The first three octets of this IP address must be identical to the first three octets of the NAT private IP address.

NAT Disabled

The NAT Disabled implementation is illustrated in [Figure 45](#).

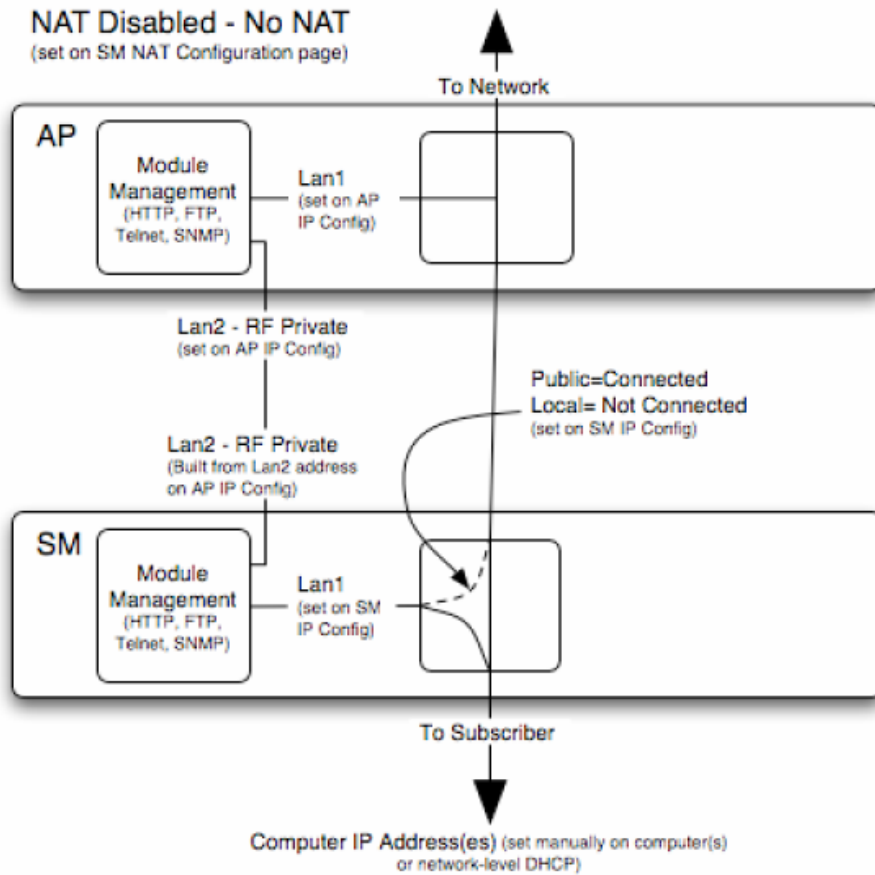


Figure 45: NAT Disabled implementation

NAT with DHCP Client and DHCP Server

The NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface) and DHCP Server implementation is illustrated in [Figure 46](#).

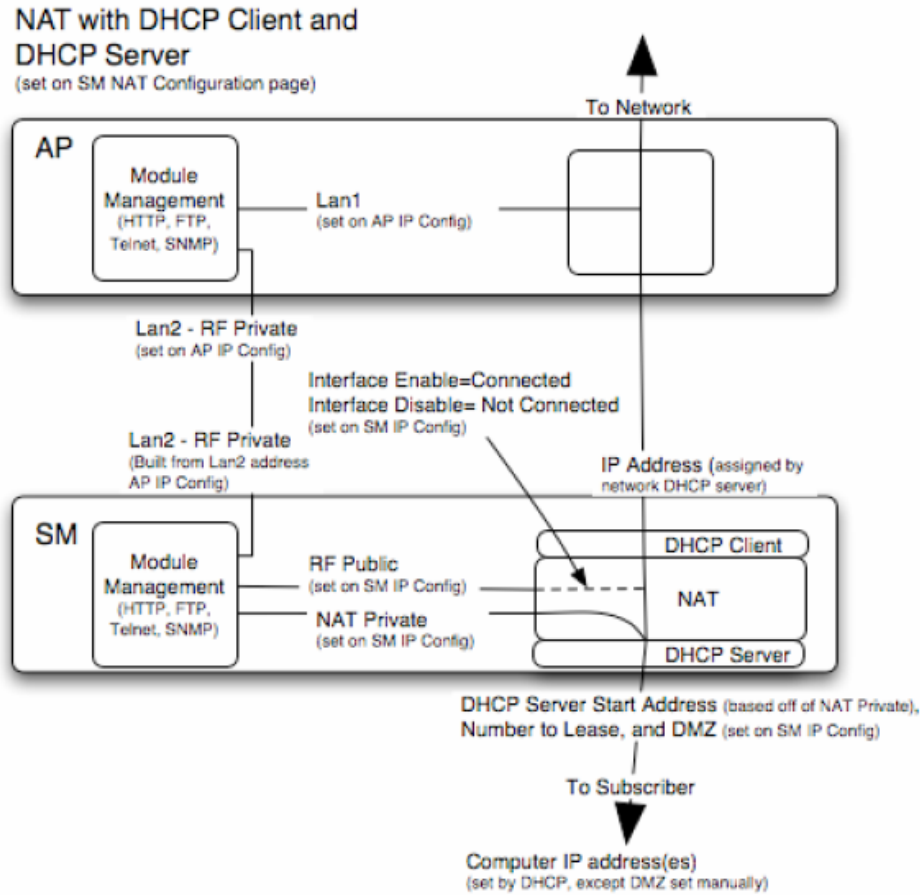


Figure 46: NAT with DHCP Client and DHCP Server implementation

NAT with DHCP Client

The NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface) implementation is illustrated in [Figure 47](#).

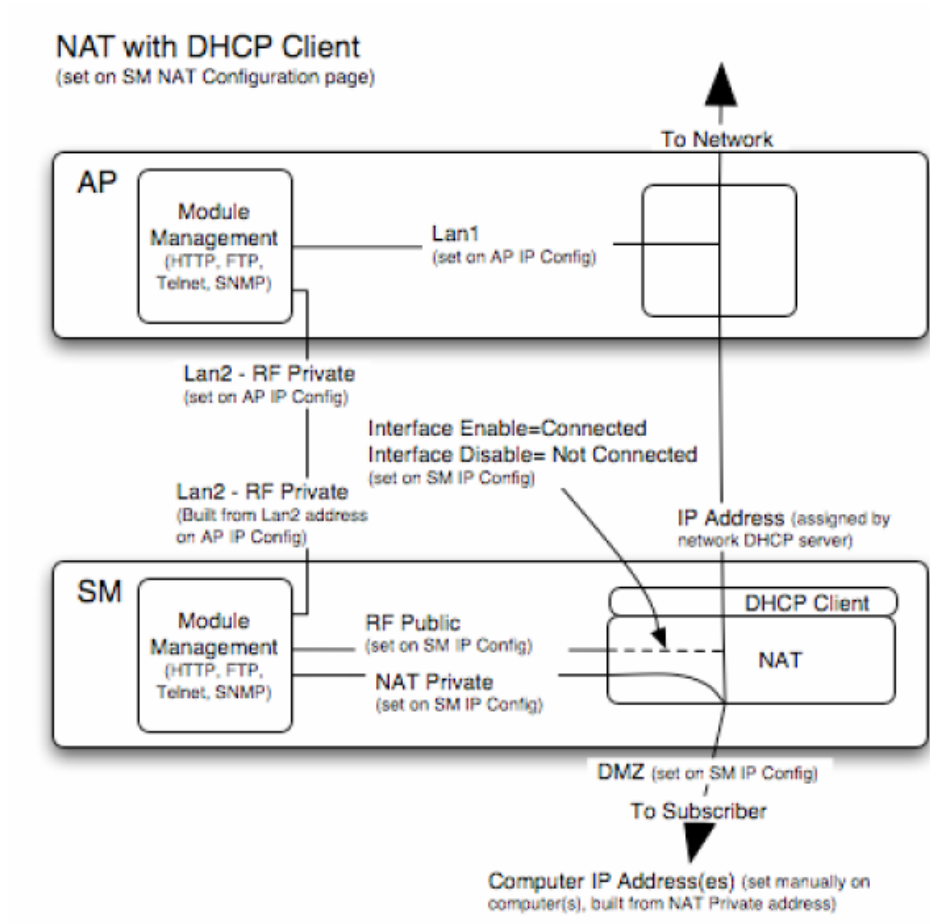


Figure 47: NAT with DHCP Client implementation

NAT with DHCP Server

The NAT with DHCP Server implementation is illustrated in [Figure 48](#).

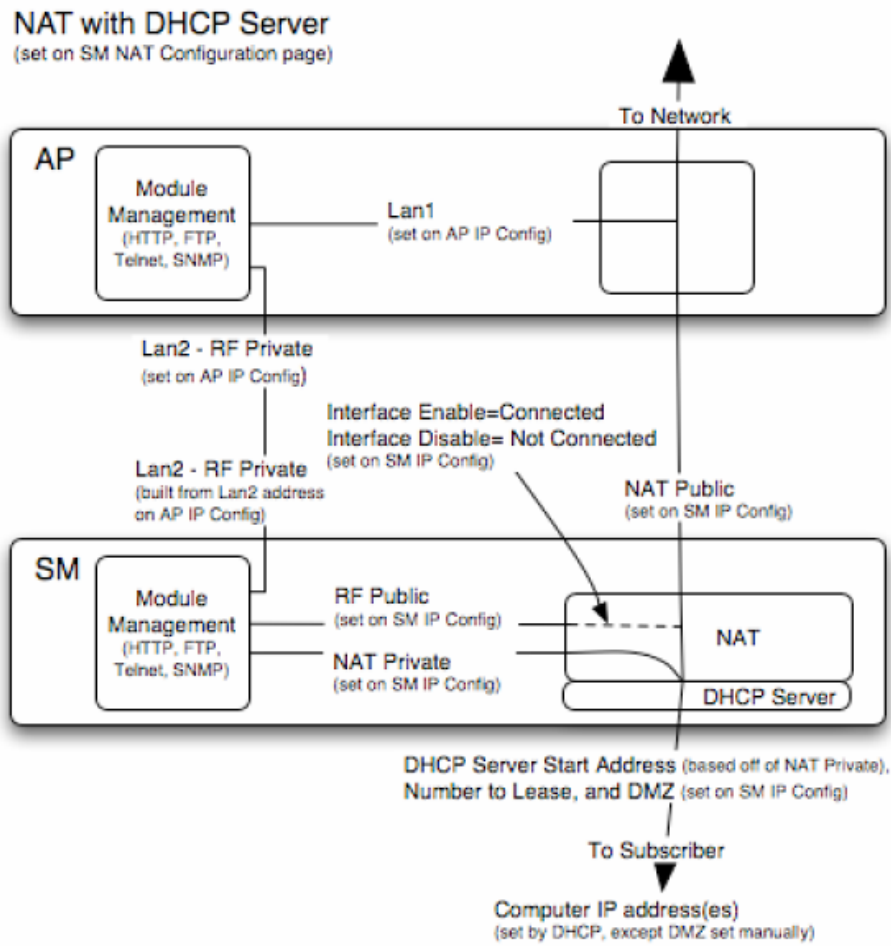


Figure 48: NAT with DHCP Server implementation

NAT without DHCP

The NAT without DHCP implementation is illustrated in [Figure 49](#).

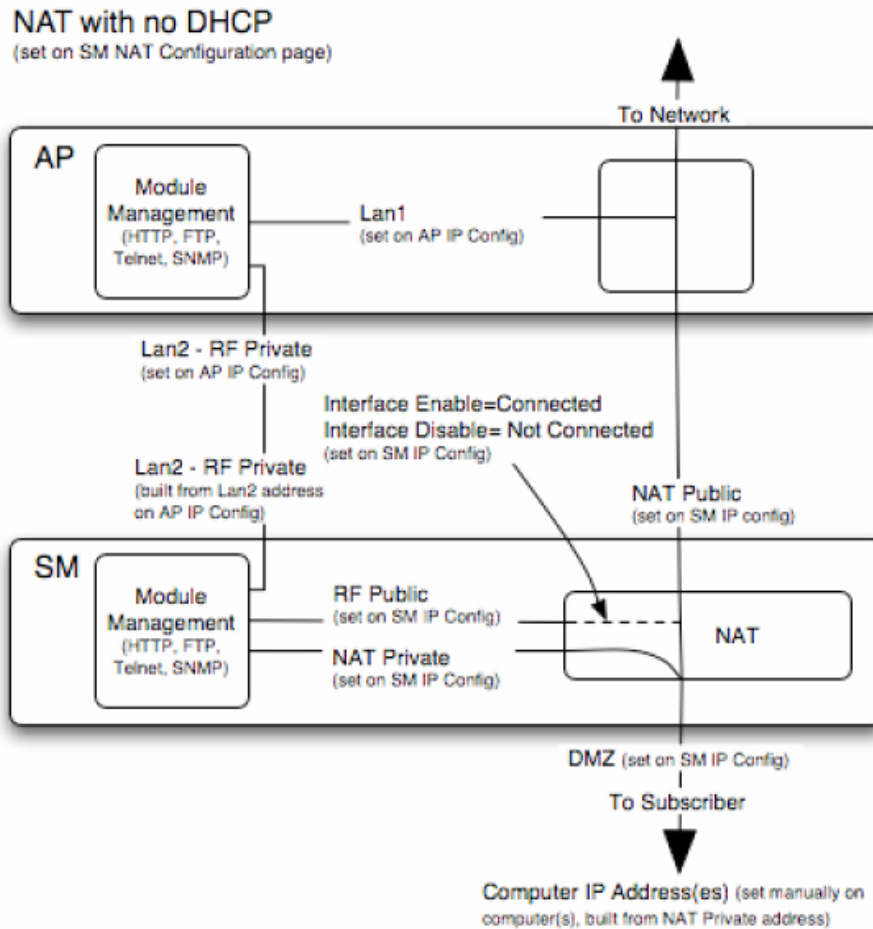


Figure 49: NAT without DHCP implementation

13.3.2 NAT and VPNs

VPN technology provides the benefits of a private network during communication over a public network. One typical use of a VPN is to connect remote employees, who are at home or in a different city, to their corporate network over the public Internet. Any of several VPN implementation schemes is possible. By design, NAT translates or changes addresses, and thus interferes with a VPN that is not specifically supported by a given NAT implementation.

With NAT enabled, SMs support L2TP over IPsec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs. With NAT disabled, SMs support all types of VPNs.

13.4 DEVELOPING AN IP ADDRESSING SCHEME

Network elements are accessed through IP Version 4 (IPv4) addressing. A proper IP addressing method is critical to the operation and security of a network.

Each module requires an IP address on the network. This IP address is for only management purposes. For security, you should either

- assign an unroutable IP address.
- assign a routable IP address only if a firewall is present to protect the module.

You will assign IP addresses to computers and network components by either *static* or *dynamic* IP addressing. You will also assign the appropriate subnet mask and network gateway to each module.

13.4.1 Address Resolution Protocol

As previously stated, the MAC address identifies a module in

- communications between modules.
- the data that modules store about each other.
- the data that BAM or Prizm applies to manage authentication and bandwidth.

The IP address is essential for data delivery through a router interface. Address Resolution Protocol (ARP) correlates MAC addresses to IP addresses.

For communications to outside the network segment, ARP reads the network gateway address of the router and translates it into the MAC address of the router. Then the communication is sent to MAC address (physical network interface card) of the router.

For each router between the sending module and the destination, this sequence applies. The ARP correlation is stored until the ARP cache times out.

13.4.2 Allocating Subnets

The subnet mask is a 32-bit binary number that filters the IP address. Where a subnet mask contains a bit set to 1, the corresponding bit in the IP address is part of the network address.

Example IP Address and Subnet Mask

In [Figure 50](#), the first 16 bits of the 32-bit IP address identify the network:

	Octet 1	Octet 2	Octet 3	Octet 4
IP address 169.254.1.1	10101001	11111110	00000001	00000001
Subnet mask 255.255.0.0	11111111	11111111	00000000	00000000

Figure 50: Example of IP address in Class B subnet

In this example, the network address is 169.254, and 2^{16} (65,536) hosts are addressable.

13.4.3 Selecting Non-routable IP Addresses

The factory default assignments for network elements are

- unique MAC address
- IP address of 169.254.1.1, except for an OFDM series BHM, whose IP address is 169.254.1.2 by default
- subnet mask of 255.255.0.0
- network gateway address of 169.254.0.0

For each radio and CMMmicro and CMM4, assign an IP address that is both consistent with the IP addressing plan for your network and cannot be accessed from the Internet. IP addresses within the following ranges are not routable from the Internet, regardless of whether a firewall is configured:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

You can also assign a subnet mask and network gateway for each CMMmicro and CMM4.

13.5 TRANSLATION BRIDGING

Optionally, you can configure the AP to change the source MAC address in every packet it receives from its SMs to the MAC address of the SM that bridged the packet, before forwarding the packet toward the public network. If you do, then

- not more than 10 IP devices at any time are valid to send data to the AP from behind the SM.
- the AP populates the Translation Table tab of its Statistics web page, displaying the MAC address and IP address of all the valid connected devices.
- each entry in the Translation Table is associated with the number of minutes that have elapsed since the last packet transfer between the connected device and the SM.
- if 10 are connected, and another attempts to connect
 - and no Translation Table entry is older than 255 minutes, the attempt is ignored.
 - and an entry is older than 255 minutes, the oldest entry is removed and the attempt is successful.
- the **Send Untranslated ARP** parameter in the General tab of the Configuration page can be
 - disabled, so that the AP will overwrite the MAC address in Address Resolution Protocol (ARP) packets before forwarding them.
 - enabled, so that the AP will forward ARP packets regardless of whether it has overwritten the MAC address.

This is the **Translation Bridging** feature, which you can enable in the General tab of the Configuration web page in the AP. When this feature is disabled, the setting of the **Send Untranslated ARP** parameter has no effect, because all packets are forwarded untranslated (with the source MAC address intact).

See [Address Resolution Protocol](#) on Page 166.

14 ENGINEERING VLANS

The radios support VLAN functionality as defined in the 802.1Q (*Virtual LANs*) specification, except for the following aspects of that specification:

- the following protocols:
 - Generic Attribute Registration Protocol (GARP) GARV
 - Spanning Tree Protocol (STP)
 - Multiple Spanning Tree Protocol (MSTP)
 - GARP Multicast Registration Protocol (GMRP)
- priority encoding (802.1P) before Release 7.0
- embedded source routing (ERIF) in the 802.1Q header
- multicast pruning
- flooding unknown unicast frames in the downlink

As an additional exception, the AP *does not* flood downward the unknown unicast frames to the SM.

A VLAN configuration in Layer 2 establishes a logical group within the network. Each computer in the VLAN, regardless of initial or eventual physical location, has access to the same data. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security.

14.1 SPECIAL CASE VLAN NUMBERS

This system handles special case VLAN numbers according to IEEE specifications:

VLAN Number	Purpose	Usage Constraint
0	These packets have 802.1p priority, but are otherwise handled as untagged.	Should not be used as a management VLAN.
1	Although not noted as special case by IEEE specifications, these packets identify traffic that was untagged upon ingress into the SM and should remain untagged upon egress. This policy is hard-coded in the AP.	Should not be used for system VLAN traffic.
4095	This VLAN is reserved for internal use.	Should not be used at all.

14.2 SM MEMBERSHIP IN VLANS

With the supported VLAN functionality, the radios determine bridge forwarding on the basis of not only the destination MAC address, but also the VLAN ID of the destination. This provides flexibility in how SMs are used:

- Each SM can be a member in its own VLAN.
- Each SM can be in its own broadcast domain, such that only the radios that are members of the VLAN can see broadcast and multicast traffic to and from the SM.

- The network operator can define a work group of SMs, regardless of the AP(s) to which they register.

PMP modules provide the VLAN frame filters that are described in [Table 41](#).

Table 41: VLAN filters in point-to-multipoint modules

Where VLAN is active, if this parameter value is selected ...	then a frame is discarded if...		because of this VLAN filter in the software:
	<i>entering the bridge/ NAT switch through...</i>		
	Ethernet...	TCP/IP...	
any combination of VLAN parameter settings	with a VID not in the membership table		Ingress
any combination of VLAN parameter settings		with a VID not in the membership table	Local Ingress
Allow Frame Types: Tagged Frames Only	with no 802.1Q tag		Only Tagged
Allow Frame Types: Untagged Frames Only	with an 802.1Q tag, regardless of VID		Only Untagged
Local SM Management: Disable in the SM, or All Local SM Management: Disable in the AP	with an 802.1Q tag and a VID in the membership table		Local SM Management
	<i>leaving the bridge/ NAT switch through...</i>		
	Ethernet...	TCP/IP...	
any combination of VLAN parameter settings	with a VID not in the membership table		Egress
any combination of VLAN parameter settings		with a VID not in the membership table	Local Egress

14.3 PRIORITY ON VLANS (802.1p)

The radios can prioritize traffic based on the eight priorities described in the IEEE 802.1p specification. When the high-priority channel is enabled on an SM, regardless of whether VLAN is enabled on the AP for the sector, packets received with a priority of 4 through 7 in the 802.1p field are forwarded onto the high-priority channel.

VLAN settings can also cause the module to convert received non-VLAN packets into VLAN packets. In this case, the 802.1p priority in packets leaving the module is set to the priority established by the DiffServ configuration.

If you enable VLAN, *immediately* monitor traffic to ensure that the results are as desired. For example, high-priority traffic may block low-priority.

For more information on the high priority channel, see [High-priority Bandwidth](#) on Page 89.

INSTALLATION AND CONFIGURATION GUIDE

15 AVOIDING HAZARDS

Use simple precautions to protect staff and equipment. Hazards include exposure to RF waves, lightning strikes, and power surges. This section specifically recommends actions to abate these hazards.

15.1 EXPOSURE SEPARATION DISTANCES

To protect from overexposure to RF energy, install the radios so as to provide and maintain the minimum separation distances shown in [Table 42](#) away from all persons.

Table 42: Exposure separation distances

Module Type	Minimum Separation Distance from Persons
FSK or OFDM module	20 cm (approx 8 in)
Module with Reflector Dish	1.5 m (approx 60 in or 5 ft)
Module with LENS	0.5 m (approx 20 in)
Antenna of connectorized 5.7-GHz AP	30 cm (approx 12 in)
Antenna of connectorized or integrated 900-MHz module	60 cm (24 in)
Indoor 900-MHz SM	10 cm (4 in)

At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.



NOTE:

These are conservative distances that include compliance margins. In the case of the reflector, the distance is even more conservative because the equation models the reflector as a point source and ignores its physical dimensions.

Section [15.1.1](#) and [Table 43](#) give details and discussion of the associated calculations.

15.1.1 Details of Exposure Separation Distances Calculations and Power Compliance Margins

Limits and guidelines for RF exposure come from:

- US FCC limits for the general population. See the FCC web site at <http://www.fcc.gov>, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See the Health Canada web site at <http://www.hc-sc.gc.ca/rpb> and Safety Code 6.

- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at <http://www.icnirp.de/> and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

The applicable power density exposure limits from the documents referenced above are

- 6 W/m² for RF energy in the 900-MHz frequency band in the US and Canada.
- 10 W/m² for RF energy in the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency bands.

Peak power density in the far field of a radio frequency point source is calculated as follows:

$$S = \frac{P \cdot G}{4 \pi d^2}$$

where

S = power density in W/m²

P = RMS transmit power capability of the radio, in W

G = total Tx gain as a factor, converted from dB

d = distance from point source, in m

$$d = \sqrt{\frac{P \cdot G}{4 \pi S}}$$

Rearranging terms to solve for distance yields

Table 43 shows calculated minimum separation distances *d*, recommended distances and resulting power compliance margins for each frequency band and antenna combination.

Table 43: Calculated exposure distances and power compliance margins

Band Range	Antenna	Variable			<i>d</i> (calculated)	Recommended Separation Distance	Power Compliance Margin
		<i>P</i>	<i>G</i>	<i>S</i>			
900 MHz	external	0.4 W (26 dBm)	10.0 (10 dB)	6 W/m ²	23 cm	60 cm (24 in)	7
	integrated	0.25 W (24 dBm)	15.8 (12 dB)	6 W/m ²	23 cm	60 cm (24 in)	7
	indoor, integrated	Simulation model used to estimate Specific Absorption Rate (SAR) levels				10 cm (4 in)	2
2.4 GHz	integrated	0.34 W (25 dBm)	6.3 (8 dB)	10 W/m ²	13 cm	20 cm (8 in)	2.3
	integrated plus reflector	0.34 W (25 dBm)	79.4 (19 dB)	10 W/m ²	46 cm	1.5 m (5 ft)	10

Band Range	Antenna	Variable			<i>d</i> (calculated)	Recommended Separation Distance	Power Compliance Margin
		<i>P</i>	<i>G</i>	<i>S</i>			
5.2 GHz	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m ²	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m ²	9 cm	1.5 m (5 ft)	279
	integrated plus LENS	0.025 W (14 dBm)	40 (16 dB)	10 W/m ²	9 cm	50 cm (12 in)	31
5.4 GHz	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m ²	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m ²	9 cm	1.5 m (5 ft)	279
	integrated plus LENS	0.020 W (13 dBm)	50 (17 dB)	10 W/m ²	9 cm	50 cm (12 in)	31
5.4 GHz OFDM	integrated	0.01 W (10 dBm)	50 (17 dB)	10 W/m ²	6 cm	20 cm (8 in)	10
5.7 GHz	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m ²	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.2 W (23 dBm)	316 (25 dB)	10 W/m ²	71 cm	1.5 m (5 ft)	4.5
	integrated plus LENS	0.2 W (23 dBm)	50 (17 dB)	10 W/m ²	28 cm	50 cm (12 in)	3.13

The Recommended Separation Distance provides significant compliance margin in all cases. To simplify exposure distances in this column, a module has the expressed separation distance regardless of whether it is retrofitted with a reflector or a LENS.

These are conservative distances:

- They are along the beam direction (the direction of greatest energy). Exposure to the sides and back of the module is significantly less.
- They satisfy sustained exposure limits for the general population (not just short term occupational exposure limits), with considerable margin.
- In the reflector cases, the calculated compliance distance *d* is greatly overestimated because the far-field equation models the reflector as a point source and neglects the physical dimension of the reflector.

15.2 GROUNDING THE EQUIPMENT

Effective lightning protection diverts lightning current safely to ground, Protective Earth (PE) ↓. It neither attracts nor prevents lightning strikes.



WARNING!

Lightning damage *is not* covered under the warranty. The recommendations in this guide give the installer the knowledge to protect the installation from the harmful effects of ESD and lightning.

These recommendations must be thoroughly and correctly performed. However, complete protection is neither implied or possible.

15.2.1 Grounding Infrastructure Equipment

To protect both your staff and your infrastructure equipment, implement lightning protection as follows:

- Observe all local and national codes that apply to grounding for lightning protection.
- Before you install your modules, perform the following steps:
 - Engage a grounding professional if you need to do so.
 - Install lightning arrestors to transport lightning strikes away from equipment. For example, install a lightning rod on a tower leg other than the leg to which you mount your module.
 - Connect your lightning rod to ground.
 - Use a 600SS Surge Suppressor on the Ethernet cable where the cable enters any structure. (Instructions for installing this surge suppressor are provided in [Procedure 21](#) on Page 348.)
- Install your modules at least 2 feet (0.6 meters) below the tallest point on the tower, pole, or roof.

15.2.2 Grounding SMs

This section provides lightning protection guidelines for SMs to satisfy the National Electrical Code (NEC) of the United States. The requirements of the NEC focus on the safety aspects of electrical shock to personnel and on minimizing the risk of fire at a dwelling. The NEC does not address the survivability of electronic products that are exposed to lightning surges.

The statistical incidence of current levels from lightning strikes is summarized in [Table 44](#).

Table 44: Statistical incidence of current from lightning strikes

Percentage of all strikes	Peak Current (amps)
<2	>140,000
25	>35,000
>50	>20,000
>80	>8,500

At peak, more than one-half of all surges due to direct lightning strikes exceed 20,000 amps. However, only one-quarter exceed 35,000 amps, and less than two percent exceed 140,000 amps. Thus, the recommended Surge Suppressor provides a degree of lightning protection to electronic devices inside a dwelling.

Summary of Grounding Recommendations

Motorola recommends that you ground each SM as follows:

- Extend the SM mounting bracket extend to the top of the SM or higher.
- Ground the SM mounting bracket via a 10-AWG (6 mm²) copper wire connected by the most direct path either to an eight foot-deep ground rod or to the ground bonding point of the AC power service utility entry. This provides the best assurance that
 - lightning takes the ground wire route
 - the ground wire does not fuse open
 - your grounding system complies with NEC 810-15.
- Ground the surge suppressor ground lug to the same ground bonding point as above, using at least a 10-AWG (6 mm²) copper wire. This provides the best assurance that your grounding system complies with NEC 810-21.

Grounding Scheme

The proper overall antenna grounding scheme per the NEC is illustrated in [Figure 136](#) on [Page 349](#). In most television antenna or dish installations, a coaxial cable connects the outdoor electronics with the indoor electronics. To meet NEC 810-20, one typically uses a coaxial cable feed-through block that connects the outdoor coax to the indoor coax and also has a screw for attaching a ground wire. This effectively grounds the outer shield of the coax. The block should be mounted on the outside of the building near the AC main panel such that the ground wire of the block can be bonded to the primary grounding electrode system of the structure.

For residential installs, in most cases an outdoor rated *unshielded* twisted pair (UTP) cable is sufficient. To comply with the NEC, Motorola provides the antenna discharge unit, 600SS, for each conductor of the cable. The surge suppressor must be

- positioned
 - outside the building.
 - as near as practicable to the power service entry panel of the building and attached to the AC main power ground electrode, or attached to a grounded water pipe.⁵
 - far from combustible material.
- grounded in accordance with NEC 810-21, with the grounding wire attached to the screw terminal.

The metal structural elements of the antenna mast also require a separate grounding conductor. Section 810-15 of the NEC states:

Masts and metal structures supporting antennas shall be grounded in accordance with Section 810-21.

⁵ It is *insufficient* to merely use the green wire ground in a duplex electrical outlet box for grounding of the antenna discharge unit.

As shown in [Figure 136](#) on [Page 349](#), the Motorola recommendation for grounding the metal structural element of the mounting bracket (SMMB1) is to route the grounding wire from the SMMB1 down to the same ground attachment point as is used for the 600SS discharge unit.

Use 10-AWG (6 mm²) Copper Grounding Wire

According to NEC 810-21 3(h), either a 16-AWG copper clad steel wire or a 10-AWG copper wire may be used. This specification appears to be based on mechanical strength considerations and *not* on lightning current handling capabilities.

For example, analysis shows that the two wire types are not equivalent when carrying a lightning surge that has a 1-microsecond rise by 65-microsecond fall:

- The 16-AWG copper clad steel wire has a peak fusing current of 35,000 amps and can carry 21,000 amps peak, at a temperature just below the ignition point for paper (454° F or 234° C).
- The 10-AWG copper wire has a peak fusing current of 220,000 amps and can carry 133,000 amps peak, at the same temperature.

Based on the electrical/thermal analysis of these wires, Motorola recommends 10-AWG copper wire for *all* grounding conductors. Although roughly double the cost of 16-AWG copper clad steel wire, 10-AWG copper wire handles six times the surge current from lightning.

Shielding is not Grounding

In part, NEC 810-21 states:

A lightning arrester is not required if the lead-in conductors are enclosed in a continuous metal shield, such as rigid or intermediate metal conduit, electrical metallic tubing, or any metal raceway or metal-shielded cable that is effectively grounded. A lightning discharge will take the path of lower impedance and jump from the lead-in conductors to the metal raceway or shield rather than take the path through the antenna coil of the receiver.

However, Motorola does not recommend relying on shielded twisted pair cable for lightning protection for the following reasons:

- Braid-shielded 10Base-T cable is uncommon, if existent, and may be unsuitable anyway.
- At a cost of about two-thirds more than 10-AWG copper UTP, CAT 5 100Base-TX foil-shielded twisted pair (FTP) cable provides a 24-AWG drain wire. If this wire melts open during a lightning surge, then the current may follow the twisted pair into the building.

More than 80 percent of all direct lightning strikes have current that exceeds 8,500 amps (see [Table 44](#) on [Page 176](#)). A 24-AWG copper wire melts open at 8,500 amps from a surge that has a 1-microsecond by 70-microsecond waveform. Hence, reliance on 24-AWG drain wire to comply with the intent of NEC 810-21 is questionable.

Shielded twisted pair cable may be useful for mitigation of interference in some circumstances, but installing surge suppressors and implementing the ground recommendations constitute the most effective mitigation against lightning damage.

Grounding PMP 400 SMs

PMP 54400 APs and SMs and PTP 54200 BHs use a nominal 30-V DC power system with power on Pins 7 and 8 and return on Pins 4 and 5. PMP 54400 APs and PTP 54200 BHs can be powered from either a CMMmicro with a 30-V DC power supply or a CMM4 with a 30-V DC power supply. A 29.5-V DC power supply is available for PMP 54400 SMs.

In contrast, PMP 49400 APs and SMs and PTP 49200 BHs use a nominal 56-V DC power system with power on Pins 5 and 8 and return on Pins 4 and 7. PMP 49400 APs and PTP 49200 BHs *must* use a CMM4 with a 56-V DC power supply. A CMMmicro *will not* power these units, because it provides the wrong voltage on the wrong pins. A 56-V DC power supply is available for PMP 49400 SMs.



IMPORTANT!

When working on sites with both power systems, use care to not wrongly mix power supplies and radios, because the two power systems use different pinout schemes and require different voltages.

On a site where you are deploying a mix of 30-V DC and 56-V DC radios (to the limit of 8 radios supported by one CMM), you can use a CMM4 that is connected to both a 30-V DC power supply and a 56-V DC power supply.

Due to the full metallic connection to the tower or support structure through the AP antenna or a connectorized BH antenna, grounding the AP or BH and installing a 600SS surge suppressor within 3 ft (1 m) of the AP or BH is *strongly recommended*. This suppresses overvoltages and overcurrents, such as those caused by near-miss lightning. APs and BHs provide a grounding lug for grounding to the tower or support structure. A pole mount kit is available for the 600SS. The pole mount kit provides a grounding point on one of its U-bolts that can be used for terminating ground straps from both the 600SS and the AP.

NEC Reference

NEC Article 810, *Radio and Television Equipment*, and associated documents and discussions are available from <http://www.neccode.com/index.php?id=homegeneral>, <http://www.constructionbook.com/xq/ASP/national-electrical-code-2005/id.370/subID.746/qx/default2.htm>, and other sources.

15.3 CONFORMING TO REGULATIONS

For all electrical purposes, ensure that your network conforms to applicable country and local codes, such as the NEC (National Electrical Code) in the US. If you are uncertain of code requirements, engage the services of a licensed electrician.

15.4 PROTECTING CABLES AND CONNECTIONS

Cables that move in the wind can be damaged, impart vibrations to the connected device, or both. At installation time, prevent these problems by securing all cables with cable ties, cleats, or PVC tape.

Over time, moisture can cause a cable connector to fail. You can prevent this problem by

- using cables that are filled with a dielectric gel or grease.
- including a drip loop where the cable approach to the module (typically a CMM) is from above.
- wrapping the cable with weather-resistant tape.

On a module with an external antenna, use accepted industry practices to wrap the connector to prevent water ingress. Although the male and female N-type connectors form a gas-tight seal with each other, the point where the cable enters each connector can allow water ingress and eventual corrosion. Wrapping and sealing is critical to long-term reliability of the connection.

Possible sources of material to seal that point include

- the antenna manufacturer (material may have been provided in the package with the antenna).
- Universal Electronics (whose web site is <http://www.coaxseal.com>), who markets a weather-tight wrap named Coax-Seal.

Perform the following steps to wrap the cable.

Procedure 4: Wrapping the cable

1. Start the wrap on the cable 0.5 to 2 inches (about 1.5 to 5 cm) from the connection.
2. Wrap the cable to a point 0.5 to 2 inches (about 1.5 to 5 cm) above the connection.
3. Squeeze the wrap to compress and remove any trapped air.
4. Wrap premium vinyl electrical tape over the first wrap where desired for abrasion resistance or appearance.
5. Tie the cable to minimize sway from wind.

===== end of procedure =====

16 TESTING THE COMPONENTS

The best practice is to connect all components—BHs, APs, GPS antenna, and CMM—in a test setting and initially configure and verify them before deploying them to an installation. In this way, any configuration issues are worked out before going on-site, on a tower, in the weather, where the discovery of configuration issues or marginal hardware is more problematic and work-flow affecting.

16.1 UNPACKING COMPONENTS

When you receive these products, carefully inspect all shipping boxes for signs of damage. If you find damage, immediately notify the transportation company.

As you unpack the equipment, verify that all the components that you ordered have arrived. Save all the packing materials to use later, as you transport the equipment to and from installation sites.

16.2 CONFIGURING FOR TEST

You can use either of two methods to configure an AP or BHM:

- Use the Quick Start feature of the product. For more information on Quick Start, see [Quick Start Page of the AP](#) on Page 187.
- Manually set each parameter.

After you change configuration parameters on a GUI web page:

1. Before you leave a web page, click the **Save** button to save the change(s).
2. After making change(s) on multiple web pages, click the **Reboot** button to reboot the module and implement the change(s).

16.2.1 Configuring the Computing Device for Test

If your computer is configured for Dynamic Host Configuration Protocol (DHCP), disconnect the computer from the network. If your computer is instead configured for static IP addressing

- set the static address in the 169.254 network
- set the subnet mask to 255.255.0.0.

16.2.2 Default Module Configuration

From the factory, the AP, SM, and BH are all configured to *not transmit* on any frequency. This configuration ensures that you do not accidentally turn on an unsynchronized module. Site synchronization of modules is required because

- modules
 - cannot transmit and receive signals at the same time.
 - use TDD (Time Division Duplexing) to distribute signal access of the downlink and uplink frames.
- when one module transmits while an unintended module nearby receives signal, the transmitting module may interfere with or desense the receiving module. In this context, interference is self-interference (within the same network).

16.2.3 Component Layout

As shown in [Figure 51](#), the base cover of the module snaps off when you depress a lever on the back of the base cover. This exposes the Ethernet and GPS sync connectors and diagnostic LEDs.

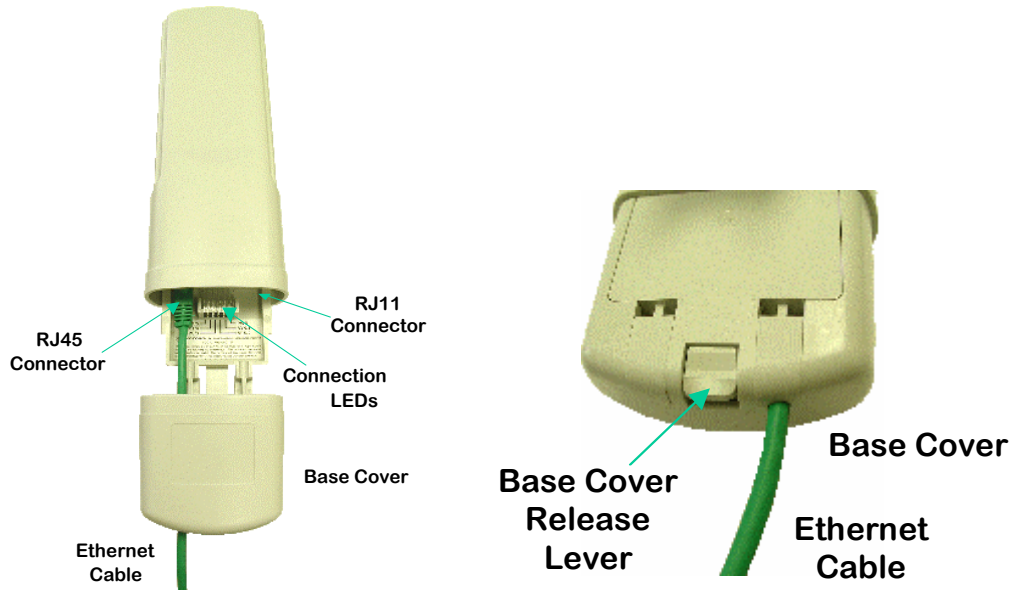


Figure 51: Base cover, detached and attached, FSK module

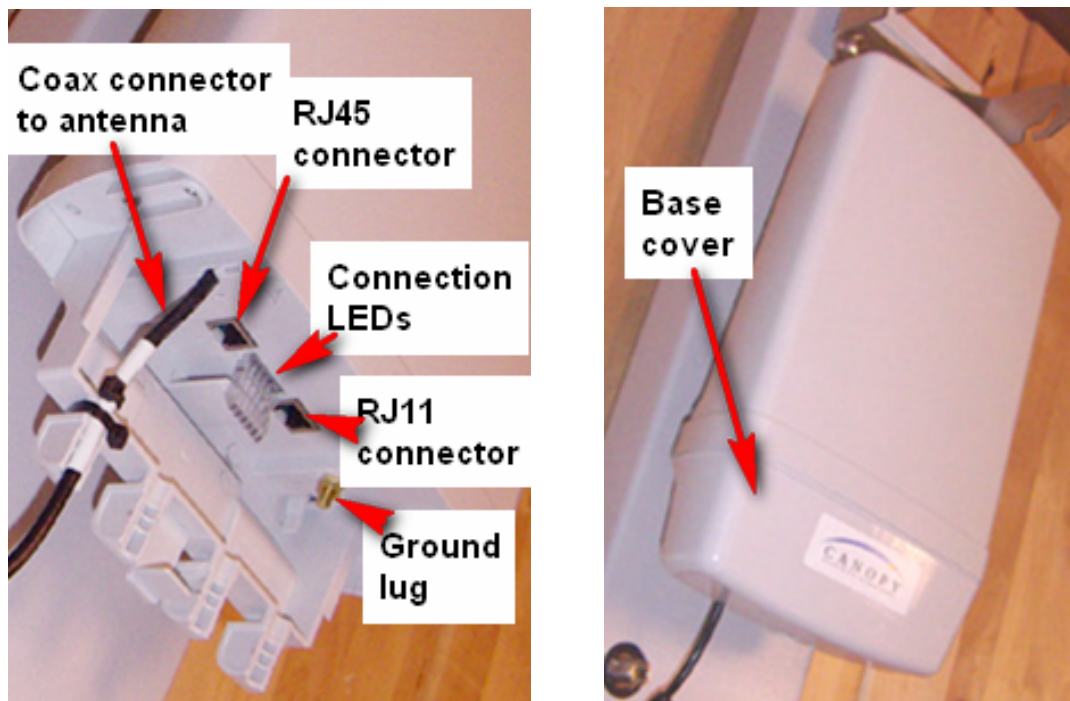


Figure 52: Base cover, detached and attached, OFDM module

16.2.4 Diagnostic LEDs

The diagnostic LEDs report the following information about the status of the module. [Table 45](#) and [Table 46](#) identify the LEDs in order of their left-to-right position as the cable connections face downward.



NOTE:

The LED color helps you distinguish position of the LED. The LED color *does not* indicate any status.

Table 45: LEDs in AP and BHM

Label	Color when Active	Status Information Provided	Notes
LNK/5	green	Ethernet link	Continuously lit when link is present.
ACT/4	yellow	Presence of data activity on the Ethernet link	Flashes during data transfer. Frequency of flash is not a diagnostic indication.
GPS/3	red	Pulse of sync	Continuously lit as pulse as AP receives pulse.
SES/2	green	<i>Unused on the AP</i>	SES is the session indicator on the CMM.
SYN/1	yellow	Presence of sync	Always lit on the AP.
PWR	red	DC power	Always lit when power is correctly supplied.

Table 46: Legacy Mode LEDs in SM and BHS

Label	Color when Active	Status if Registered	Notes	
			Operating Mode	Aiming Mode
LNK/5	green	Ethernet link	Continuously lit when link is present.	These five LEDs act as a bar graph to indicate the relative quality of alignment. As power level and jitter (if present) improve during alignment, more of these LEDs are lit.
ACT/4	yellow	Presence of data activity on the Ethernet link	Flashes during data transfer. Frequency of flash is not a diagnostic indication.	
GPS/3	red	<i>Unused</i>	If this module is not registered to another, then these three LEDs cycle on and off from left to right.	
SES/2	green	<i>Unused</i>		
SYN/1	yellow	Presence of sync		
PWR	red	DC power	Always lit when power is correctly supplied.	Always lit when power is correctly supplied.

An optional light scheme configurable in all FSK SMs supports end customers who install the SM (for example, the 9000SMQ indoor SM) on their own premises. The scheme uses the LEDs and labels listed in [Table 46](#) above, but is based on the traffic signal light

analogy: green is good, yellow is okay, and red is bad. This scheme can also be useful in some settings and workflows for outdoor SMs. As with Legacy mode, while the SM is scanning, the green, yellow, and red LEDs blink in sequence.

Table 47: Revised Mode LEDs in SM

Label	Color	Revised Mode Indication
LNK/5	green	<i>Link.</i>
ACT/4	yellow	<i>Activity.</i>
GPS/3	red	<i>Interference (Jitter)</i> On - high interference. Blinking - medium interference. Off - low interference.
SES/2	green	<i>Strong Receive Signal Power</i> Blinking from slow to full-on to indicate strong power, getting stronger.
SYN/1	yellow	<i>Medium Receive Signal Power</i> Blinking from slow to full-on to indicate medium power, getting stronger.
PWR	red	<i>Not Registered</i> Off when registered to AP. On when not registered to AP.

To configure an SM into the Revised Mode, see [LED Panel Mode](#) on Page 291.

16.2.5 Standards for Wiring

Modules automatically sense whether the Ethernet cable in a connection is wired as straight-through or crossover. You may use either straight-through or crossover cable to connect a network interface card (NIC), hub, router, or switch to these modules. For a straight-through cable, use the EIA/TIA-568B wire color-code standard on both ends. For a crossover cable, use the EIA/TIA-568B wire color-code standard on one end, and the EIA/TIA-568A wire color-code standard on the other end.

Where you use the AC wall adapter

- the power supply output is +24 VDC.
- the power input to the SM is +11.5 VDC to +30 VDC.
- the maximum Ethernet cable run is 328 feet (100 meters).

16.2.6 Best Practices for Cabling

The following practices are essential to the reliability and longevity of cabled connections:

- Use only shielded cables to resist interference.
- For vertical runs, provide cable support and strain relief.
- Include a 2-ft (0.6-m) service loop on each end of the cable to allow for thermal expansion and contraction and to facilitate terminating the cable again when needed.
- Include a drip loop to shed water so that most of the water does not reach the connector at the device.
- Properly crimp all connectors.

- Use dielectric grease on all connectors to resist corrosion.
- Use only shielded connectors to resist interference and corrosion.

16.2.7 Recommended Tools for Wiring Connectors

The following tools may be needed for cabling the AP:

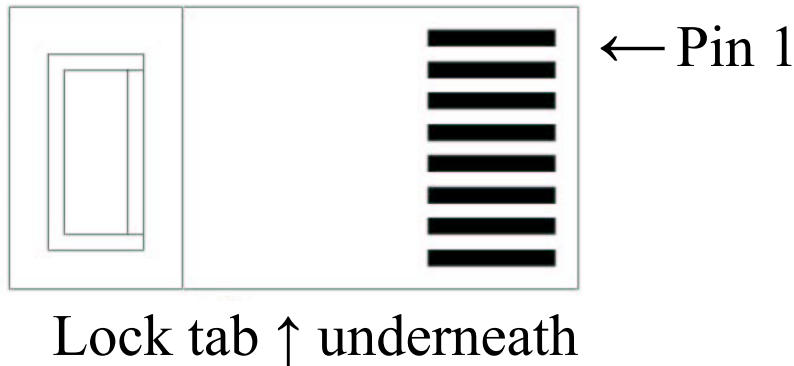
- RJ-11 crimping tool
- RJ-45 crimping tool
- electrician scissors
- wire cutters
- cable testing device.

16.2.8 Wiring Connectors

The following diagrams correlate pins to wire colors and illustrate crossovers where applicable.

Location of Pin 1

Pin 1, relative to the lock tab on the connector of a straight-through cable is located as shown below.



RJ-45 Pinout for Straight-through Ethernet Cable

- Pin 1 → white / orange ← Pin 1 Pin 2
- orange ← Pin 2
- Pin 3 → white / green ← Pin 3
- Pin 4 → blue ← Pin 4
- Pin 5 → white / blue ← Pin 5
- Pin 6 → green ← Pin 6
- Pin 7 → white / brown ← Pin 7
- Pin 8 → brown ← Pin 8
- Pins 7 and 8 carry power to the modules.

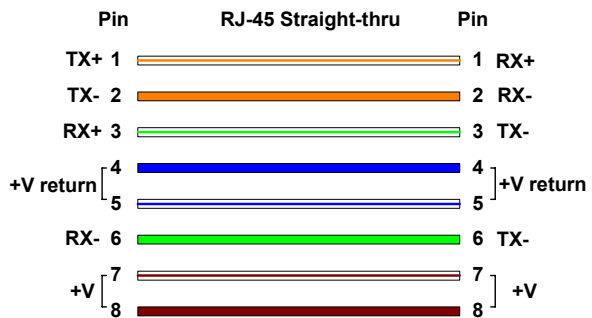


Figure 53: RJ-45 pinout for straight-through Ethernet cable

RJ-45 Pinout for Crossover Ethernet Cable

Pin 1 → white / orange ← Pin 3
 Pin 2 → orange ← Pin 6
 Pin 3 → white / green ← Pin 1
 Pin 4 → blue ← Pin 4
 Pin 5 → white / blue ← Pin 5
 Pin 6 → green ← Pin 2
 Pin 7 → white / brown ← Pin 7
 Pin 8 → brown ← Pin 8
 Pins 7 and 8 carry power to the modules.

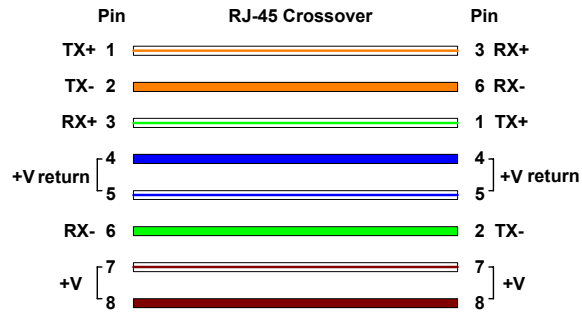


Figure 54: RJ-45 pinout for crossover Ethernet cable

RJ-11 Pinout for Straight-through Sync Cable

The system uses a utility cable with RJ-11 connectors between the AP or BH and synchronization pulse. Presuming CAT 5 cable and 6-pin RJ-11 connectors, the following diagram shows the wiring of the cable for sync.

Pin 1 → white / orange ← Pin 1
 Pin 2 → white / green ← Pin 2
 Pin 3 → white / blue ← Pin 3
 Pin 4 → green ← Pin 4
 Pin 5 → blue ← Pin 5
 Pin 6 → orange ← Pin 6
NOTE: The fourth pair is not used.

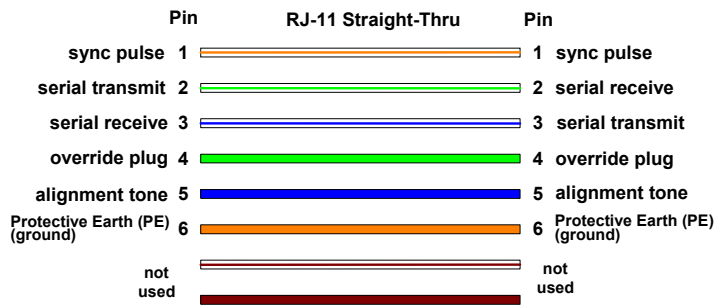


Figure 55: RJ-11 pinout for straight-through sync cable

16.2.9 Alignment Tone—Technical Details

The alignment tone output from a module is available on Pin 5 of the RJ-11 connector, and ground is available on Pin 6. Thus the load at the listening device should be between Pins 5 and 6. The listening device may be a headset, earpiece, or battery-powered speaker.

16.3 CONFIGURING A POINT-TO-MULTIPOINT LINK FOR TEST

Perform the following steps to begin the test setup.

Procedure 5: Setting up the AP for Quick Start

1. In one hand, securely hold the top (larger shell) of the AP. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the AP.

3. Plug the Ethernet cable connector labeled To Radio into the jack in the pig tail that hangs from the power supply.

**WARNING!**

From this point until you remove power from the AP, stay at least as far from the AP as the minimum separation distance specified in [Table 42](#) on Page 173.

4. Plug the other connector of the pig tail (this connector labeled To Computer) into the Ethernet jack of the computing device.
5. Plug the power supply into an electrical outlet.
6. Power up the computing device.
7. Start the browser in the computing device.

===== end of procedure =====

The AP interface provides a series of web pages to configure and monitor the unit. You can access the web-based interface through a computing device that is either directly connected or connected through a network to the AP. If the computing device is not connected to a network when you are configuring the module in your test environment, and if the computer has used a proxy server address and port to configure a module, then you may need to first disable the proxy setting in the computer.

Perform the following procedure to toggle the computer to *not* use the proxy setting.

Procedure 6: Bypassing proxy settings to access module web pages

1. Launch Microsoft Internet Explorer.
2. Select **Tools**→**Internet Options**→**Connections**→**LAN Settings**.
3. Uncheck the **Use a proxy server...** box.

NOTE: If you use an alternate web browser, the menu selections differ from the above.

===== end of procedure =====

In the address bar of your browser, enter the IP address of the AP. (For example, enter `http://169.254.1.1` to access the AP through its default IP address). The AP responds by opening the General Status tab of its Home page.

16.3.1 Quick Start Page of the AP

To proceed with the test setup, click the **Quick Start** button on the left side of the General Status tab. The AP responds by opening the Quick Start page. The Quick Start tab of that page is displayed in [Figure 56](#).

**NOTE:**

If you cannot find the IP address of the AP, see [Override Plug](#) on Page 65.

The screenshot displays the 'Quick Start' configuration wizard for an AP. The breadcrumb trail at the top includes: Quick Start, Region Settings, Radio Carrier Frequency, Synchronization, LAN IP Address, and Review and Save Configuration. The main content area is titled 'Quick Start => Quick Start' and '2.4GHz - Access Point - 0a-00-3e-23-20-66'. A blue header bar reads 'Welcome to the Canopy Quick Start Configuration Wizard'. The main text explains that the Canopy system consists of highly flexible fixed wireless access devices and that the wizard will guide the user through configuration. It lists three required parameters: RF Carrier Frequency, Synchronization, and Network IP Address. Below this, it states that these are the only parameters to be configured and that the user will be asked for choices that best address their network needs. At the end, the user will be given the opportunity to review the configuration and save it to non-volatile memory. A final paragraph notes that Canopy is a highly flexible system that can be used to build networks ranging from very simple to very sophisticated. A 'Go To Next Page=>' button is located at the bottom of the main content area.

Figure 56: Quick Start tab of AP, example

Quick Start is a wizard that helps you to perform a basic configuration that places an AP into service. Only the following parameters must be configured:

- **Region Code**
- **RF Carrier Frequency**
- **Synchronization**
- **LAN (Network) IP Address**

In each Quick Start tab, you can

- specify the settings to satisfy the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Proceed with the test setup as follows.

Procedure 7: Using Quick Start to configure a standalone AP for test

1. At the bottom of the Quick Start tab, click the **Go To Next Page =>** button.
RESULT: The AP responds by opening the Region Settings tab. An example of this tab is shown in [Figure 57](#).

The screenshot shows a web-based configuration interface for an AP. On the left is a navigation menu with options: Home, Configuration, Statistics, Tools, Account, Quick Start, Copyright, and Logoff. Below the menu, it displays 'Account: admin', 'Level: ADMINISTRATOR'. The main content area has a breadcrumb trail: Quick Start | Region Settings | Radio Carrier Frequency | Synchronization | LAN IP Address | Review and Save Configuration. The current page title is 'Quick Start => Region Settings' for '2.4GHz - Access Point - 0a-00-3e-23-20-66'. There are two expandable sections: 'Region Settings Descriptions' and 'Regional Settings'. The 'Regional Settings' section contains a 'Region Code' dropdown menu currently set to 'United States'. At the bottom are two buttons: '<=>Go To Previous Page' and 'Go To Next Page=>'.

Figure 57: Region Settings tab of AP, example

2. From the pull-down menu, select the region in which the AP will operate.

3. Click the **Go To Next Page =>** button.
RESULT: The AP responds by opening the Radio Carrier Frequency tab.
 An example of this tab is shown in [Figure 58](#).

Quick Start Configuration | Region Settings | **Radio Carrier Frequency** | Synchronization | LAN IP Address | Review and Save

Quick Start => Radio Carrier Frequency

2.4GHz - Access Point - 0a-00-3e-23-20-66

Radio Carrier Frequency

To communicate, each Access Point (AP) and Backhaul (BH) timing master must be assigned a specific carrier frequency. By default, this frequency is not set at the factory to ensure that new units do not accidentally transmit on an unintended frequency. For our purposes, frequency selection has two basic rules:

1. Frequencies should be separated by **at least** 20 MHz (4 MHz for 900 MHz radios)
2. Two radios located at a single location (such as an AP cluster) and on the same frequency should not have an overlapping pattern

We recommend multipoint AP clusters use frequencies separated by 25 MHz (9 MHz for 900 MHz radios) where convenient. For a 360 degree multipoint AP, each frequency is used twice with the back-to-back units sharing the same frequency.

Direction of Access Point Radio	Frequency	Sector ID	Symbol
North	2415.0 MHz	0	A
Northeast	2435.0 MHz	1	B
Southeast	2455.0 MHz	2	C
South	2415.0 MHz	0	A
Southwest	2435.0 MHz	1	B
Northwest	2455.0 MHz	2	C

AP Carrier Frequency Parameter

Please select Carrier Frequency from the list :

<-Go To Previous Page | Go To Next Page=>

Figure 58: Radio Carrier Frequency tab of AP, example

4. From the pull-down menu, select a frequency for the test.
5. Click the **Go To Next Page =>** button.
RESULT: The AP responds by opening the Synchronization tab. An example of this tab is shown in [Figure 59](#).

Quick Start | Region Settings | Radio Carrier Frequency | **Synchronization** | LAN IP Address | Review and Save

Quick Start => Synchronization

2.4GHz - Access Point - 0a-00-3e-23-20-66

Synchronization

When any radio transmits, it radiates energy. If a nearby radio is trying to receive at the same time another is transmitting, interference can result. One of the mechanisms used by Canopy to avoid this issue is to synchronize all transmissions. This approach ensures that all Canopy units will transmit and receive during the same time interval.

To accomplish this, Canopy Cluster Management Module's (CMM) each contain a GPS radio; this radio is used to create a precision timing signal which is then used by the attached APs/BHs. For systems that have only one AP/BH timing master location, this signal can be simulated. For systems that have multiple AP/BH timing master locations, an external CMM GPS signal should be used. Selecting "Generate Sync Signal" causes that AP/BH timing master to output a simulated GPS signal.

Each AP/BH timing master must be programmed to either generate its own synchronization pulse (for single AP/BH use only) or to use an external pulse. If you are using a CMM or other source of synchronization timing, you should select "Sync to Received Signal"; if not, you should select "Generate Sync Signal". There are two ports on the AP/BH timing master from which to receive the synchronization pulse: 1) The Power Port, 2) The Timing Port. By selecting the power port, only one cable is necessary to the AP/BH timing master to obtain power and the synchronization pulse. If the timing port is selected, two cables will be necessary to the AP/BH timing master to obtain power and the synchronization pulse.

Please be aware that operating multiple APs/BHs without an external GPS timing source may lead to degraded system operation.

Synchronization Parameters

Synchronization :

<=Go To Previous Page Go To Next Page=>

Figure 59: Synchronization tab of AP, example

6. At the bottom of this tab, select **Generate Sync Signal**.
7. Click the **Go To Next Page =>** button.
RESULT: The AP responds by opening the LAN IP Address tab. An example of this tab is shown in [Figure 60](#).

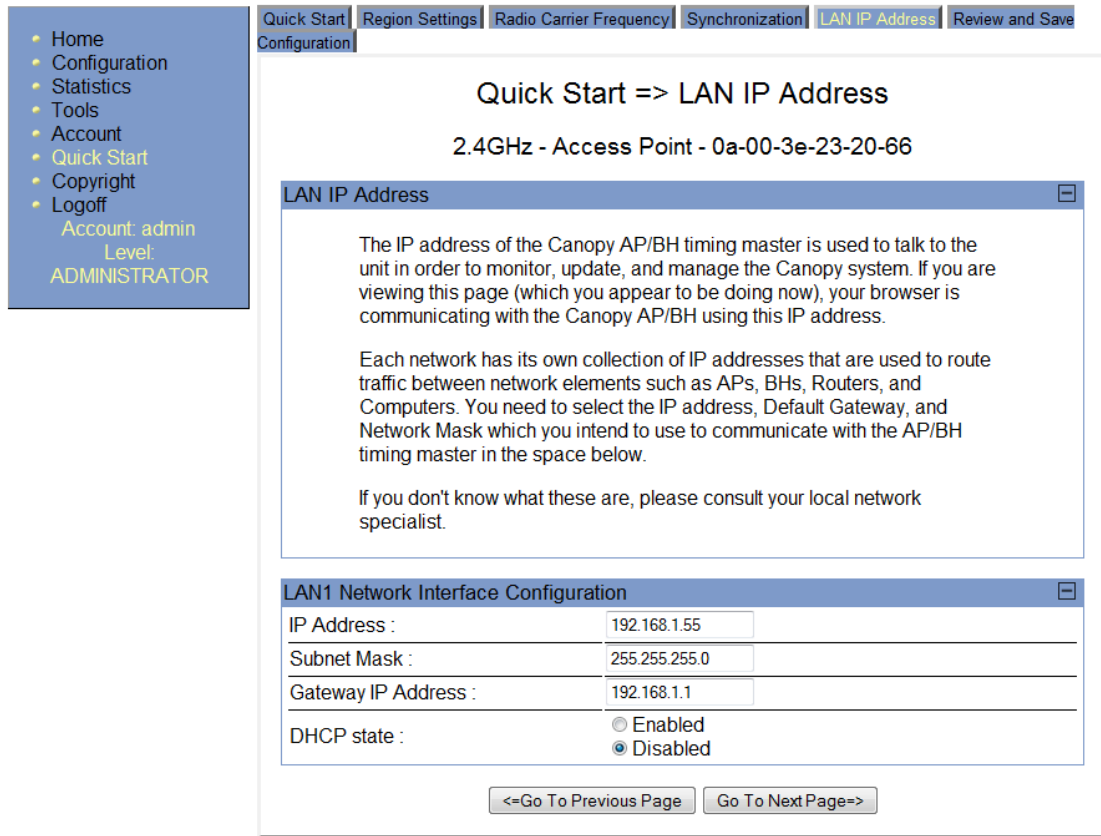


Figure 60: LAN IP Address tab of AP, example

8. At the bottom of this tab, either
 - specify an **IP Address**, a **Subnet Mask**, and a **Gateway IP Address** for management of the AP and leave the **DHCP state** set to **Disabled**.
 - set the **DHCP state** to **Enabled** to have the IP address, subnet mask, and gateway IP address automatically configured by a domain name server (DNS).



NOTE:

Motorola encourages you to experiment with the interface. Unless you save a configuration and reboot the AP after you save the configuration, none of the changes are effected.

9. Click the **Go To Next Page =>** button.
RESULT: The AP responds by opening the Review and Save Configuration tab. An example of this tab is shown in [Figure 61](#).

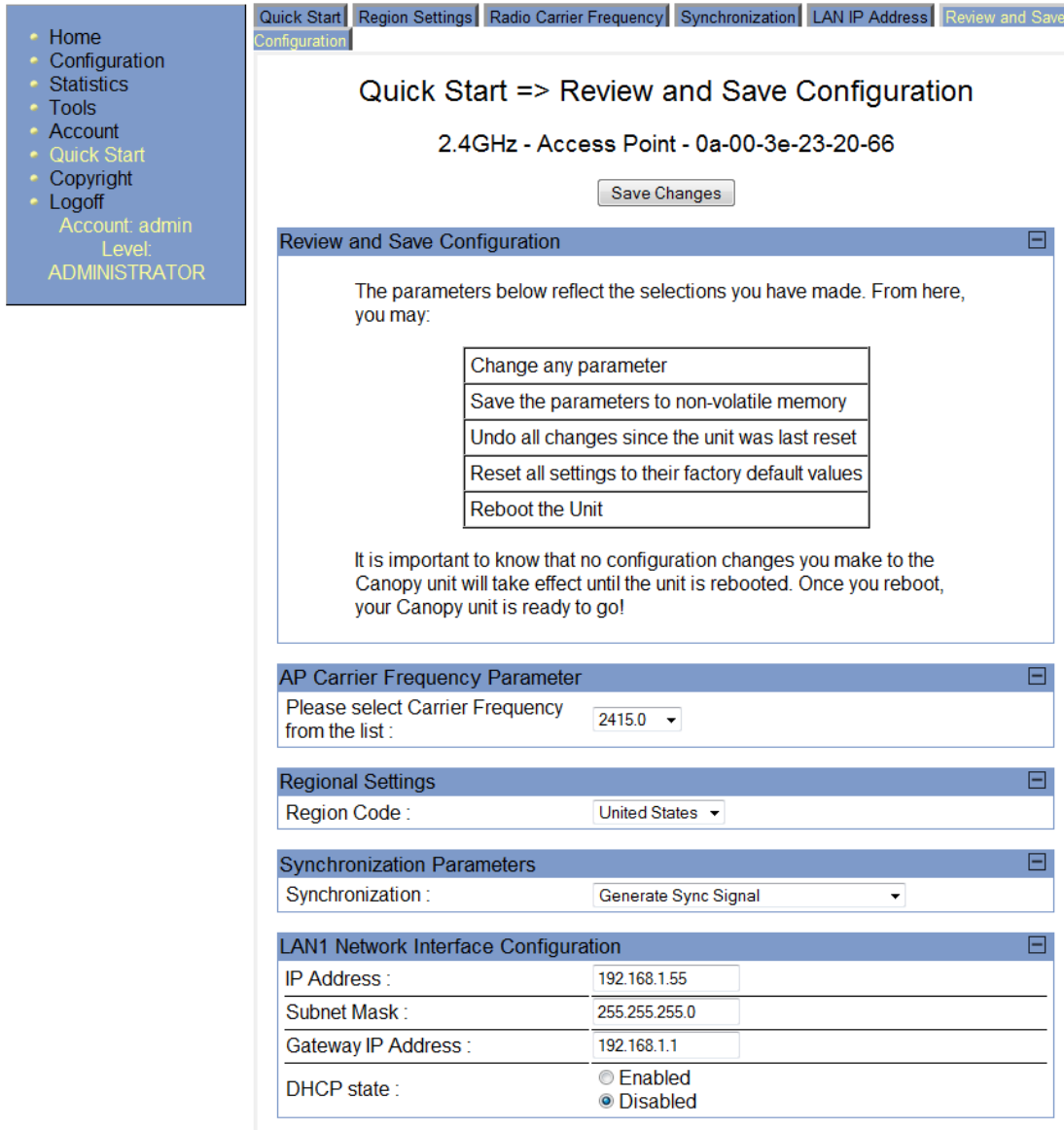


Figure 61: Review and Save Configuration tab of AP, example

10. Ensure that the initial parameters for the AP are set as you intended.
11. Click the **Save Changes** button.
12. Click the **Reboot** button.
*RESULT: The AP responds with the message **Reboot Has Been Initiated...***
13. Wait until the indicator LEDs are not red.
14. Trigger your browser to refresh the page until the AP redisplay the General Status tab.
15. Wait until the red indicator LEDs are not lit.

===== **end of procedure** =====

16.3.2 Time Tab of the AP

To proceed with the test setup, click the **Configuration** link on the left side of the General Status tab. When the AP responds by opening the Configuration page to the General tab, click the Time tab. An example of this tab is displayed in [Figure 62](#).

The screenshot shows the 'Configuration => Time' page for a 2.4GHz Access Point (ID: 0a-00-3e-20-a5-36). The page is divided into three main sections:

- NTP Server Configuration:** Includes a text input field for 'NTP server IP Address', a 'Save Changes' button, and a 'Reboot' button.
- Current System Time:** Displays 'System Time : 18:51:29 02/28/2003'.
- Time and Date:** Includes input fields for 'Time : [] / [] / []' and 'Date : [] / [] / []', along with 'Set Time and Date' and 'Get Time through NTP' buttons.

On the left side, there is a navigation menu with links: Home, Configuration, Statistics, Tools, Account, Quick Start, Copyright, and Logoff. Below the menu, it shows 'Account: root' and 'Level: ADMINISTRATOR'. At the top, there is a breadcrumb trail: General Settings | IP | Radio | SNMP | Quality of Service (QoS) | Security | Time | VLAN | VLAN Membership | DiffServe | Unit.

Figure 62: Time tab of AP, example

To have each log in the AP correlated to a meaningful time and date, either a reliable network element must pass time and date to the AP or you must set the time and date whenever a power cycle of the AP has occurred. A network element passes time and date in any of the following scenarios:

- A connected CMM2 passes time and date (GPS time and date, if received).
- A connected CMMmicro passes the time and date (GPS time and date, if received), but only if both the CMMmicro is operating on CMMmicro Release 2.1 or later release. (These releases include an NTP server functionality.)
- A separate NTP server is addressable from the AP.

If the AP should obtain time and date from a CMMmicro, CMM4, or a separate NTP server, enter the IP address of the CMM or NTP server on this tab. To force the AP to obtain time and date before the first (or next) 15-minute interval query of the NTP server, click **Get Time through NTP**.

If you enter a time and date, the format for entry is

Time :

<i>hh</i>

 /

<i>mm</i>

 /

<i>ss</i>

Date :

<i>MM</i>

 /

<i>dd</i>

 /

<i>YYYY</i>

where


- hh* represents the two-digit hour in the range 00 to 24
- mm* represents the two-digit minute
- ss* represents the two-digit second
- MM* represents the two-digit month
- dd* represents the two-digit day
- YYYY* represents the four-digit year

Proceed with the test setup as follows.

- Enter the appropriate information in the format shown above.
 - Then click the **Set Time and Date** button.
- NOTE:* The time displayed at the top of this page is static unless your browser is set to automatically refresh.

Procedure 8: Setting up the SM for test

1. In one hand, securely hold the top (larger shell) of the SM. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the SM RJ-45 jack.
3. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
4. Roughly aim the SM toward the AP.



WARNING!
From this point until you remove power from the SM, stay at least as far from the SM as the minimum separation distance specified in [Table 42](#) on Page [173](#).

5. Plug the power supply into an electrical outlet.
6. Repeat the foregoing steps for each SM that you wish to include in the test.
7. Back at the computing device, on the left side of the Time & Date tab, click **Home**.
8. Click the Session Status tab.

===== end of procedure =====

16.3.3 Session Status Tab of the AP

An example of the AP Session Status tab is displayed in [Figure 63](#).

The screenshot shows the 'Session Status' tab of an AP configuration page. The page title is 'Home ==> Session Status' and the AP identifier is '2.4GHz - Access Point - 0a-00-3e-20-a5-36'. The 'Session Status List' contains two entries:

- LUID: 002 : MAC: 0a-00-3e-20-00-32** State: IN SESSION (Encrypt Active)
 - Site Name : SM 10.40.14.121
 - Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
 - Software Boot Version : CANOPYBOOT 3.0
 - FPGA Version : 071305 (DES Sched) P8
 - Session Timeout: 0, AirDelay 6 (approximately 0.06 miles (294 feet))
 - Session Count: 1, Reg Count 1, Re-Reg Count 0
 - RSSI (Avg/Last): 2034/2030 Jitter (Avg/Last): 2/1 Power Level (Avg/Last): -37/-37
 - Sustained Uplink Data Rate (APCAP): 3500 (kbit)
 - Uplink Burst Allocation (APCAP): 500000 (kbit)
 - Sustained Downlink Data Rate (APCAP): 3500 (kbit)
 - Downlink Burst Allocation (APCAP): 500000 (kbit)
 - Low Priority Uplink CIR (D): 0 (kbps) Low Priority Downlink CIR (D): 0 (kbps)
 - Rate : VC 18 Rate 1X/1X
- LUID: 003 : MAC: 0a-00-3e-20-a6-6f** (Lite SM) State: IN SESSION (Encrypt Active)
 - Site Name : SM 10.40.14.147
 - Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
 - Software Boot Version : CANOPYBOOT 3.0
 - FPGA Version : 022706 (DES Sched) P9
 - Session Timeout: 0, AirDelay 3 (approximately 0.03 miles (147 feet))
 - Session Count: 1, Reg Count 1, Re-Reg Count 0
 - RSSI (Avg/Last): 2030/2029 Jitter (Avg/Last): 5/1 Power Level (Avg/Last): -37/-37
 - Sustained Uplink Data Rate (DLCAP): 256 (kbit)
 - Uplink Burst Allocation (DLCAP): 768 (kbit)
 - Sustained Downlink Data Rate (DLCAP): 256 (kbit)
 - Downlink Burst Allocation (DLCAP): 768 (kbit)

Figure 63: Session Status tab data from AP, example

If no SMs are registered to this AP, then the Session Status tab displays the simple message **No sessions**. In this case, try the following steps.

Procedure 9: Retrying to establish a point-to-multipoint link

1. More finely aim the SM or SMs toward the AP.
2. Recheck the Session Status tab of the AP for the presence of LUIDs.
3. If still no LUIDs are reported on the Session Status tab, click the **Configuration** button on the left side of the Home page.
RESULT: The AP responds by opening the AP Configuration page.
4. Click the Radio tab.
5. Find the **Color Code** parameter and note the setting.
6. In the same sequence as you did for the AP directly under [Configuring a Point-to-Multipoint Link for Test](#) on Page 186, connect the SM to a computing device and to power.
7. On the left side of the SM Home page, click the **Configuration** button.
RESULT: The Configuration page of the SM opens.
8. Click the Radio tab.
9. If the transmit frequency of the AP is not selected in the **Custom Radio Frequency Scan Selection List** parameter, select the frequency that matches.
10. If the **Color Code** parameter on this page is not identical to the **Color Code** parameter you noted from the AP, change one of them so that they match.

11. At the bottom of the Radio tab for the SM, click the **Save Changes** button.
12. Click the **Reboot** button.
13. Allow several minutes for the SM to reboot and register to the AP.
14. Return to the computing device that is connected to the AP.
15. Recheck the Session Status tab of the AP for the presence of LUIDs.

===== **end of procedure** =====

The Session Status tab provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a system. All information that you have entered in the **Site Name** field of the SM displays in the Session Status tab of the linked AP.

The Session Status tab also includes the current active values on each SM (LUID) for MIR, CIR, and VLAN, as well as the source of these values (representing the SM itself, BAM, or the AP and cap, if any—for example, APCAP as shown in [Figure 63](#) above). L indicates a Lite SM (CSM 110), and D indicates from the device. As an SM registers to the AP, the configuration source that this page displays for the associated LUID may change. After registration, however, the displayed source is stable and can be trusted.

The Session Status tab of the AP provides the following parameters.

LUID

This field displays the LUID (logical unit ID) of the SM. As each SM registers to the AP, the system assigns an LUID of 2 or a higher unique number to the SM. If an SM loses registration with the AP and then regains registration, the SM will retain the same LUID.



NOTE:

The LUID association is lost when a power cycle of the AP occurs.

Both the LUID and the MAC are hot links to open the interface to the SM. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.

MAC

This field displays the MAC address (or electronic serial number) of the SM. Both the LUID and the MAC are hot links to open the interface to the SM. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.

State

This field displays the current status of the SM as either

- **IN SESSION** to indicate that the SM is currently registered to the AP.
- **IDLE** to indicate that the SM was registered to the AP at one time, but now is not.

This field also indicates whether the encryption scheme in the module is enabled.

Site Name

This field indicates the name of the SM. You can assign or change this name on the Configuration web page of the SM. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Software Version

This field displays the software release that operates on the SM, the release date and time of the software.

Software Boot Version

This field indicates the CANOPYBOOT version number.

FPGA Version

This field displays the version of FPGA that runs on the SM.

Session Timeout

This field displays the timeout in seconds for management sessions via HTTP, telnet, or ftp access to the SM. 0 indicates that no limit is imposed.

AirDelay

This field displays the distance of the SM from the AP. To derive the distance in meters, multiply the displayed number by 0.3048. At close distances, the value in this field is unreliable.

Session Count

This field displays how many sessions the SM has had with the AP. Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum.

If the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem or an interference problem.

Reg Count

When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field.

Re-Reg Count

When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field. Typically, a Re-Reg is the case where both

- an SM attempts to reregister for having lost communication with the AP.
- the AP has not yet observed the link to the SM as being down.

A high number in this field is often an indication of link instability or interference problems.

RSSI, Jitter, and Power Level (Avg/Last)

The Session Status tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm.

For example, if coarse alignment gives an SM a power level of -75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to -78 dBm and the jitter to 2 or 3, use the refined alignment, with the following caveats:

- When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
- When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

However, Jitter is not calculated and reported in the PMP 400 Series OFDM AP. The Session Status tab also shows a historical **RSSI**, a unitless measure of power. Use **Power Level** and ignore **RSSI**. **RSSI** implies more accuracy and precision than is inherent in its measurement.

In both an FSK and an OFDM module, the spectrum analyzer measures and displays the detected *peak* power level. This is consistent with the received Power Level that various tabs in the FSK modules report. However, it is inconsistent with received Power Level indications in OFDM modules, which use this parameter to report the detected *average* power level. For this reason, you will observe a difference in how the spectrum analyzer and the Power Level field separately report on the same OFDM signal at the same time.

Sustained Uplink Data Rate

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified rate at which each SM registered to this AP is replenished with credits for transmission. The configuration source of the value is indicated in parentheses. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Uplink Burst Allocation

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified maximum amount of data that each SM is allowed to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. The configuration source of the value is indicated in parentheses. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Sustained Downlink Data Rate

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified the rate at which the AP should be replenished with credits (tokens) for transmission to each of the SMs in its sector. The configuration source of the value is indicated in parentheses. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Downlink Burst Allocation

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the **Sustained Downlink Data Rate**. The configuration source of the value is indicated in parentheses. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Low Priority Uplink CIR

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. The configuration source of the value is indicated in parentheses. See

- [Committed Information Rate](#) on Page 88
- [Setting the Configuration Source](#) on Page 292.

Low Priority Downlink CIR

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. The configuration source of the value is indicated in parentheses. See

- [Committed Information Rate](#) on Page 88
- [Setting the Configuration Source](#) on Page 292.

Rate

This field displays whether the high-priority channel is enabled in the SM and the status of 1X or 2X operation in the SM. See [Checking the Status of 2X Operation](#) on Page 94.

16.3.4 Beginning the Test of Point-to-Multipoint Links

To begin the test of links, perform the following steps:

1. In the Session Status tab of the AP, note the LUID associated with the MAC address of any SM you wish to involve in the test.
2. Click the Remote Subscribers tab.

16.3.5 Remote Subscribers Tab of the AP

An example of a Remote Subscribers tab is displayed in [Figure 64](#).

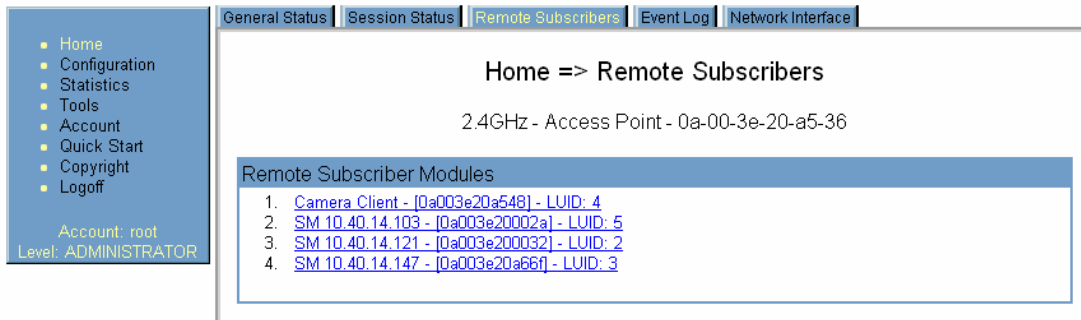


Figure 64: Remote Subscribers tab of AP, example

This tab allows you to view the web pages of registered SMs over the RF link. To view the pages for a selected SM, click its link. The General Status tab of the SM opens.

16.3.6 General Status Tab of the SM

An example of the General Status tab of an SM is displayed in [Figure 65](#).

General Status Event Log Network Interface Layer 2 Neighbors	
Home => General Status	
2.4GHz - Subscriber Module - 0a-00-3e-23-20-67	
Device Information	
Device Type :	2.4GHz - Subscriber Module - 0a-00-3e-23-20-67
Software Version :	CANOPY 9.4.2 SM-DES
Software BOOT Version :	CANOPYBOOT 3.0
Board Type :	P9
FPGA Version :	061708
Uptime :	00:02:19
System Time :	04:04:59 01/01/2001
Ethernet Interface :	No Link
Subscriber Module Stats	
Session Status :	REGISTERED VC 18 Rate 2X/2X
Session Uptime :	00:02:15
Registered AP :	0a-00-3e-23-20-66
Power Level :	Actual: -41 dBm Min: -42 dBm Max: -41 dBm
Jitter (Interference Level) :	Actual: 1 Min: 0 Max: 3
Air Delay :	1 approximately 0.01 miles (49 feet)
Frame Configuration Information	
Data Slots Down :	28 +
Data Slots Up :	9 +
Control Slots :	0
Region Specific Information	
Regional Code :	United States
Transmit Power Setting :	25 dBm
Site Information	
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location
Key Features Information	
Maximum Throughput :	Unlimited
Advantage Radio Status :	Advantage

Figure 65: General Status tab of SM, example

The General Status tab provides information on the operation of this SM. This is the tab that opens by default when you access the GUI of the SM. The General Status tab provides the following read-only fields.

Device Type

This field indicates the type of the module. Values include the frequency band of the SM, its module type, and its MAC address.

Software Version

This field indicates the system release, the time and date of the release, and whether communications involving the module are secured by DES or AES encryption (see [Encrypting Radio Transmissions](#) on Page 379). If you request technical support, provide the information from this field.

Software BOOT Version

This field indicates the version of the CANOPYBOOT file. If you request technical support, provide the information from this field.

Board Type

This field indicates the series of hardware. See [Designations for Hardware in Radios](#) on Page 377.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. Any SM that registers to an AP inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).

Ethernet Interface

This field indicates the speed and duplex state of the Ethernet interface to the SM.

Antenna

The presence of this field depends on whether antenna options are available for the module. This field indicates the polarity of the antenna in the modules as one of the following:

- **Horizontal**
- **Vertical**
- **External (Connectorized)**

Session Status

This field displays the following information about the current session:

- **Scanning** indicates that this SM currently cycles through the radio frequencies that are selected in the Radio tab of the Configuration page.
- **Syncing** indicates that this SM currently attempts to receive sync.
- **Registering** indicates that this SM has sent a registration request message to the AP and has not yet received a response.
- **Registered** indicates that this SM is both
 - registered to an AP.
 - ready to transmit and receive data packets.
- **Alignment** indicates that this SM is in an aiming mode. See [Table 46](#) on Page 183.

Session Uptime

This field displays the duration of the current link. The syntax of the displayed time is *hh:mm:ss*.

Registered AP

This field displays the MAC address of the AP to which this SM is registered.

Power Level and Jitter

The General Status tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm. For example, if coarse alignment gives an SM a power level of -75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to -78 dBm and the jitter to 2 or 3, use the refined alignment, with the following caveats:

- When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
- When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

PMP 400 Series OFDM SMs do not have this parameter. For historical relevance, the General Status tab also shows the **RSSI**, the unitless measure of power. Use **Power Level** and ignore **RSSI**. **RSSI** implies more accuracy and precision than is inherent in its measurement.

**NOTE:**

Unless the page is set to auto-refresh, the values displayed are from the instant the General Status tab was selected. To keep a current view of the values, refresh the browser screen or set to auto-refresh.

Air Delay

This field displays the distance in feet between this SM and the AP. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.

Region Code

From the drop-down list, select the region in which the radio is operating. Selectable regions are

- **Australia**
- **Brazil**
- **Canada**
- **Europe**
- **Russia**
- **United States**
- **Other**
- **None**

When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see [Radar Signature Detection and Shutdown](#) on Page 133.

The slave radio automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), you should always set the value that corresponds to the local region.

Unlike selections in other parameters, your **Region Code** selection requires a **Save Changes** and a **Reboot** cycle before it will force the context-sensitive GUI to display related options (for example, **Alternate Frequency Carrier 1 and 2** in the Configuration => Radio tab). Thus, a proper configuration exercise in environments that are subject to DFS requirements has two imperative **Save Changes** and **Reboot** cycles: one after the **Region Code** is set, and a second after related options are set.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the SM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Location

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page.

Maximum Throughput

This field indicates the limit of aggregate throughput for the SM and is based on the default (factory) limit of the SM and any floating license that is currently assigned to it.

Advantage Radio Status

This field reflects whether the SM is currently licensed for enhanced caps (Advantage, also known as Cap 2) on uplink and downlink traffic.

16.3.7 Continuing the Test of Point-to-Multipoint Links

To resume the test of links, perform the following steps.

Procedure 10: Verifying and recording information from SMs

1. Verify that the **Session Status** field of the General Status tab in the SM indicates **REGISTERED**.
2. While you view the General Status tab in the SM, note (or print) the values of the following fields:
 - **Device type**
 - **Software Version**
 - **Software BOOT Version**
 - **Board Type**
 - **FPGA Version**
3. Systematically ensure that you can retrieve this data (from a database, for example) when you later prepare to deploy the SM to subscriber premises.
4. Return to the Remote Subscribers tab of the AP.

5. Click the link of the next SM that you wish to test.
6. Repeat the test procedure from that point. When you have tested all of the SMs that you intend to test, return your browser to the General Status tab of the AP.

===== end of procedure =====

16.3.8 General Status Tab of the AP

Examples of AP General Status tabs are displayed in [Figure 66](#) and [Figure 67](#).

Home => General Status

5.7GHz - Access Point - 0a-00-3e-d5-b9-68

Device Information	
Device Type :	5.7GHz - Access Point - 0a-00-3e-d5-b9-68
Software Version :	CANOPY 9.4.2 AP-DES
Software BOOT Version :	CANOPYBOOT 1.0
Board Type :	P11
FPGA Version :	021909
FPGA Type :	C40
PLD Version :	1
Uptime :	00:56:12
System Time :	00:56:12 01/01/2001
Last NTP Time Update :	00:00:00 00/00/0000
Ethernet Interface :	100Base-TX Full Duplex
Regulatory :	Passed
Antenna :	Vertical

Access Point Stats	
Registered SM Count :	0
GPS Sync Pulse Status :	Generating Sync
Max Registered SM Count :	0

Frame Configuration Information	
Data Slots Down :	29
Data Slots Up :	9
Control Slots :	0

Site Information	
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Key Features Information	
MP Double Rate :	Enable
Advantage Radio Status :	Advantage

Figure 66: General Status tab of AP (5.7 GHz), example

- Home
- Configuration
- Statistics
- Tools
- Account
- Quick Start
- Copyright
- Logoff
- Account: admin
- Level: ADMINISTRATOR

General Status
Session Status
Remote Subscribers
Event Log
Network Interface
Layer 2 Neighbors

Home => General Status

900MHz - Access Point - 0a-00-3e-92-9f-90

Device Information	
Device Type :	900MHz - Access Point - 0a-00-3e-92-9f-90
Software Version :	CANOPY 9.4.2 AP-DES
Software BOOT Version :	CANOPYBOOT 1.0
Board Type :	P10
FPGA Version :	061808
PLD Version :	9
Uptime :	00:57:39
System Time :	00:57:39 01/01/2001
Last NTP Time Update :	00:00:00 00/00/0000
Ethernet Interface :	100Base-TX Full Duplex
Regulatory :	Passed
Antenna :	External (Connectorized)

Access Point Stats	
Registered SM Count :	4
GPS Sync Pulse Status :	Generating Sync
Max Registered SM Count :	4

Frame Configuration Information	
Data Slots Down :	18 +
Data Slots Up :	6
Control Slots :	0

Site Information	
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Key Features Information	
MP Double Rate :	Enable
Advantage Radio Status :	Advantage

Figure 67: General Status tab of AP (900 MHz), example

The General Status tab provides information on the operation of this AP. This is the tab that opens by default when you access the GUI of the AP. The General Status tab provides the following read-only fields.

Device Type

This field indicates the type of the module. Values include the frequency band of the AP, its module type, and its MAC address.

Software Version

This field indicates the system release, the time and date of the release, and whether communications involving the module are secured by DES or AES encryption (see [Encrypting Radio Transmissions](#) on Page 379). If you request technical support, provide the information from this field.

Software BOOT Version

This field indicates the version of the CANOPYBOOT file. If you request technical support, provide the information from this field.

Board Type

This field indicates the series of hardware. See [Designations for Hardware in Radios](#) on Page 377.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. If you request technical support, provide the value of this field.

FPGA Type

Where the type of logic as a subset of the logic version in the module as manufactured distinguishes its circuit board, this field is present to indicate that type. If you request technical support, provide the value of this field.

PLD Version

This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. If the AP is connected to a CMM, then this field provides GMT (Greenwich Mean Time). Any SM that registers to the AP inherits the system time.

Last NTP Time Update

This field displays when the AP last used time sent from an NTP server. If the AP has not been configured in the Time tab of the Configuration page to request time from an NTP server, then this field is populated by 00:00:00 00/00/00.

Ethernet Interface

This field indicates the speed and duplex state of the Ethernet interface to the AP.

Regulatory

This field indicates whether the configured Region Code and radio frequency are compliant with respect to their compatibility. For example, you may configure a 5.4-GHz AP with a **Region Code** set to **United States** and configure a frequency that lies within the weather notch. This is a compliant combination, the radio properly operates, and its **Regulatory** field displays Passed. If later you change its Region Code to Canada, then the combination becomes non-compliant (since frequencies within the weather notch are disallowed in Canada. In this case, the radio ceases to transmit, and its **Regulatory** field displays an error message.

For further information on Region Codes and DFS, see [Radar Signature Detection and Shutdown](#) on Page 133.

Antenna

The presence of this field depends on whether antenna options are available for the module. This field indicates the polarity of the antenna in the modules as one of the following:

- **Horizontal**
- **Vertical**
- **External (Connectorized)**

Registered SM Count

This field indicates how many SMs are registered to the AP.

GPS Sync Pulse Status

This field indicates the status of synchronization as follows:

- **Generating sync** indicates that the module is set to *generate* the sync pulse.
- **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse.
- **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse.



NOTE:

When this message is displayed, the AP transmitter is turned off to avoid self-interference within the system.

Max Registered SM Count

This field displays the largest number of SMs that have been simultaneously registered in the AP since it was last rebooted. This count can provide some insight into sector history and provide comparison between current and maximum SM counts at a glance.

Data Slots Down

This field indicates the number of frame slots that are designated for use by data traffic in the downlink (sent from the AP to the SM). The AP calculates the number of data slots based on the **Max Range**, **Downlink Data**, and (reserved) **Control Slots** configured by the operator. See [Max Range](#) on Page 235 and [Downlink Data](#) on Page 236.

A + in this field (for example, 28+) indicates that there are additional bit times that the scheduler can take advantage of for internal system communication, but not enough for a full data slot.

Data Slots Up

This field indicates the number of frame slots that are designated for use by data traffic in the uplink (sent from the SM to the AP). The AP calculates the number of data slots based on the Max Range, Downlink Data, and (reserved) Control Slots configured by the operator. See [Max Range](#) on Page 235 and [Downlink Data](#) on Page 236.

A + in this field (for example, 9+) indicates that there are additional bit times that the scheduler can take advantage of for control slots (which are half the size of data slots), but not enough for a full data slot.

Control Slots

This field indicates the number of (reserved) control slots configured by the operator. Control slots are half the size of data slots. The SM uses reserved control slots and unused data slots for bandwidth requests. See [Control Slots](#) on Page 237.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Location

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page.

Scheduling Type

This field indicates the type of frame scheduler that is active in the AP.

MP Double Rate

This field indicates whether 2X modulation rate is enabled for the sector.

Advantage Radio Status

This field indicates whether the radio is operating as an Advantage or a standard radio.

16.3.9 Concluding the Test of Point-to-Multipoint Links

To conclude the test, perform the following steps.

Procedure 11: Verifying and recording information from the AP

1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.
NOTE: This indication confirms that the AP is properly functional.
2. While your browser is directed to this General Status tab, note (or print) the values of the following fields:
 - **Device type**
 - **Software Version**
 - **Software BOOT Version**
 - **Board Type**
 - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the AP.

===== end of procedure =====

16.4 CONFIGURING A POINT-TO-POINT LINK FOR TEST

Perform the following steps to begin the test setup.

Procedure 12: Setting up the BH for Quick Start

1. In one hand, securely hold the top (larger shell) of the BH that you intend to deploy as a timing master. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the timing master.
3. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
4. Plug the other connector of the pig tail into the Ethernet jack of the computing device.



WARNING!

From this point until you remove power from the BH, stay at least as far from the BH as the minimum separation distance specified in [Table 42](#) on Page [173](#).

5. Plug the power supply into an electrical outlet.
6. Power up the computing device.
7. Start the browser in the computing device.

===== end of procedure =====

The PTP 100 Series BH interface provides a series of web pages to configure and monitor the unit. These screens are subject to change by subsequent software releases.

You can access the web-based interface through only a computing device that is either directly connected or connected through a network to the BH. If the computing device is not connected to a network when you are configuring the module in your test environment, and if the computer has used a proxy server address and port to configure the module, then you may need to first disable the proxy setting in the computer.

To toggle the computer to *not* use the proxy setting, perform [Procedure 6](#) on Page [187](#).

In the address bar of your browser, enter the IP address of the BHM (default is 169.254.1.1). The BHM responds by opening the General Status tab of its Home page.

16.4.1 Quick Start Page of the BHM

To proceed with the test setup, click the **Quick Start** button on the left side of the General Status tab. The BHM responds by opening the Quick Start tab of the Quick Start page. An example of this tab is displayed in [Figure 68](#).

Quick Start Configuration

Home
Configuration
Statistics
Tools
Account
Quick Start
Copyright
Logoff
Account: admin
Level: ADMINISTRATOR

Quick Start => Quick Start

5.4GHz - Backhaul - Timing Master - 0a-00-3e-53-fa-b7

Welcome to the Canopy Quick Start Configuration Wizard

The Canopy system consists of a family of highly flexible fixed wireless access devices that can be put into service very quickly and with a minimal configuration. This program walks you through that configuration. To do this, we need to cover the use of only three parameters:

RF Carrier Frequency
Synchronization
Network IP Address

These are the only parameters that need to be configured to start using your Canopy system! Each of the following pages will tell you a little about Canopy and ask you for a choice that best addresses your network needs. At the end, you will be given the opportunity to review the configuration you have selected and save it to non-volatile memory. None of the changes you make prior to saving the configuration will affect your system so feel free to experiment.

Canopy is a highly flexible system that can be used to build networks ranging from very simple to very sophisticated. If more advanced options are required for your application, please refer to the Canopy configuration page and Canopy user guides.

Go To Next Page=>

Figure 68: Quick Start tab of BHM, example

Quick Start is a wizard that helps you to perform a basic configuration that places a BHM into service. Only the following variables must be configured:

- **Region Code**
- **RF Carrier Frequency**
- **Synchronization**
- **LAN (Network) IP Address**

In each page under Quick Start, you can

- specify the settings to satisfy the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Proceed with the test setup as follows.

Procedure 13: Using Quick Start to configure the BHs for test

1. At the bottom of the Quick Start tab, click the **Go To Next Page =>** button.
RESULT: The BHM responds by opening the Region Settings tab.
2. From the pull-down menu, select the region in which the BHM will operate.
3. Click the **Go To Next Page =>** button.
RESULT: The BHM responds by opening the RF Carrier Frequency tab.
4. From the pull-down menu, select a frequency for the test.
5. Click the **Go To Next Page =>** button.
RESULT: The BHM responds by opening the Synchronization tab.
6. At the bottom of this page, select **Generate Sync Signal**.
7. Click the **Go To Next Page =>** button.
RESULT: The BHM responds by opening the LAN IP Address tab.
8. At the bottom of this tab, either
 - specify an **IP Address**, **Subnet Mask**, and **Gateway IP Address** for management of the BHM and leave the **DHCP State** set to **Disabled**.
 - set the **DHCP State** to **Enabled** to have the IP address, subnet mask, and gateway IP address automatically configured by a domain name server (DNS).
9. Click the **Go To Next Page =>** button.
RESULT: The BHM responds by opening the Review and Save Configuration tab.
10. Ensure that the initial parameters for the BHM are set as you intended.



NOTE:

Motorola encourages you to experiment with the interface. Unless you save a configuration and reboot the BHM after you save the configuration, none of the changes are effected.

11. Click the **Save Changes** button.
12. On the left side of the tab, click the **Configuration** button.
RESULT: The BH responds by opening the General tab of its Configuration page.
13. In the **Timing Mode** parameter, select **Timing Master**.
14. Click the **Save Changes** button.
15. Click the **Reboot** button.
RESULT: The BHM responds with the message **Reboot Has Been Initiated....**
This BH is now forced to provide sync for the link and has a distinct set of web interface pages, tabs, and parameters for the role of BHM.
16. Wait until the indicator LEDs are not red.

17. Trigger your browser to refresh the page until the BHM redisplay the General Status tab of its Home page.
18. Repeat these steps to configure the other BH in the pair to be a BHS, selecting **Timing Slave** in Step 13.

===== end of procedure =====

16.4.2 Time Tab of the BHM

To proceed with the test setup, in the BHM, click the **Configuration** button on the left side of the General Status tab. The BHM responds by opening its Configuration page to the General tab. Click the Time tab. An example of this tab is displayed in [Figure 69](#).

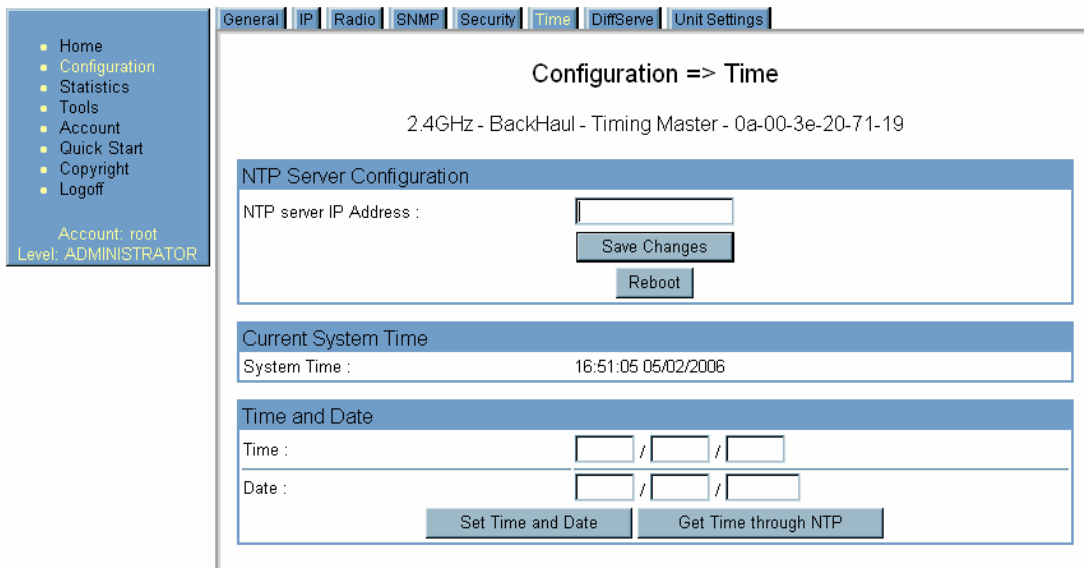


Figure 69: Time tab of BHM, example

To have each log in the BHM correlated to a meaningful time and date, either a reliable network element must pass time and date to the BHM or you must set the time and date whenever a power cycle of the BHM has occurred. A network element passes time and date in any of the following scenarios:

- A connected CMM2 passes time and date (GPS time and date, if received).
- A connected CMMmicro passes the time and date (GPS time and date, if received), but only if the CMMmicro is operating on CMMmicro Release 2.1 or later release. (These releases include an NTP server functionality.)
- A separate NTP server is addressable from the BHM.

If the BHM should derive time and date from either a CMMmicro or a separate NTP server, enter the IP address of the CMMmicro or NTP server on this tab. To force the BHM to derive time and date before the first (or next) 15-minute interval query of the NTP server, click **Get Time through NTP**.

If you enter a time and date, the format for entry is

Time : / /
 Date : / /

where

- hh* represents the two-digit hour in the range 00 to 24
- mm* represents the two-digit minute
- ss* represents the two-digit second
- MM* represents the two-digit month
- dd* represents the two-digit day
- YYYY* represents the four-digit year

Proceed with the test setup as follows.

Procedure 14: Setting up the BHS for test

1. Enter the appropriate information in the format shown above.
2. Click the **Set Time and Date** button.
NOTE: The time displayed at the top of this page is static unless your browser is set to automatically refresh.
3. In one hand, securely hold the top (larger shell) of the BH that you intend to deploy as a timing slave. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
4. Plug one end of a CAT 5 Ethernet cable into the BHS.
5. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
6. Roughly aim the BHS toward the BHM.



WARNING!

From this point until you remove power from the BHS, stay at least as far from the BHS as the minimum separation distance specified in [Table 42](#) on Page [173](#).

7. Plug the power supply into an electrical outlet.
8. Back at the computing device, on the left side of the BHM Time tab, click the **Home** button. When the Home page opens to the General Status tab, click the **Remote Subscribers** tab.
RESULT: The BHM opens the Remote Subscribers tab. An example of this tab is shown in [Figure 70](#).

===== end of procedure =====

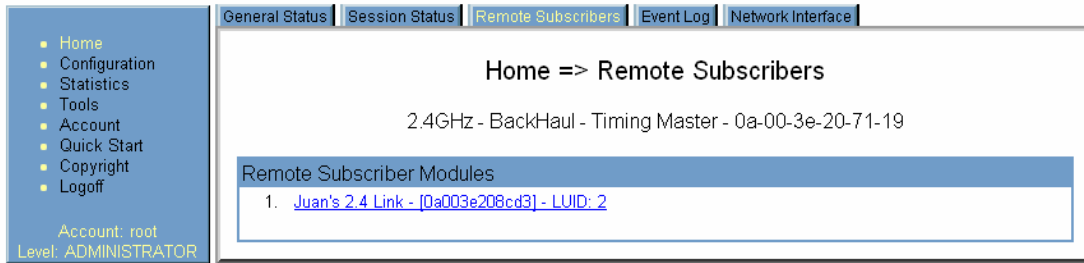


Figure 70: Remote Subscribers tab of BHM, example

16.4.3 Beginning the Test of Point-to-Point Links

To begin the test of your BH link, in the Remote Subscribers tab of the BHM, click the link to the BHS. The BHS GUI opens to the General Status tab of its Home page.

An example of the BHS General Status tab is displayed in Figure 71.

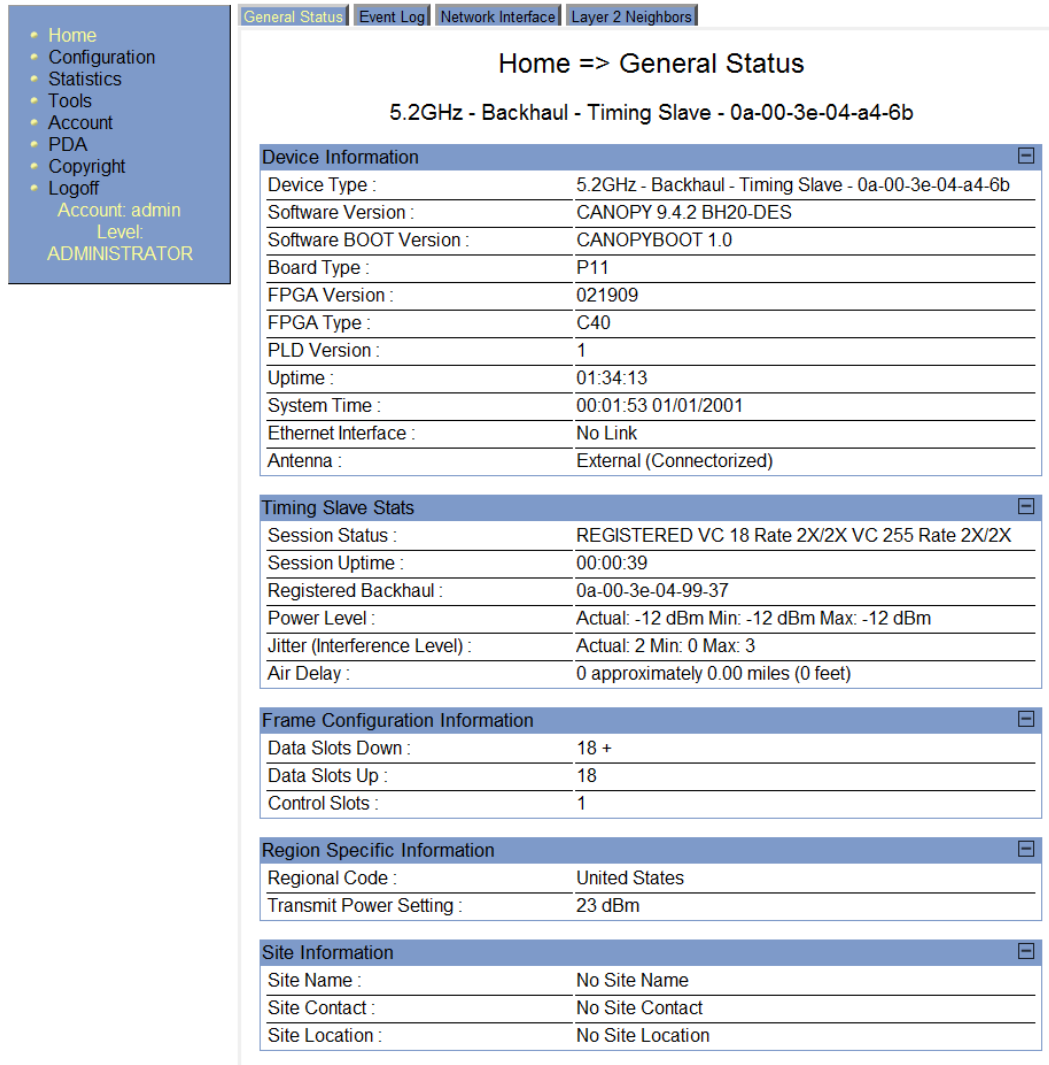


Figure 71: General Status tab of BHS, example

The General Status tab provides information on the operation of this BHS. This is the tab that opens by default when you access the GUI of the BHS. The General Status tab provides the following read-only fields.

Device Type

This field indicates the type of the module. Values include the frequency band of the BHS, its module type, and its MAC address.

Software Version

This field indicates the system release, the time and date of the release, the modulation rate, and whether communications involving the module are secured by DES or AES encryption (see [Encrypting Radio Transmissions](#) on Page 379). If you request technical support, provide the information from this field.

Software BOOT Version

This field indicates the version of the CANOPYBOOT file. If you request technical support, provide the information from this field.

Board Type

This field indicates the series of hardware. See [Designations for Hardware in Radios](#) on Page 377.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the value of this field.

FPGA Type

Where the type of logic as a subset of the logic version in the module as manufactured distinguishes its circuit board, this field is present to indicate that type. If you request technical support, provide the value of this field.

PLD Version

This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. When a BHS registers to a BHM, it inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).

Ethernet Interface

This field indicates the speed and duplex state of the Ethernet interface to the BHS.

Antenna

The presence of this field depends on whether antenna options are available for the module. This field indicates the polarity of the antenna in the modules as one of the following:

- **Horizontal**
- **Vertical**
- **External (Connectorized)**

Session Status

This field displays the following information about the current session:

- **Scanning** indicates that this SM currently cycles through the RF frequencies that are selected in the Radio tab of the Configuration page.
- **Syncing** indicates that this SM currently attempts to receive sync.
- **Registering** indicates that this SM has sent a registration request message to the AP and has not yet received a response.
- **Registered** indicates that this SM is both
 - registered to an AP.
 - ready to transmit and receive data packets.
- **Alignment** indicates that this SM is in an aiming mode. See [Table 46](#) on Page 183.

Session Uptime

This field displays the duration of the current link. The syntax of the displayed time is *hh:mm:ss*.

Registered Backhaul

This field displays the MAC address of the BHM to which this BHS is registered.

Power Level and Jitter

The General Status tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm. For example, if coarse alignment gives the BHS a power level of -75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to -78 dBm and the jitter to 2 or 3, use the refined alignment, with the following caveats:

- When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
- When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

OFDM BHSs do not have this parameter. For historical relevance, the General Status tab also shows the **RSSI**, the unitless measure of power. Use **Power Level** and ignore **RSSI**. **RSSI** implies more accuracy and precision than is inherent in its measurement.

**NOTE:**

Unless the page is set to auto-refresh, the values displayed are from the instant the General Status tab was selected. To keep a current view of the values, refresh the browser screen or set to auto-refresh.

Air Delay

This field displays the distance in feet between the BHS and the BHM. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.

Data Slots Down

This field indicates the currently configured number of frame slots that are designated for use by data traffic in the downlink (sent from the backhaul slave to the backhaul master). See [Max Range](#) on Page 235 and [Downlink Data](#) on Page 236.

Data Slots Up

This field indicates the currently configured number of frame slots that are designated for use by data traffic in the uplink (sent from the backhaul master to the backhaul slave). See [Max Range](#) on Page 235 and [Downlink Data](#) on Page 236.

Control Slots

This field indicates the currently configured number of frame slots that are designated for use by control (overhead) traffic. See [Control Slots](#) on Page 237.

Region Code

This field indicates the region in which the radio is currently set to operate. When the appropriate region has been set, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see [Radar Signature Detection and Shutdown](#) on Page 133.

The slave radio automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this field should always indicate the value that corresponds to the local region.

Transmit Power Setting

This field displays the value of the Transmitter Output Power parameter in the module. See [Table 59: Transmitter output power settings, example cases](#) on Page 333.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the BHS Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the BHS Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Location

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the BHS Configuration page.

16.4.4 Continuing the Test of Point-to-Point Links

To resume the test, perform the following steps.

Procedure 15: Verifying and recording information from the BHS

1. Verify that the **Session Status** field of the General Status tab in the BHS indicates **REGISTERED**.
NOTE: This indication confirms that the BHS is properly functional.
2. While your browser is set to the General Status tab, note (or print) the values of the following fields:
 - **Device type**
 - **Software Version**
 - **Software BOOT Version**
 - **Board Type**
 - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the BHS.
4. Return your browser to the General Status tab of the BHM.

===== end of procedure =====

16.4.5 General Status Tab of the BHM

An example of a BHM General Status tab is displayed in [Figure 72](#).

The screenshot shows a web interface for the BHM General Status tab. On the left is a navigation menu with options like Home, Configuration, Statistics, Tools, Account, Quick Start, Copyright, and Logoff. The user is logged in as 'admin' with 'ADMINISTRATOR' level. The main content area has tabs for General Status, Session Status, Event Log, Network Interface, Layer 2 Neighbors, and DFS Status. The 'General Status' tab is active, displaying 'Home => General Status' for a device identified as '5.2GHz - Backhaul - Timing Master - 0a-00-3e-04-99-37'. The data is organized into four expandable sections: Device Information, Backhaul Stats, Frame Configuration Information, and Site Information.

Device Information	
Device Type :	5.2GHz - Backhaul - Timing Master - 0a-00-3e-04-99-37
Software Version :	CANOPY 9.4.2 BH20-DES
Software BOOT Version :	CANOPYBOOT 1.0
Board Type :	P11
FPGA Version :	021909
FPGA Type :	C40
PLD Version :	1
Uptime :	00:03:23
System Time :	00:03:23 01/01/2001
Last NTP Time Update :	00:00:00 00/00/0000
Ethernet Interface :	100Base-TX Full Duplex
Regulatory :	Passed
DFS :	Normal Transmit
Antenna :	External (Connectorized)

Backhaul Stats	
Timing Slave Status :	Connected
GPS Sync Pulse Status :	Generating Sync

Frame Configuration Information	
Data Slots Down :	18 +
Data Slots Up :	18
Control Slots :	1

Site Information	
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Figure 72: General Status tab of BHM, example

The Status page provides information on the operation of the module. This is the default web page for the module. The Status page provides the following fields.

Device Type

This field indicates the type of the module. Values include the frequency band of the module, the module type, timing mode, and the MAC address of the module.

Software Version

This field indicates the software release that is operated on the module, the release date and time of the software release, the modulation rate capability, and whether the module is secured by DES or AES encryption (see [Encrypting Radio Transmissions](#) on Page 379). When you request technical support, provide the information from this field.

Software BOOT Version

This field indicates the version of the CANOPYBOOT file. If you request technical support, provide the information from this field.

Board Type

This field indicates the series of hardware. See [Designations for Hardware in Radios](#) on Page 377.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. If you request technical support, provide the value of this field.

FPGA Type

Where the type of logic as a subset of the logic version in the module as manufactured distinguishes its circuit board, this field is present to indicate that type. If you request technical support, provide the value of this field.

PLD Version

This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. If the BHM is connected to a CMM, then this field provides GMT (Greenwich Mean Time). The BHS that registers to the BHM inherits the system time.

Last NTP Time Update

If the Time & Date page of the module specifies that time should be received from an NTP server, then this field indicates when the time was last updated by a Network Time Protocol (NTP) server.

Ethernet Interface

If an Ethernet link to the module exists, this field indicates the speed and duplex state of the Ethernet interface to the module.

Regulatory

This field indicates whether the configured Region Code and radio frequency are compliant with respect to their compatibility. For example, you may configure a 5.4-GHz AP with a **Region Code** set to **United States** and configure a frequency that lies within the weather notch. This is a compliant combination, the radio properly operates, and its **Regulatory** field displays Passed. If later you change its Region Code to Canada, then the combination becomes non-compliant (since frequencies within the weather notch are disallowed in Canada. In this case, the radio ceases to transmit, and its **Regulatory** field displays an error message.

For further information on Region Codes and DFS, see [Radar Signature Detection and Shutdown](#) on Page 133.

DFS

This field indicates the current behavior of the radio with respect to Dynamic Frequency Selection. Possible messages in this field are

- **Normal Transmit**
- **Radar Detected Stop Transmitting for n minutes**, where n counts down from 30 to 1.
- **Checking Channel Availability Remaining time n seconds**, where n counts down from 60 to 1.

Antenna

The presence of this field depends on whether antenna options are available for the module. This field indicates the polarity of the antenna in the modules as one of the following:

- **Horizontal**
- **Vertical**
- **External (Connectorized)**

Timing Slave Status

This field indicates whether this backhaul master is currently in link with a backhaul slave.

GPS Sync Pulse Status

This field indicates the status of synchronization as follows:

- **Generating sync** indicates that the module is set to *generate* the sync pulse.
- **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse.
- **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse.

**NOTE:**

When this message is displayed, the BHM transmitter is turned off to avoid self-interference within the system.

Data Slots Down

This field indicates the number of frame slots that are designated for use by data traffic in the downlink (sent from the backhaul slave to the backhaul master). See [Max Range](#) on Page 235 and [Downlink Data](#) on Page 236.

Data Slots Up

This field indicates the number of frame slots that are designated for use by data traffic in the uplink (sent from the backhaul master to the backhaul slave). See [Max Range](#) on Page 235 and [Downlink Data](#) on Page 236.

Control Slots

This field indicates the number of frame slots that are designated for use by control (overhead) traffic. See [Control Slots](#) on Page 237.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the BHM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the BHM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Location

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the BHM Configuration page.

16.4.6 Concluding the Test of Point-to-Point Links

To conclude the test, perform the following steps.

Procedure 16: Verifying and recording information from the BHM

1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.
NOTE: This indication confirms that the BHM is properly functional.
2. While your browser is set to this BHM Status page, note (or print) the values of the following fields:
 - **Device type**
 - **Software Version**
 - **Software BOOT Version**
 - **Board Type**
 - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the BHM.

===== end of procedure =====

17 PREPARING COMPONENTS FOR DEPLOYMENT

Your test of the modules not only verified that they are functional, but also yielded data that you have stored about them. Most efficiently preparing modules for deployment involves

- retrieving that data.
- systematically collecting the data into a single repository, while keeping a strong (quick) association between the data and the module.
- immediately merging module access data into this previously stored data.

17.1 CORRELATING COMPONENT-SPECIFIC INFORMATION

You can use the data that you noted or printed from the Status pages of the modules to

- store modules for future deployment.
- know, at a glance, how well-stocked you are for upcoming network expansions.
- efficiently draw modules from stock for deployment.
- plan any software updates that you
 - wish to perform to acquire features.
 - need to perform to have the feature set be consistent among all modules in a network expansion.

You can make these tasks even easier by collecting this data into a sortable database.

17.2 ENSURING CONTINUING ACCESS TO THE MODULES

As you proceed through the steps under [Configuring for the Destination](#) on Page 227, you will set values for parameters that specify the sync source, data handling characteristics, security measures, management authorities, and other variables for the modules. While setting these, you will also tighten access to the module, specifically in

- the **Color Code** parameter of Configuration page
- the **Display-Only Access** and **Full Access** password parameters of the Configuration page.
- the addressing parameters of the IP Configuration page.

Before you set these, consider whether and how you may want to set these by a self-devised scheme. A password scheme can help you when you have forgotten or misfiled a password. An IP addressing scheme may be essential to the operation of your network and to future expansions of your network.

As you set these, note the color code and note or print the parameters you set on the Configuration page tabs. Immediately associate them with the following previously stored data about the modules:

- device type, frequency band, and MAC address
- software version and encryption type
- software boot version
- FPGA version

18 CONFIGURING FOR THE DESTINATION

18.1 CONFIGURING AN AP FOR THE DESTINATION

If an ADMINISTRATOR-level password has been set in the AP, you must log into the module before you can configure its parameters. See [Managing Module Access by Passwords](#) on Page 381.

18.1.1 General Tab of the AP

An example of an AP General tab is displayed in [Figure 73](#).

Configuration => General

5.7GHz - Access Point - 0a-00-3e-d5-b9-97

Save Changes

Device Type AP SM

Link Speeds
Link Speed : Auto 100F/100H/10F/10H

Bandwidth Configuration Source
Configuration Source : SM

Sync Setting
Sync Input : Sync to Received Signal (Power Port)

Regional Settings
Region Code : Europe

Web Page Configuration
Webpage Auto Update : 1 Seconds (0 = Disable Auto Update)

Bridge Configuration
Bridge Entry Timeout : 25 Minutes (Range : 25—1440 Minutes)
Translation Bridging : Enabled Disabled
Send Untranslated ARP : Enabled Disabled
SM Isolation : Disable SM Isolation

Update Application Information
Update Application Address : 192.168.1.205

MAC Control Parameters
Dynamic Rate Adapt : 1x/2x

TCP Settings
Prioritize TCP ACK : Enabled Disabled

Layer 2 Discovery Destination Address
Multicast Destination Address : Broadcast LLDP Multicast

Save Changes

Reboot

Figure 73: General tab of AP, example

The General tab of the AP contains many of the configurable parameters that define how the AP and the SMs in the sector operate. As shown in [Figure 73](#), you may set the Configuration page parameters as follows.

Device Setting

You can temporarily transform an AP into an SM and thereby use the spectrum analyzer functionality. See [Using the AP as a Spectrum Analyzer](#) on Page 375. Otherwise, the selection for this parameter is **AP**.

Link Speeds

From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected: **Auto 100F/100H/10F/10H**. In this setting, the two ends of the link automatically negotiate with each other whether the speed that they will use is 10 Mbps or 100 Mbps and whether the Ethernet traffic will be full duplex or half duplex. However, Ethernet links work best when either

- both ends are set to the same forced selection
- both ends are set to auto-negotiate and both have capability in least one common speed and traffic type combination.

Configuration Source

See [Setting the Configuration Source](#) on Page 292.



CAUTION!

Do not set this parameter to **BAM** where both

- a BAM release earlier than 2.1 is implemented.
- the **All Local SM Management** parameter (in the VLAN Configuration page of the AP) is set to **Enable**.

This combination causes the SMs to become unmanageable, until you gain direct access with an Override Plug and remove this combination from the AP configuration.

Sync Input

Specify the type of synchronization for this AP to use:

- Select **Sync to Received Signal (Power Port)** to set this AP to receive sync from a connected CMMmicro or CMM4.
- Select **Sync to Received Signal (Timing Port)** to set this AP to receive sync from a connected CMM2, an AP in the cluster, an SM, or a BH timing slave.
- Select **Generate Sync Signal** where the AP does not receive sync, and no other AP or BHM is active within the link range.

Region Code

From the drop-down list, select the region in which the radio is operating. Selectable regions are

- **Australia**
- **Brazil**
- **Canada**
- **Europe**
- **Russia**
- **United States**
- **Other**
- **None**

When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see [Radar Signature Detection and Shutdown](#) on Page 133.

Unlike selections in other parameters, your **Region Code** selection requires a **Save Changes** and a **Reboot** cycle before it will force the context-sensitive GUI to display related options (for example, **Alternate Frequency Carrier 1 and 2** in the Configuration => Radio tab). Thus, a proper configuration exercise in environments that are subject to DFS requirements has two imperative **Save Changes** and **Reboot** cycles: one after the **Region Code** is set, and a second after related options are set.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.



CAUTION!

An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

Translation Bridging

If you want the Translation Bridging feature, select **Enabled**. This has numerous implications. For a full description of them, see [Uplink Frame](#) on Page 85.

Send Untranslated ARP

If the **Translation Bridging** parameter is set to **Enabled**, then the **Send Untranslated ARP** parameter can be

- disabled, so that the AP will overwrite the MAC address in Address Resolution Protocol (ARP) packets before forwarding them.
- enabled, so that the AP will forward ARP packets regardless of whether it has overwritten the MAC address.

See [Uplink Frame](#) on Page 85 and [Address Resolution Protocol](#) on Page 166.

If the **Translation Bridging** parameter is set to **Disabled**, then the **Send Untranslated ARP** parameter has no effect.

SM Isolation

Prevent or allow SM-to-SM communication by selecting from the following drop-down menu items:

- **Disable SM Isolation** (the default selection). This allows full communication between SMs.
- **Block SM Packets from being forwarded**. This prevents both multicast/broadcast and unicast SM-to-SM communication.
- **Block and Forward SM Packets to Backbone**. This not only prevents multicast/broadcast and unicast SM-to-SM communication but also sends the packets, which otherwise would have been handled SM to SM, through the Ethernet port of the AP.

Update Application Address

Enter the address of the server to access for software updates on this AP and registered SMs.

2X Rate

This parameter is present in only PMP 100 Series APs. You should generally keep this parameter set to **Enabled** to allow the module to automatically the operation rate. For troubleshooting, you may lock the rate down (Disabled), but be aware that this locks down the operation rate for all uplinks and downlinks across the sector. See [2X Operation](#) on Page 92.

Dynamic Rate Adapt

This parameter is present in only PMP 400 Series APs. You should generally keep this parameter set to **Enabled** to allow the module to automatically the operation rate. For troubleshooting, you may lock the rate down (Disabled), but be aware that this locks down the operation rate for all uplinks and downlinks across the sector. See [2X Operation](#) on Page 92 and [3X Operation](#) on Page 95.

Prioritize TCP ACK

To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. See [AP-SM Links](#) on Page 101.

The General tab also provides the following buttons.

Multicast Destination Address

Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMMmicro, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the **Multicast Destination Address** parameter value in the connected device that has it populated.

In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to **LLDP Multicast**. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.

Where the AP is not behind another device, the **Broadcast** mode will allow discovery of the AP.

Save Changes

When you click this button, any changes that you made on the this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.1.2 IP Tab of the AP

An example of the IP tab of the AP is displayed in [Figure 74](#).

Figure 74: IP tab of AP, example

You may set the IP tab parameters as follows.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this AP. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See [Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH](#) on Page 383.



RECOMMENDATION:

Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the AP to communicate on the network. The default subnet mask is 255.255.0.0. See [Allocating Subnets](#) on Page 166.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the AP to communicate with the network. The default gateway is 169.254.0.0.

The values of these four LAN1 network interface configuration parameters are displayed read only along with the Ethernet speed and duplex state on the Network Interface tab of the Home page in the AP.

LAN1 Network Interface Configuration, DHCP State

If you select **Enabled**, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.

LAN2 Network Interface Configuration (RF Private Interface), IP Address

You should not change this parameter from the default AP private IP address of 192.168.101.1. A /24 CIDR subnet is used to communicate with each of the SMs that are registered. The AP uses a combination of the private IP and the LUID (logical unit ID) of the SM.

For example, if an SM is the first to register in an AP, and another SM registers later, then the AP whose Private IP address is 192.168.101.1 uses the following SM Private IP addresses to communicate to each:

SM	LUID	Private IP
First SM registered	2	192.168.101.2
Second SM registered	3	192.168.101.3



NOTE:

Where space is limited for subnet allocation, be advised that an SM *need not* have an operator-assigned IP address. The SM is directly accessible without an LUID if either the SM **Color Code** parameter is set to 0 or the AP has a direct Ethernet connection to the SM.

The IP Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.1.3 Radio Tab of the AP

Examples of the Radio tab of the AP are shown in [Figure 75](#) and [Figure 76](#).

The screenshot displays the 'Radio Configuration' page for a 900MHz Access Point. The page is titled 'Configuration => Radio' and shows the following configuration details:

Radio Configuration	
Radio Frequency Carrier :	906.0
Color Code :	127 (0—254)
Power Save Mode :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Sector ID :	5
Max Range :	30 Miles (Range: 1— 120 miles)
Downlink Data :	70 % (Range: 1 — 99 %)
Schedule Whitening :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Hardware Scheduler Link Configurations	
Control Slots :	0 (Range: 0 — 15)
External Filters Delay	
External Filters Delay :	0 Nanoseconds
Scan Policy	
Broadcast Repeat Count :	2 (Range : 0 — 2)
Transmitter Output Power	
Transmitter Output Power :	26 dBm (Range: 5 — 26 dBm)

Buttons: Save Changes, Reboot

Figure 75: Radio tab of AP (900 MHz), example

Configuration => Radio
5.4GHz - Access Point - 0a-00-3e-52-14-62

Save Changes

Radio Configuration	
Radio Frequency Carrier :	5580
Alternate Frequency Carrier 1 :	5590
Alternate Frequency Carrier 2 :	5600
Color Code :	0 (0—254)
Power Save Mode :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Sector ID :	0
Max Range :	2 Miles (Range: 1—30 miles)
Downlink Data :	75 % (Range: 1 — 99 %)
Schedule Whitening :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
External Gain :	0 dB (Range : 0—35 dB)

Hardware Scheduler Link Configurations	
Control Slots :	0 (Range: 0 -- 10)

Scan Policy	
Broadcast Repeat Count :	2 (Range : 0 — 2)
Transmit Frame Spreading :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Transmitter Output Power	
Transmitter Output Power :	23 dBm (Range: -4 -- 23 dBm)

Save Changes

Reboot

Figure 76: Radio tab of AP (5.4 GHz), example

The Radio tab of the AP contains some of the configurable parameters that define how the AP operates. As shown in [Figure 75](#), you may set the Radio tab parameters as follows.

Radio Frequency Carrier

Specify the frequency for the module to transmit. The default for this parameter is **None**. (The selection labeled **Factory** requires a special software key file for implementation.) For a list of channels in the band, see the drop-down list or [Considering Frequency Band Alternatives](#) on Page 138.

Alternate Frequency Carrier 1

If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:

1. Click the General tab.
2. Set the **Region Code** parameter from its drop-down list.
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. Click the Radio tab.

From the drop-down list, select the frequency that the AP should switch to if it detects a radar signature on the frequency configured in the **Radio Frequency Carrier** parameter. See [Radar Signature Detection and Shutdown](#) on Page 133.

Alternate Frequency Carrier 2

From the drop-down list, select the frequency that the AP should switch to if it detects a radar signature on the frequency configured in the **Alternate Frequency Carrier 1** parameter. See [Radar Signature Detection and Shutdown](#) on Page 133.

Color Code

Specify a value from 0 to 254. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code.

Color code allows you to force an SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).



RECOMMENDATION:

Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Power Save Mode

Select either

- **Enabled** (the default), to reduce module power consumption by approximately 10% without affecting the transmitter output power. This is the recommended setting.
- **Disabled**, to continue normal power consumption, but do so only under guidance from technical support.

Sector ID

Specify a number in the range 1 to 6 to associate with this AP. The Sector ID setting does not affect the operation of the AP. On the AP Evaluation tab of the Tools page in the SM, the **Sector ID** field identifies the AP that the SM sees. The following steps may be useful:

- Assign a unique Sector ID to each sector in an AP cluster.
- Repeat the assignment pattern throughout the entire system.

Max Range

Enter a number of miles (or kilometers divided by 1.61, then rounded to an integer) for the furthest distance from which an SM is allowed to register to this AP. Do not set the distance to any greater number of miles. A greater distance

- does not increase the power of transmission from the AP.
- can reduce aggregate throughput. See [Table 25](#) on Page 102.

Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. If the AP is in cluster, then you *must* set this parameter on all other APs in the cluster exactly the same, except as described in the NOTE admonition below. The default value of this parameter is 2 miles (3.2 km).

For APs in the non 900-MHz frequency band ranges, although the typical maximum range where an SM is deployed with a reflector is 15 miles (24 km), you can set this parameter to as far as 30 miles (48 km). Without increasing the power or sensitivity of the AP or SM, the greater value allows you to attempt greater distance where the RF environment and Fresnel zone⁶ are especially clear.

For the PMP 400 Series AP, the typical maximum range achievable depends on the operation mode as follows:

- 5 miles (8 km) in 1X operation
- 2.5 miles (4 km) in 2X operation
- 1.25 miles (2 km) in 3X operation

A value of 15 for this parameter decreases the number of available data slots by 1. With a higher value, the number is further decreased as the AP compensates for the expected additional air delay.

Downlink Data

Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the AP to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the AP is 6 Mb, then 75% specified for this parameter allocates 4.5 Mb for the downlink and 1.5 Mb for the uplink. The default for this parameter is 75%.



CAUTION!

You must set this parameter exactly the same for all APs in a cluster.

Schedule Whitening

Select either

- **Enable**, to spread the transmitted signal power to avoid peaks that modules with Dynamic Frequency Selection (DFS) configured might interpret as radar. This is the recommended setting.
- **Disable**, to allow peaks in transmitted signal power.

PMP 400 Series OFDM APs do not have this parameter.

⁶ See [Noting Possible Obstructions in the Fresnel Zone](#) on Page 132.

External Gain

If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:

1. Click the **General** tab.
2. Set the **Region Code** parameter from its drop-down list.
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. Click the **Radio** tab.

Using [Table 48](#) as a guide, type in the dB value by which to reduce Dynamic Frequency Selection (DFS) sensitivity to radar signals.

Table 48: Recommended External Gain values for AP

Module Type	Recommended Setting
FSK with only integrated patch antenna	0
FSK with 9 dB Canopy LENS	9
FSK with standard 18 dB reflector	18
FSK connectorized with 15.5 dBi antenna and 0.5 dB cable loss	15
OFDM with only integrated antenna	17
OFDM connectorized with antenna that was purchased with it	17
OFDM connectorized with separately purchased antenna	antenna gain minus coax + connector loss

The value of this parameter does not affect transmitter output power. This parameter is present in only radios that support DFS and hence is not present in 900-MHz radios.

Control Slots

Field results have indicated that, in general, systems perform better with a slightly higher number of control slots than previously recommended. If you are experiencing latency or SM-servicing issues, increasing the number of control slots may increase system performance, depending on traffic mix over time.

Use care when changing the control slot configuration of only some APs, because changes affect the uplink/downlink ratio and can cause collocation issues. For APs in a cluster of mismatched control slots settings, or where OFDM and FSK AP of the same frequency band are collocated, use the frame calculator. See [Using the Frame Calculator Tool \(All\) for Collocation](#) on [Page 446](#).

**CAUTION!**

Change control slot configuration in an operating, stable system cautiously and with a back-out plan. After changing a control slot configuration, monitor the system closely for problems as well as improvements in system performance.

The recommended number of control slots is as stated in [Table 49](#) or [Table 50](#).

Table 49: Control slot settings for all FSK APs in cluster

Number of SMs that Register to the AP	Number of Control Slots Recommended
1 to 10	1
11 to 50	2
51 to 150	4
151 to 200	6

Table 50: Control slot settings for all OFDM APs in cluster

Number of SMs that Register to the AP	Number of Control Slots Recommended
1 to 10	2
11 to 50	4
51 to 150	6
151 to 200	8

This field indicates the number of (reserved) control slots configured by the operator. Control slots are half the size of data slots. The SM uses reserved control slots and unused data slots for bandwidth requests.

If too few reserved control slots are specified, then latency increases in high traffic periods. If too many are specified, then the maximum capacity is unnecessarily reduced.

In a typical cluster, each AP should be set to the same number of control slots to assure proper timing in the send and receive cycles. However, where high incidence of small packets exists, as in a sector that serves several VoIP streams, additional control slots may provide better results. For APs in a cluster of mismatched control slots settings, or where OFDM and FSK APs of the same frequency band are collocated, use the frame calculator. See [Using the Frame Calculator Tool \(All\) for Collocation](#) on Page 446.

Broadcast Repeat Count

The default is 2 repeats (in addition to the original broadcast packet, for a total of 3 packets sent for every one needed), and is settable to 1 or 0 repeats (2 or 1 packets for every broadcast).

ARQ (Automatic Repeat reQuest) is not present in downlink broadcast packets, since it would cause unnecessary uplink traffic from every SM for each broadcast packet. For successful transport without ARQ, the AP repeats downlink broadcast packets. The SMs filter out all repeated broadcast packets and, thus, do not transport further.

The default of 2 repeats is optimum for typical uses of the network as an internet access system. In applications with heavy download broadcast such as video distribution, overall throughput is significantly improved by setting the repeat count to 1 or 0. This avoids flooding the downlink with repeat broadcast packets.

External Filters Delay

This parameter is present in only 900-MHz modules and can have effect in only those that have interference mitigation filter(s). Leave this value set to **0**, regardless of whether the AP has an interference mitigation filter.

Transmit Frame Spreading

As [Figure 75](#) on [Page 233](#) displays, the GUI of the 900-MHz AP includes this parameter. However, this feature has been ineffective in 900-MHz APs. Thus, the following description applies to APs only in the other frequency band ranges.

Where multiple AP clusters operate in the same frequency band range and same geographical area, select **Enable**. Then SMs between two APs can register in the assigned AP (do not register in another AP).

Where multiple AP clusters *do not* operate in the same frequency band range and same geographical area, select **Disable**, but observe the following caveat.



IMPORTANT!

SM throughput is 10% greater with this feature disabled. However, if you disable **Transmit Frame Spreading** where this feature was previously enabled, monitor the zone for interference over a period of days to ensure that this action has not made any SMs sensitive to the wrong beacon.

With this selection enabled, the AP does not transmit a beacon in each frame, but rather transmits a beacon in only pseudo-random frames in which the SM expects the beacon. This allows multiple APs to send beacons to multiple SMs in the same range without interference.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- Both 900-MHz and 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance.
- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.

- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power. In the 5.4-GHz PMP 400 Series OFDM AP, transmitter output power is settable in the range of -30 to 15 dBm. However, with only the integrated antenna, where regulation⁷ requires that EIRP is not greater than 27 dBm, compliance requires that the transmitter output power is set to 10 dBm or less. With a 12 dBi external antenna on the connectorized version of this AP, the full range (up to 15 dBm) is acceptable.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant with national or regional regulations.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see [Adjusting Transmitter Output Power](#) on Page 330.

The Radio tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

⁷ This is the case in most regions, including the U.S.A., Europe, and Canada.

18.1.4 SNMP Tab of the AP

An example of the SNMP tab of the AP is displayed in [Figure 77](#).

Configuration => SNMP
5.7GHz - Access Point - 0a-00-3e-d5-b9-97

Save Changes

SNMP Community Strings

SNMP Community String 1 : Canopy
 SNMP Community String 1 Permissions : Read Only Read / Write
 SNMP Community String 2 (Read Only) : Canopy

SNMP Accessing Addresses

Accessing IP / Subnet Mask 1 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 2 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 3 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 4 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 5 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 6 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 7 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 8 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 9 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 10 :	0.0.0.0	/ 0

Trap Addresses

Trap Address 1 :	0.0.0.0
Trap Address 2 :	0.0.0.0
Trap Address 3 :	0.0.0.0
Trap Address 4 :	0.0.0.0
Trap Address 5 :	0.0.0.0
Trap Address 6 :	0.0.0.0
Trap Address 7 :	0.0.0.0
Trap Address 8 :	0.0.0.0
Trap Address 9 :	0.0.0.0
Trap Address 10 :	0.0.0.0

Trap Enable

Sync Status : Enabled Disabled
 Session Status : Enabled Disabled

Site Information

Site Name : No Site Name
 Site Contact : No Site Contact
 Site Location : No Site Location

Save Changes
Reboot

Figure 77: SNMP tab of AP, example

You may set the SNMP tab parameters as follows.

SNMP Community String 1

Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

SNMP Community String 1 Permissions

You can designate the **SNMP Community String 1** to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.

SNMP Community String 2 (Read Only)

Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is **Canopy2**. This password will never authenticate a user or an NMS to read/write access.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet, Trap Address**, and **Permission** parameters.

Accessing IP / Subnet Mask 1 to 10

Specify the addresses that are allowed to send SNMP requests to this AP. The NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the AP, presuming that the device supplies the correct **Community String** value.

The default treatment is to allow all networks access. For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.” You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.

Trap Address 1 to 10

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which SNMP traps should be sent. Traps inform Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when an NMS attempts to access agent information but either
 - supplied an inappropriate community string or SNMP version number.
 - is associated with a subnet to which access is disallowed.

Trap Enable, Sync Status

If you want sync status traps (sync lost and sync regained) sent to Prizm or an NMS, select **Enabled**. If you want these traps suppressed, select **Disabled**.

Trap Enable, Session Status

If you want session status traps sent to Prizm or an NMS, select **Enabled**. For the names and descriptions of session status traps, see [Traps Provided in the Canopy Enterprise MIB](#) on Page 410. If you want these traps suppressed, select **Disabled**.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by PrizmEMS or an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by PrizmEMS or an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by PrizmEMS or an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.1.5 Quality of Service (QoS) Tab of the AP

An example of the Quality of Service (QoS) tab of the AP is displayed in [Figure 78](#).

Configuration => Quality of Service (QoS)

2.4GHz - Access Point - 0a-00-3e-23-20-66

Save Changes

AP Bandwidth Settings

(Uplink + Downlink) Sustained Data Rate <= 40000 kbps	
Sustained Uplink Data Rate :	20000 (kbps) (Range: 0— 40000 kbps)
Uplink Burst Allocation :	500000 (kbits) (Range: 0— 500000 kbits)
Sustained Downlink Data Rate :	20000 (kbps) (Range: 0— 40000 kbps)
Downlink Burst Allocation :	500000 (kbits) (Range: 0— 500000 kbits)
Broadcast Downlink CIR :	200 (kbps) (Range: 0— 2333 kbps)

Save Changes

Reboot

Figure 78: Quality of Service (QoS) tab of AP, example

In the Quality of Service (QoS) tab, you may set AP bandwidth parameters as follows.

Sustained Uplink Data Rate

Specify the rate that each SM registered to this AP is replenished with credits for transmission. This default imposes no restriction on the uplink. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Uplink Burst Allocation

Specify the maximum amount of data to allow each SM to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Sustained Downlink Data Rate

Specify the rate at which the AP should be replenished with credits (tokens) for transmission to each of the SMs in its sector. This default imposes no restriction on the uplink. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Downlink Burst Allocation

Specify the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the **Sustained Downlink Data Rate**. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Broadcast Downlink CIR

Broadcast Downlink CIR (Committed Information Rate, a minimum) supports some system designs where downlink broadcast is desired to have higher priority than other traffic. For many other system designs, especially typical internet access networks, leave the Broadcast Downlink CIR at the default.

Broadcast Downlink CIR is closely related to the **Broadcast Repeat Count** parameter, which is settable in the Radio tab of the Configuration page in the AP: when the **Broadcast Repeat Count** is changed, the total of available bandwidth is also changed, since packets are being sent one, two, or three times, according to the setting in the **Broadcast Repeat Count** parameter. (See **Broadcast Repeat Count** on Page 238.) This relationship is shown in [Table 51](#).

Table 51: Broadcast Downlink CIR achievable per Broadcast Repeat Count

Broadcast Repeat Count	Number of times each packet is sent	Highest Achievable Value for Broadcast Downlink CIR
0	1	7000 kbps
1	2	3500 kbps
2	3	2333 kbps

The Quality of Server (QoS) tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.1.6 Security Tab of the AP

An example of the Security tab of the AP is displayed in [Figure 79](#).

The screenshot shows a web-based configuration interface for an AP. On the left is a navigation menu with options like Home, Configuration, Statistics, Tools, Account, Quick Start, Copyright, and Logoff. The main content area is titled 'Configuration => Security' and shows settings for a '2.4GHz - Access Point - 0a-00-3e-20-a5-36'. The 'Security' tab is active in the top navigation bar. The configuration is organized into several sections:

- Authentication Server Settings:** Authentication Mode is set to 'Authentication Disabled' (selected). Authentication Server 1, 2, and 3 fields are empty.
- Airlink Security:** Encryption is set to 'Enabled' (selected).
- Encrypted Downlink Broadcast Configuration:** Encrypt Downlink Broadcast is set to 'Disabled' (selected).
- AP Evaluation Configuration:** SM Display of AP Evaluation Data is set to 'Enable Display' (selected).
- Session Timeout:** Web, Telnet, FTP Session Timeout is set to 600 Seconds.
- IP Access Filtering:** IP Access Control is set to 'IP Access Filtering Disabled - Allow access from all IP addresses' (selected). Allowed Source IP 1, 2, and 3 fields are all set to 0.0.0.0.

At the bottom of the configuration area, there are 'Save Changes' and 'Reboot' buttons.

Figure 79: Security tab of AP, example

In the Security tab of the AP, you may set the following parameters.

Authentication Mode

If the AP has authentication capability, then you can use this field to select from among the following authentication modes:

- **Authentication Disabled**—the AP requires no SMS to authenticate.
- **Authentication Required**—the AP requires any SM that attempts registration to be authenticated in BAM or Prizm before registration.

If the AP *does not* have authentication capability, then this parameter displays **Authentication Not Available**.

Authentication Server 1 to 3

If either BAM or the BAM subsystem in Prizm is implemented and the AP has authentication capability, enter the IP address of one or more BAM servers that perform authentication for SMS registered to this AP. Enter these in order of primary, secondary, then tertiary.

Encryption

Specify the type of air link security to apply to this AP:

- **Encryption Disabled** provides no encryption on the air link. This is the default mode.
- **Encryption Enabled** provides encryption, using a factory-programmed secret key that is unique for each module.

Encrypt Downlink Broadcast

When **Encryption Enabled** is selected in the **Airlink Security** parameter (described above) and **Enable** is selected in the **Encrypt Downlink Broadcast** parameter, the AP encrypts downlink broadcast packets as

- DES where the AP is DES capable.
- AES where the AP is AES capable.

For more information about the Encrypt Downlink Broadcast feature, see [Encrypting Downlink Broadcasts](#) on Page 387.

SM Display of AP Evaluation Data

You can use this field to suppress the display of data about this AP on the AP Evaluation tab of the Tools page in all SMS that register.

Web, Telnet, FTP Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the AP.

IP Access Control

You can permit access to the AP from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address, including access and management by Prizm.

Allowed Source IP 1 to 3

If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the AP from any IP address. You may populate as many as all three.

If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

The Security tab of the AP also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.1.7 VLAN Tab of the AP

An example of the AP VLAN tab is displayed in [Figure 80](#).

General | IP | Radio | SNMP | Quality of Service (QoS) | Security | Time | **VLAN** | VLAN Membership

DiffServ | Unit Settings

Home
 Configuration
 Statistics
 Tools
 Account
 Quick Start
 Copyright
 Logoff
 Account: admin
 Level:
 ADMINISTRATOR

Configuration => VLAN

5.4GHz OFDM - Access Point - 0a-00-3e-30-01-d4

Save Changes

VLAN Configuration

VLAN : Enabled
 Disabled

Always use Local VLAN Config : Enabled
 Disabled
 (NOTE: If you want to run spectrum analysis on this AP, enable this option to keep VLAN settings intact when booting as an SM.)

Dynamic Learning : Enabled
 Disabled

Allow Frame Types : All Frames

VLAN Aging Timeout : 25 Minutes (Range : 5 — 1440 Minutes)

Management VID : 1 (Range : 1 — 4094)

SM Management VID Pass-through : Disable
 Enable
 (NOTE: If disabled, all MVID traffic ingressing or egressing at SM wired interface will be dropped.)

Active Configuration

Active Configuration Untagged Ingress VID : 1
 Management VID : 1
 SM Management VID Passthrough : Enabled
 Dynamic Ageing Timeout : 25
 Allow Learning : Yes
 Allow Frame Type : All Frame Types

Current VID Member Set:

VID Number	Type	Age
1	Permanent	0

Save Changes

Reboot

Figure 80: VLAN tab of AP, example

In the VLAN tab of the AP, you may set the following parameters.

VLAN

Specify whether VLAN functionality for the AP and all linked SMs should (**Enabled**) or should not (**Disabled**) be allowed. The default value is **Disabled**.

Always use Local VLAN Config

Enable this option before you reboot this AP as an SM to use it to perform spectrum analysis. After the spectrum analysis is completed and before you reboot this module as an AP, disable this option.

Dynamic Learning

Specify whether the AP should (**Enabled**) or should not (**Disabled**) add the VLAN IDs (VIDs) of upstream frames to the VID table. (The AP passes frames with VIDs that are stored in the table both upstream and downstream.) The default value is **Enabled**.

Allow Frame Types

Select the type of arriving frames that the AP should tag, using the VID that is stored in the **Untagged Ingress VID** parameter. The default value is **All Frames**.

VLAN Aging Timeout

Specify how long the AP should keep dynamically learned VLANs. The range of values is 5 to 1440 (minutes). The default value is **25** (minutes).



NOTE:

VLANs that you enter for the **Management VID** and **VLAN Membership** parameters do not time out.

Management VID

Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4095. The default value is **1**.

SM Management VID Pass-through

Specify whether to allow the SM (**Enable**) or the AP (**Disable**) to control the VLAN settings of the SM. The default value is **Enable**.



CAUTION!

Do not set this parameter to **Enable** where both

- a BAM release earlier than 2.1 is implemented.
- the **Configuration Source** parameter in the AP is set to **BAM**.

This combination causes the SMs to become unmanageable, until you gain direct access with an override plug and remove this combination from the AP configuration.

When VLAN is enabled in the AP, the Active Configuration block provides the following details as read-only information in this tab. In the Motorola fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

Active Configuration Untagged Ingress VID

Some switches refer to this parameter as the Port VLAN ID. This is the VID that the AP will use for tagging frames of the type specified by **Allow Frame Types**.

Next, the following fields simply summarize how the VLAN features are currently configured:

Management VID

This is the value of the parameter of the same name, configured above.

SM Management VID Pass-Through

This is the value of the parameter of the same name, configured above.

Dynamic Ageing Timeout

This is the value of the **VLAN Aging Timeout** parameter configured above.

Allow Learning

Yes is displayed if the value of the **Dynamic Learning** parameter above is **Enabled**.

No is displayed if the value of **Dynamic Learning** is **Disabled**.

Allow Frame Type

This displays the selection that was made from the drop-down list at the **Allow Frame Types** parameter above.

Current VID Member Set, VID Number

This column lists the ID numbers of the VLANs in which this module is a member, whether through assignment or through dynamic learning.

Current VID Member Set, Type


For each VID number in the first column, the entry in this column correlates the way in which the module became and continues to be a member:

- **Permanent**—This indicates that the module was assigned the VID number through direct configuration by the operator.
- **Dynamic**—This indicates that the module adopted the VID number through enabled dynamic learning, when a tagged packet from an SM behind it in the network, or from a customer equipment that is behind the SM in this case, was read.

Current VID Member Set, Age

For each VID number in the first column of the table, the entry in this column reflects whether or when the VID number will time out:

- for **Permanent** type—the number will never time out, and this is indicated by the digit 0.
- for **Dynamic** type—the **Age** reflects what is configured in the **VLAN Aging Timeout** parameter in the Configuration => VLAN tab of the AP or reflects a fewer number of minutes that represents the difference between what was configured and what has elapsed since the VID was learned. Each minute, the Age decreases by one until, at zero, the AP deletes the learned VID, but can it again from packets sent by elements that are beneath it in the network.



IMPORTANT!

Values in this Active Configuration block can differ from attempted values in configurations:

- A VLAN profile administered by the BAM subsystem in Prizm is capable of overriding any configured VLAN value, if the **Configuration Source** parameter in the AP is set to **Authentication Server**.
- The AP itself can override the value that the SM has configured for **SM Management VID Pass-Through**.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.1.8 VLAN Membership Tab of the AP

An example of the VLAN Membership tab of the AP is displayed in [Figure 81](#).

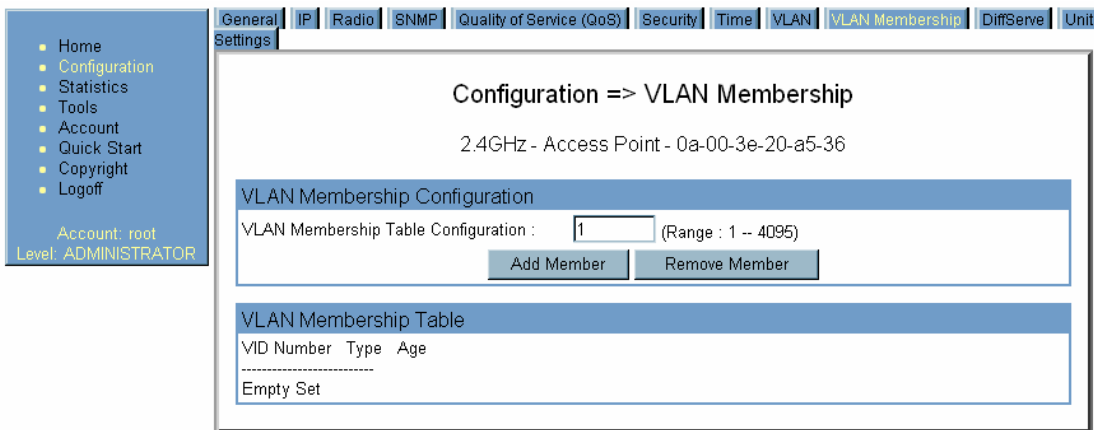


Figure 81: VLAN Membership tab of AP, example

You may set the VLAN Membership tab parameter as follows.

VLAN Membership Table Configuration

For each VLAN in which you want the AP to be a member, enter the VLAN ID and then click the **Add Member** button. Similarly, for any VLAN in which you want the AP to no longer be a member, enter the VLAN ID and then click the **Remove Member** button.

18.1.9 DiffServe Tab of the AP

An example of the DiffServe tab of the AP is displayed in [Figure 82](#).

Account: root
Level: ADMINISTRATOR

General | IP | Radio | SNMP | Quality of Service (QoS) | Security | Time | VLAN | VLAN Membership | DiffServe | Unit Settings

Configuration => DiffServe

2.4GHz - Access Point - 0a-00-3e-20-a5-36

DiffServe Configuration							
CodePoints (00) -- (07):							
CP00 : 0	CP01 : 0	CP02 : 0	CP03 : 0	CP04 : 4	CP05 : 4	CP06 : 4	CP07 : 4
CodePoints (08) -- (15):							
CP08 : 0	CP09 : 0	CP10 : 0	CP11 : 0	CP12 : 4	CP13 : 4	CP14 : 4	CP15 : 4
CodePoints (16) -- (23):							
CP16 : 0	CP17 : 0	CP18 : 0	CP19 : 0	CP20 : 4	CP21 : 4	CP22 : 4	CP23 : 4
CodePoints (24) -- (31):							
CP24 : 0	CP25 : 0	CP26 : 0	CP27 : 0	CP28 : 4	CP29 : 4	CP30 : 4	CP31 : 4
CodePoints (32) -- (39):							
CP32 : 0	CP33 : 0	CP34 : 0	CP35 : 0	CP36 : 4	CP37 : 4	CP38 : 4	CP39 : 4
CodePoints (40) -- (47):							
CP40 : 0	CP41 : 0	CP42 : 0	CP43 : 0	CP44 : 4	CP45 : 4	CP46 : 4	CP47 : 4
CodePoints (48) -- (55):							
CP48 : 6	CP49 : 0	CP50 : 0	CP51 : 0	CP52 : 4	CP53 : 4	CP54 : 4	CP55 : 4
CodePoints (56) -- (63):							
CP56 : 7	CP57 : 0	CP58 : 0	CP59 : 0	CP60 : 4	CP61 : 4	CP62 : 4	CP63 : 4

CodePoint Select :

Priority Select :

Save Changes

Reboot

Figure 82: DiffServe tab of AP, example

You may set the following DiffServe tab parameters.

**CodePoint 1
through
CodePoint 47**

The default priority value for each settable CodePoint is shown in [Figure 115](#). Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

**CodePoint 49
through
CodePoint 55**

**CodePoint 57
through
CodePoint 63**

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the AP for all downlinks within the sector and in the SM for each uplink. See [DSCP Field](#) on Page 90.

The DiffServe tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.1.10 Unit Settings Tab of the AP

An example of the Unit Settings tab of the AP is shown in [Figure 83](#).

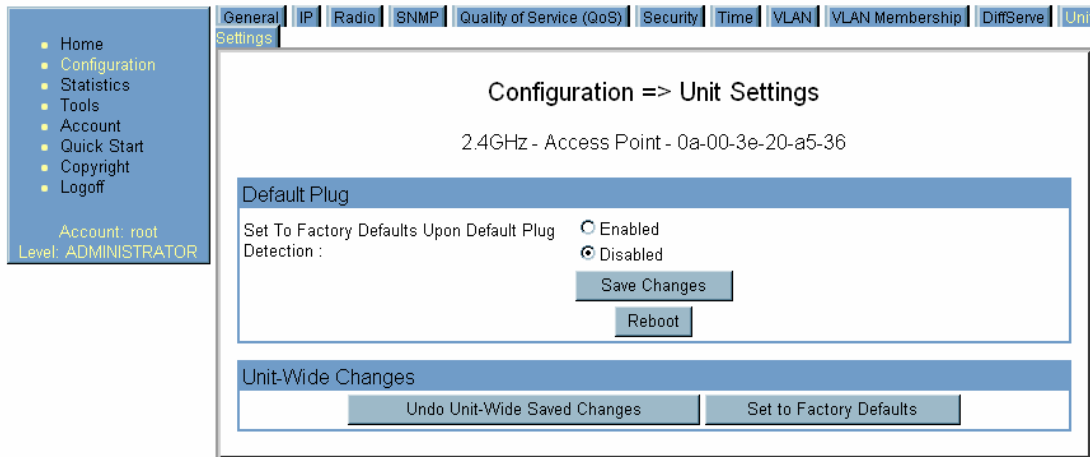


Figure 83: Unit Settings tab of AP, example

The Unit Settings tab of the AP contains an option for how the AP should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See [Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH](#) on Page 383.

The Unit Settings tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Undo Unit-Wide Saved Changes

When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

18.2 CONFIGURING AN SM FOR THE DESTINATION

If an ADMINISTRATOR-level password has been set in the SM, you must log into the module before you can configure its parameters. See [Managing Module Access by Passwords](#) on Page 381.

18.2.1 General Tab of the SM

An example of a General tab in the SM is displayed in [Figure 84](#).



Figure 84: General tab of SM, example

In the General tab of the SM, you may set the following parameters.

Link Speeds

From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

Ethernet Link Enable/Disable

Specify whether to enable or disable Ethernet/802.3 connectivity on the wired port of the SM. This parameter has no effect on the wireless link. When you select **Enable**, this feature allows traffic on the Ethernet/802.3 port. This is the factory default state of the port. When you select **Disable**, this feature prevents traffic on the port. Typical cases of when you may want to select **Disable** include:

- The subscriber is delinquent with payment(s).
- You suspect that the subscriber is sending or flooding undesired broadcast packets into the network, such as when
 - a virus is present in the subscriber's computing device.
 - the subscriber's home router is improperly configured.

Region Code

This parameter allows you to set the region in which the radio will operate. When the appropriate region has been set, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see [Radar Signature Detection and Shutdown](#) on Page 133.

The slave radio automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this parameter should always be set to the value that corresponds to the local region.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the AP encounters no activity with the SM (whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is 25 minutes.

**CAUTION!**

An inappropriately low **Bridge Entry Timeout** setting may lead to temporary loss of communication with some end users.

SM Power Up Mode With No 802.3 Link

This parameter is present in only PMP 100 Series SMs. Specify the default mode in which this SM will power up when the SM senses no Ethernet link. Select either

- **Power Up in Aim Mode**—the SM boots in an aiming mode. When the SM senses an Ethernet link, this parameter is automatically reset to Power Up in Operational Mode. When the module senses no Ethernet link within 15 minutes after power up, the SM carrier shuts off.
- **Power Up in Operational Mode**—the SM boots in Operational mode. The module attempts registration. This is the default selection.

2X Rate

This parameter is present in only PMP 100 Series (FSK) SMs. Whatever value that you set in this parameter is overridden by a lock-down to 1X operation, if that is configured in the AP. In some cases, disabling this parameter facilitates aiming. Be aware that a lock-down to 1X in the AP locks down the uplink and downlink between the AP and all SMs in its sector, and thus would affect traffic and performance across the entire sector. Hence, a temporary lock-down for aiming is better done in the individual SM. See [2X Operation](#) on Page 92.

Dynamic Rate Adapt

This parameter is present in only PMP 400 Series (OFDM) SMs. Whatever value that you set in this parameter is overridden by a lock-down to 1X or 2X operation, if that is configured in the AP. As with the **2X Rate** parameter in a PMP 100 Series SM, a temporary lock-down to facilitate aiming may be helpful. Be aware that a lock-down to 1X or 2X in the AP locks down the uplink and downlink between the AP and all SMs in its sector, and thus would affect traffic and performance across the entire sector. Hence, a temporary lock-down for aiming is better done in the individual SM. See [2X Operation](#) on Page 92 and [3X Operation](#) on Page 95.

Frame Timing Pulse Gated

If this SM extends the sync pulse to a BH master or an AP, select either

- **Enable**—If this SM loses sync from the AP, then *do not* propagate a sync pulse to the BH timing master or other AP. This setting prevents interference in the event that the SM loses sync.
- **Disable**—If this SM loses sync from the AP, then propagate the sync pulse to the BH timing master or other AP.

See [Wiring to Extend Network Sync](#) on Page 378.

The General tab also contains the following buttons.

Multicast Destination Address

Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMMmicro, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the **Multicast Destination Address** parameter value in the connected device that has it populated.

In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to **LLDP Multicast**. Set this parameter in the SM to **Broadcast**. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.

Where the AP is not behind another device, the **Broadcast** mode will allow discovery of the AP.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.2.2 NAT and IP Tabs of the SM with NAT Disabled

An example of the NAT tab in an SM with NAT disabled is displayed in [Figure 85](#).

- Home
- Configuration
- Statistics
- Tools
- Logs
- Account
- PDA
- Copyright
- Logoff
- Account: admin
- Level: ADMINISTRATOR

[General](#) | [IP](#) | [Radio](#) | [SNMP](#) | [Quality of Service \(QoS\)](#) | [Security](#) | [VLAN](#) | [VLAN Membership](#) | [DiffServ](#)
[Protocol Filtering](#) | [NAT](#) | [PPPoE](#) | [NAT Port Mapping](#) | [Unit Settings](#)

Configuration => NAT

5.2GHz - Subscriber Module - 0a-00-3e-04-99-42

NAT Enable [-]

NAT Enable/Disable : Enabled Disabled

WAN Interface [-]

Connection Type : v

IP Address :

Subnet Mask :

Gateway IP Address :

Reply to Ping on WAN Interface : Enabled Disabled

LAN Interface [-]

IP Address :

Subnet Mask :

DMZ Enable : Enabled Disabled

DMZ IP Address :

LAN DHCP Server [-]

DHCP Server Enable/Disable : Enabled Disabled

DHCP Server Lease Timeout : Days (Range : 1 — 30)

DHCP Start IP :

Number of IP's to Lease :

DNS IP Address : Obtain Automatically (From WAN DHCP or PPPoE) Set Manually

Preferred DNS IP Address :

Alternate DNS IP Address :

Remote Configuration Interface [-]

Interface Enable/Disable : Enabled Disabled

Connection Type : DHCP Static IP

IP Address :

Subnet Mask :

Gateway IP Address :

NAT Protocol Parameters [-]

ARP Cache Timeout : Minutes (Range : 1 — 30)

TCP Session Garbage Timeout : Minutes (Range : 4 — 1440)

UDP Session Garbage Timeout : Minutes (Range : 1 — 1440)

Figure 85: NAT tab of SM with NAT disabled, example

This implementation is illustrated in [Figure 45](#) on Page 161. In the NAT tab of an SM with NAT disabled, you may set the following parameters.

NAT Enable/Disable

This parameter enables or disabled the Network Address Translation (NAT) feature for the SM. NAT isolates devices connected to the Ethernet/wired side of an SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic separate from its address for management, terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet/wired side of the SM. For further information, see [Network Address Translation \(NAT\)](#) on Page 160 and [NAT and IP Tabs of the SM with NAT Enabled](#) on Page 265.

When NAT is enabled, VLANs are not supported on the wired side of that SM. You can enable NAT in SMs within a sector where VLAN is enabled in the AP, but this may constrain network design.

WAN Interface, Connection Type

This parameter is not configurable when NAT is disabled.

WAN Interface, IP Address

This field displays the IP address for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.

WAN Interface, Subnet Mask

This field displays the subnet mask for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.

WAN Interface, Gateway IP Address

This field displays the gateway IP address for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.

WAN Interface, Reply to Ping on WAN Interface

This parameter is not configurable when NAT is disabled.

LAN Interface, IP Address

This parameter is not configurable when NAT is disabled.

LAN Interface, Subnet Mask

This parameter is not configurable when NAT is disabled.

LAN Interface, DMZ Enable

This parameter is not configurable when NAT is disabled.

LAN Interface, DMZ IP Address

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, DHCP Server Enable/Disable

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, DHCP Server Lease Timeout

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, DHCP Start IP

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, Number of IPs to Lease

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, DNS IP Address

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, Preferred DNS IP Address

This parameter is not configurable when NAT is disabled.

LAN DHCP Server, Alternate DNS IP Address

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, Interface Enable/Disable

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, Connection Type

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, IP Address

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, Subnet Mask

This parameter is not configurable when NAT is disabled.

Remote Configuration Interface, Gateway IP Address

This parameter is not configurable when NAT is disabled.

NAT Protocol Parameters, ARP Cache Timeout

If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 minutes.

NAT Protocol Parameters, TCP Session Garbage Timeout

Where a large network exists behind the SM, you can set this parameter to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates.

NAT Protocol Parameters, UDP Session Garbage Timeout

You may adjust this parameter in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 minutes.

The NAT tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

An example of the IP tab in an SM with NAT disabled is displayed in [Figure 86](#).

The screenshot shows a web interface for configuring a Subscriber Module (SM). The top navigation bar includes tabs for General, IP, Radio, SNMP, Quality of Service (QoS), Security, VLAN, and VLAN Membership. The IP tab is selected, and sub-tabs for DiffServe, Protocol Filtering, NAT, NAT Port Mapping, and Unit Settings are visible. The main content area is titled 'Configuration => IP' and shows '5.2GHz Adjustable Power - Subscriber Module - 0a-00-3e-01-13-10'. Below this is the 'LAN1 Network Interface Configuration' section with the following fields:

- IP Address : [Empty text box]
- Network Accessibility : Public, Local
- Subnet Mask : [255.255.255.0]
- Gateway IP Address : [Empty text box]
- DHCP state : Enabled, Disabled

At the bottom of the configuration area are two buttons: 'Save Changes' and 'Reboot'.

Figure 86: IP tab of SM with NAT disabled, example

This implementation is illustrated in [Figure 45](#) on Page 161. In the IP tab of an SM with NAT disabled, you may set the following parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this SM. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See [Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH](#) on Page 383.



RECOMMENDATION:

Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Network Accessibility

Specify whether the IP address of the SM should be visible to only a device connected to the SM by Ethernet (**Local**) or should be visible to the AP as well (**Public**).

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the SM to communicate on the network. The default subnet mask is 255.255.0.0. See [Allocating Subnets](#) on Page 166.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the SM to communicate with the network. The default gateway is 169.254.0.0.

LAN1 Network Interface Configuration, DHCP state

If you select **Enabled**, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.

In this tab, DHCP State is settable only if the **Network Accessibility** parameter in the IP tab is set to **Public**. This parameter is also settable in the NAT tab of the Configuration web page, but only when NAT is enabled.

If the **DHCP state** parameter is set to **Enabled** in the Configuration => IP tab of the SM, *do not* check the **BootpClient** option for **Packet Filter Types** in its Protocol Filtering tab, because doing so would block the DHCP request. (Filters apply to all packets that leave the SM via its RF interface, including those that the SM itself generates.) If you want to keep DHCP enabled and avoid the blocking scenario, select the **Bootp Server** option instead. This will result in responses being appropriately filtered and discarded.

The IP tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.2.3 NAT and IP Tabs of the SM with NAT Enabled

An example of the NAT tab in an SM with NAT enabled is displayed in [Figure 87](#).

The screenshot displays the NAT configuration interface for a subscriber module. On the left is a navigation sidebar with links: Home, Configuration, Statistics, Tools, Logs, Account, PDA, Copyright, and Logoff. Below these links, it shows 'Account: admin' and 'Level: ADMINISTRATOR'. The main content area has a breadcrumb trail: General > IP > Radio > SNMP > Quality of Service (QoS) > Security > VLAN > VLAN Membership > DiffServ > Protocol Filtering > NAT > PPPoE > NAT Port Mapping > Unit Settings. The title is 'Configuration => NAT' for '5.2GHz - Subscriber Module - 0a-00-3e-04-99-42'. The 'NAT Enable' section has 'NAT Enable/Disable' set to 'Enabled'. The 'WAN Interface' section shows 'Connection Type' as 'DHCP', 'IP Address' as '0.0.0.0', 'Subnet Mask' as '255.255.255.0', 'Gateway IP Address' as '0.0.0.0', and 'Reply to Ping on WAN Interface' as 'Disabled'. The 'LAN Interface' section shows 'IP Address' as '169.254.1.1', 'Subnet Mask' as '255.255.255.0', 'DMZ Enable' as 'Disabled', and 'DMZ IP Address' as '169.254.1.52'. The 'LAN DHCP Server' section has 'DHCP Server Enable/Disable' as 'Enabled', 'DHCP Server Lease Timeout' as '30 Days', 'DHCP Start IP' as '169.254.1.2', 'Number of IP's to Lease' as '50', 'DNS IP Address' as 'Obtain Automatically (From WAN DHCP or PPPoE)', 'Preferred DNS IP Address' as '0.0.0.0', and 'Alternate DNS IP Address' as '0.0.0.0'. The 'Remote Configuration Interface' section has 'Interface Enable/Disable' as 'Enabled', 'Connection Type' as 'Static IP', 'IP Address' as '192.168.1.28', 'Subnet Mask' as '255.255.255.0', and 'Gateway IP Address' as '192.168.1.1'. The 'NAT Protocol Parameters' section shows 'ARP Cache Timeout' as '20 Minutes', 'TCP Session Garbage Timeout' as '120 Minutes', and 'UDP Session Garbage Timeout' as '4 Minutes'. There are 'Save Changes' and 'Reboot' buttons at the bottom.

Figure 87: NAT tab of SM with NAT enabled, example

In the NAT tab of an SM with NAT enabled, you may set the following parameters.

NAT Enable/Disable

This parameter enables or disabled the Network Address Translation (NAT) feature for the SM. NAT isolates devices connected to the Ethernet/wired side of an SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic separate from its address for management, terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet/wired side of the SM. For further information, see [Network Address Translation \(NAT\)](#) on Page 160 and [NAT and IP Tabs of the SM with NAT Enabled](#) on Page 265.

When NAT is enabled, VLANs are not supported on the wired side of that SM. You can enable NAT in SMs within a sector where VLAN is enabled in the AP, but this may constrain network design.

WAN Interface

The WAN interface is the RF-side address for transport traffic.

WAN Interface, Connection Type

This parameter may be set to

- **Static IP**—when this is the selection, the following three parameters (**IP Address**, **Subnet Mask**, and **Gateway IP Address**) must all be properly populated.
- **DHCP**—when this is the selection, the information from the DHCP server configures the interface.
- **PPPoE**—when this is the selection, the information from the PPPoE server configures the interface.

WAN Interface, IP Address

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the IP address of the SM for RF transport traffic.

WAN Interface, Subnet Mask

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the subnet mask of the SM for RF transport traffic.

WAN Interface, Gateway IP Address

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the gateway IP address for the SM for RF transport traffic.

WAN Interface, Reply to Ping on WAN Interface

By default, the radio interface *does not* respond to pings. If you use a management system (such as Prizm or WM) that will occasionally ping the SM, set this parameter to **Enabled**.

LAN Interface

The LAN interface is both the management access through the Ethernet port and the Ethernet-side address for transport traffic. When NAT is enabled, this interface is redundantly shown as the **NAT Network Interface Configuration** on the IP tab of the Configuration web page in the SM.

LAN Interface, IP Address

Assign an IP address for SM management through Ethernet access to the SM. This address becomes the base for the range of DHCP-assigned addresses.

LAN Interface, Subnet Mask

Assign a subnet mask of 255.255.255.0 or a more restrictive subnet mask. Set only the last byte of this subnet mask. Each of the first three bytes is permanently set to 255.

LAN Interface, DMZ Enable

Either enable or disable DMZ for this SM. See [DMZ](#) on Page 160.

LAN Interface, DMZ IP Address

If you enable DMZ in the parameter above, set the last byte of the DMZ host IP address to use for this SM when DMZ is enabled. Only one such address is allowed. The first three bytes are identical to those of the NAT private IP address. Ensure that the device that should receive network traffic behind this SM is assigned this address. The system provides a warning if you enter an address within the range that DHCP can assign.

LAN DHCP Server

This is the server (in the SM) that provides an IP address to the device connected to the Ethernet port of the SM.

LAN DHCP Server, DHCP Server Enable/Disable

Select either

- **Enabled** to
 - allow this SM to assign IP addresses, subnet masks, and gateway IP addresses to attached devices.
 - assign a start address for DHCP.
 - designate how many IP addresses may be temporarily used (leased).
- **Disabled** to disallow the SM to assign addresses to attached devices.

The implementation of NAT with DHCP server is illustrated in [Figure 48](#) on Page 50. The implementation of NAT with DHCP client (**DHCP** selected as the **Connection Type** of the WAN interface) and DHCP server is illustrated in [Figure 46](#) on Page 162. The implementation of NAT without DHCP is illustrated in [Figure 49](#) on Page 165.

LAN DHCP Server, DHCP Server Lease Timeout

Based on network performance, enter the number of days between when the DHCP server assigns an IP address and when that address expires. The range of values for this parameter is 1 to 30 days. The default value is 30 days.

LAN DHCP Server, DHCP Start IP

If you will be enabling DHCP Server below, set the last byte of the starting IP address that the DHCP server will assign. The first three bytes are identical to those of the NAT private IP address.

LAN DHCP Server, Number of IPs to Lease

Enter how many IP addresses the DHCP server is allowed to assign. The default value is 50 addresses.

LAN DHCP Server, DNS IP Address

Select either

- **Obtain Automatically** to allow the system to set the IP address of the DNS server.
- **Set Manually** to enable yourself to set both a preferred and an alternate DNS IP address.

LAN DHCP Server, Preferred DNS IP Address

Enter the preferred DNS IP address to use when the **DNS IP Address** parameter is set to **Set Manually**.

LAN DHCP Server, Alternate DNS IP Address

Enter the DNS IP address to use when the **DNS IP Address** parameter is set to **Set Manually** and no response is received from the preferred DNS IP address.

Remote Configuration Interface, Interface Enable/Disable

If you want over-the-air management capability for the SM, select **Enabled**. If you want to limit management of the SM to its Ethernet interface, select **Disabled**.

Remote Configuration Interface

The Remote Configuration interface is the RF-side address for management by an EMS or NMS (Prizm or WM, for example).

Remote Configuration Interface, Interface Enable/Disable

When this interface is **Disabled**, the SM is not directly accessible by IP address, and management access is only through either

- the LAN (Ethernet) interface
- a link from an AP web page into the WAN (RF-side) interface.

When this interface is **Enabled**, you can configure management access through either

- a **Static IP** address
- an IP address that **DHCP** provides for the WAN interface.

Remote Configuration Interface, Connection Type

This parameter may be set to

- **Static IP**—when this is the selection, the following three parameters (**IP Address**, **Subnet Mask**, and **Gateway IP Address**) must all be properly populated.
- **DHCP**—when this is the selection, the information from the DHCP server configures the interface.

Remote Configuration Interface, IP Address

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the IP address of the SM for RF management traffic.

Remote Configuration Interface, Subnet Mask

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the subnet mask of the SM for RF management traffic.

Remote Configuration Interface, Gateway IP Address

If **Static IP** is set as the **Connection Type** of the WAN interface, then this parameter configures the gateway IP address for the SM for RF management traffic.

**RECOMMENDATION:**

Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

NAT Protocol Parameters, ARP Cache Timeout

If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 minutes.

NAT Protocol Parameters, TCP Session Garbage Timeout

Where a large network exists behind the SM, you can set this parameter to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates. The default value of this parameter is 120 minutes.

NAT Protocol Parameters, UDP Session Garbage Timeout

You may adjust this parameter in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 minutes.

The NAT tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

An example of the IP tab in an SM with NAT enabled is displayed in [Figure 88](#).

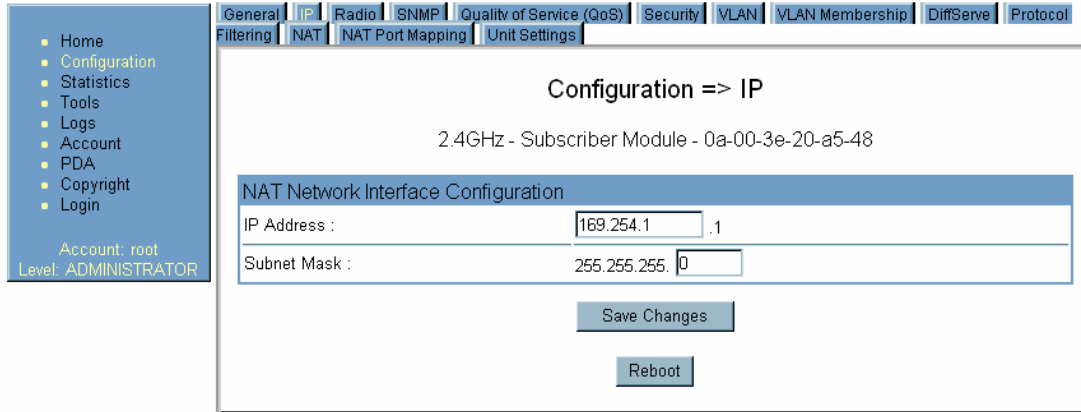


Figure 88: IP tab of SM with NAT enabled, example

In the IP tab of an SM with NAT enabled, you may set the following parameters.

NAT Network Interface Configuration, IP Address

Assign an IP address for SM management through Ethernet access to the SM. Set only the first three bytes. The last byte is permanently set to 1. This address becomes the base for the range of DHCP-assigned addresses.

NAT Network Interface Configuration, Subnet Mask

Assign a subnet mask of 255.255.255.0 or a more restrictive subnet mask. Set only the last byte of this subnet mask. Each of the first three bytes is permanently set to 255.

The IP tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

An example of the IP tab in an SM with NAT enabled is displayed in [Figure 88](#).

18.2.4 Radio Tab of the SM

An example of the Radio tab in the SM is displayed in [Figure 89](#).

The screenshot shows the 'Radio' configuration page for a 900MHz Subscriber Module. The page is titled 'Configuration => Radio' and includes a 'Save Changes' button. The configuration is divided into several sections:

- Radio Configuration:**
 - Custom Radio Frequency Scan Selection List: A list of frequencies from 906.0 to 924.0 MHz, each with a checked checkbox. The 'None' option is unchecked.
 - Color Code: A dropdown menu set to '5' (range 0-254).
 - Power Save Mode: Radio buttons for 'Enabled' (selected) and 'Disabled'.
- External Filters Delay:**
 - External Filters Delay: A dropdown menu set to '0' Nanoseconds.
- Transmitter Output Power:**
 - Transmitter Output Power: A dropdown menu set to '6' dBm (Range: 6 — 26 dBm).

At the bottom of the page, there are two buttons: 'Save Changes' and 'Reboot'.

Figure 89: Radio tab of SM, example

In the Radio tab of the SM, you may set the following parameters.

Custom Radio Frequency Scan Selection List

Check any frequency that you want the SM to scan for AP transmissions. The frequency *band* of the SM affects what channels you should select.



IMPORTANT!

In the 2.4-GHz frequency band, the SM can register to an AP that transmits on a frequency 2.5 MHz higher than the frequency that the SM receiver locks when the scan terminates as successful. This establishes a poor-quality link. To prevent this, select frequencies that are at least 5 MHz apart.

In a 2.4-GHz SM, this parameter displays all available channels, but has only three recommended channels selected by default. See [2.4-GHz AP Cluster Recommended Channels](#) on Page 139.

In a 5.2- or 5.4-GHz SM, this parameter displays only ISM frequencies. In a 5.7-GHz SM, this parameter displays both ISM and U-NII frequencies. If you select all frequencies that are listed in this field (default selections), then the SM scans for a signal on any channel. If you select only one, then the SM limits the scan to that channel. Since the frequencies that this parameter offers for each of these two bands are 5 MHz apart, a scan of *all* channels does not risk establishment of a poor-quality link as in the 2.4-GHz band.

A list of channels in the band is provided in [Considering Frequency Band Alternatives](#) on Page 138.

(The selection labeled **Factory** requires a special software key file for implementation.)

Color Code

Color code allows you to force the SM to register to only a specific AP, even where the SM can communicate with multiple APs. For registration to occur, the color code of the SM and the AP *must* match. Specify a value from 0 to 254.

Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).



RECOMMENDATION:

Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Power Save Mode

This mode significantly economizes on power consumption, and **Enabled** is the default setting. Disable this feature only under guidance from technical support.

External Filters Delay

This parameter is present in only 900-MHz modules and can have effect in only those that have interference mitigation filter(s). If this value is present, leave it set to **0**, regardless of whether the SM has an interference mitigation filter.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- Both 900-MHz and 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance.
- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.
- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant with national or regional regulations.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see [Adjusting Transmitter Output Power](#) on Page 330.

In 5.4-GHz OFDM links, the operator sets the **Transmitter Output Power parameter** in the AP, and the AP then manages the transmitter output power of the SM appropriately.

The Radio tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.2.5 SNMP Tab of the SM

An example of the SNMP tab in an SM is displayed in Figure 90.

The screenshot shows the configuration interface for the SNMP tab of a Subscriber Module (SM). The page title is "Configuration => SNMP" for a "2.4GHz - Subscriber Module - 0a-00-3e-23-20-67".

SNMP Community Strings:

- SNMP Community String 1: Canopy
- SNMP Community String 1 Permissions: Read Only, Read / Write
- SNMP Community String 2 (Read Only): Canopyro

SNMP Accessing Addresses:

Accessing IP / Subnet Mask 1 :	0.0.0.0	/	0
Accessing IP / Subnet Mask 2 :	0.0.0.0	/	0
Accessing IP / Subnet Mask 3 :	0.0.0.0	/	0
Accessing IP / Subnet Mask 4 :	0.0.0.0	/	0
Accessing IP / Subnet Mask 5 :	0.0.0.0	/	0
Accessing IP / Subnet Mask 6 :	0.0.0.0	/	0
Accessing IP / Subnet Mask 7 :	0.0.0.0	/	0
Accessing IP / Subnet Mask 8 :	0.0.0.0	/	0
Accessing IP / Subnet Mask 9 :	0.0.0.0	/	0
Accessing IP / Subnet Mask 10 :	0.0.0.0	/	0

Trap Addresses:

Trap Address 1 :	0.0.0.0
Trap Address 2 :	0.0.0.0
Trap Address 3 :	0.0.0.0
Trap Address 4 :	0.0.0.0
Trap Address 5 :	0.0.0.0
Trap Address 6 :	0.0.0.0
Trap Address 7 :	0.0.0.0
Trap Address 8 :	0.0.0.0
Trap Address 9 :	0.0.0.0
Trap Address 10 :	0.0.0.0

Site Information:

- Site Name : No Site Name
- Site Contact : No Site Contact
- Site Location : No Site Location

Buttons: Save Changes, Reboot

Figure 90: SNMP tab of SM, example

In the SNMP tab of the SM, you may set the following parameters.

SNMP Community String 1

Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

SNMP Community String 1 Permissions

You can designate the **SNMP Community String 1** to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.

SNMP Community String 2 (Read Only)

Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is **Canopy2**. This password will never authenticate a user or an NMS to read/write access.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet, Trap Address**, and **Permission** parameters.

Accessing IP / Subnet Mask 1 to 10

Specify the addresses that are allowed to send SNMP requests to this SM. Prizm or the NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the SM, presuming that the device supplies the correct **Community String** value.

The default treatment is to allow all networks access (set to 0). For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.” You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.



RECOMMENDATION:

The subscriber can access the SM by changing the subscriber device to the accessing subnet. This hazard exists because the **Community String** and **Accessing Subnet** are both visible parameters. To avoid this hazard, configure the SM to filter (block) SNMP requests. See [Filtering Protocols and Ports](#) on Page 385.

Trap Address 1 to 10

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which trap information should be sent. Trap information informs Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when Prizm or an NMS attempts to access agent information but either
 - supplied an inappropriate community string or SNMP version number.
 - is associated with a subnet to which access is disallowed.

Read Permissions

Select **Read Only** if you wish to disallow Prizm or NMS SNMP access to configurable parameters and read-only fields of the SM.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.2.6 Quality of Service (QoS) Tab of the SM

An example of the Quality of Service (QoS) tab in the SM is displayed in [Figure 91](#).

The screenshot shows the configuration page for the Quality of Service (QoS) tab of a Subscriber Module (SM). The page title is "Configuration => Quality of Service (QoS)" and the device identifier is "2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48".

MIR Bandwidth Settings
(Uplink + Downlink) Sustained Data Rate <= 40000 kbps

Sustained Uplink Data Rate :	<input type="text" value="3500"/>	(kbps) (Range: 0-- 40000 kbps)
Sustained Downlink Data Rate :	<input type="text" value="3500"/>	(kbps) (Range: 0-- 40000 kbps)
Uplink Burst Allocation :	<input type="text" value="500000"/>	(kbits) (Range: 0 -- 500000 kbits)
Downlink Burst Allocation :	<input type="text" value="500000"/>	(kbits) (Range: 0 -- 500000 kbits)

CIR Bandwidth Settings

Low Priority Uplink CIR :	<input type="text" value="0"/>	(kbps) (Range: 0 -- 20000 kbps)
Low Priority Downlink CIR :	<input type="text" value="0"/>	(kbps) (Range: 0 -- 20000 kbps)
Hi Priority Channel :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Hi Priority Uplink CIR :	<input type="text" value="0"/>	(kbps) (Range: 0 -- 20000 kbps)
Hi Priority Downlink CIR :	<input type="text" value="0"/>	(kbps) (Range: 0 -- 20000 kbps)

Buttons:

Figure 91: Quality of Service (QoS) tab of SM, example

In the Quality of Service (QoS) tab of the SM, you may set the following parameters.

Sustained Uplink Data Rate

Specify the rate that this SM is replenished with credits for transmission. This default imposes no restriction on the uplink. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Sustained Downlink Data Rate

Specify the rate at which the AP should be replenished with credits (tokens) for transmission to this SM. This default imposes no restriction on the uplink. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Uplink Burst Allocation

Specify the maximum amount of data to allow this SM to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Downlink Burst Allocation

Specify the maximum amount of data to allow the AP to transmit to this SM before the AP is replenished at the **Sustained Downlink Data Rate** with transmission credits. See

- [Maximum Information Rate \(MIR\) Parameters](#) on Page 87
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Low Priority Uplink CIR

See

- [Committed Information Rate](#) on Page 88
- [Setting the Configuration Source](#) on Page 292.

Low Priority Downlink CIR

See

- [Committed Information Rate](#) on Page 88
- [Setting the Configuration Source](#) on Page 292.

Hi Priority Channel

See

- [High-priority Bandwidth](#) on Page 89
- [Setting the Configuration Source](#) on Page 292.

Hi Priority Uplink CIR

See

- [High-priority Bandwidth](#) on Page 89
- [Committed Information Rate](#) on Page 88
- [Setting the Configuration Source](#) on Page 292.

Hi Priority Downlink CIR

See

- [High-priority Bandwidth](#) on Page 89
- [Committed Information Rate](#) on Page 88
- [Setting the Configuration Source](#) on Page 292.

The Quality of Service (QoS) tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made in this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.2.7 Security Tab of the SM

An example of the Security tab in an SM is displayed in [Figure 92](#).

The screenshot displays the 'Security' configuration page for a Subscriber Module (SM). The page title is 'Configuration => Security' and the device identifier is '2.4GHz - Subscriber Module - 0a-00-3e-23-20-67'. A 'Save Changes' button is located at the top right of the configuration area.

The configuration is organized into several sections:

- Authentication Key Settings:** Includes an 'Authentication Key' field (with a note '(Using All 0xFF's Key)'), a 'Select Key' section with radio buttons for 'Use Key above' and 'Use Default Key' (selected).
- Session Timeout:** Includes a 'Web, Telnet, FTP Session Timeout' field set to '600' seconds.
- SM Management Interface Access via Ethernet Port:** Includes an 'Ethernet Access' section with radio buttons for 'Enabled' (selected) and 'Disabled'.
- IP Access Filtering:** Includes an 'IP Access Control' section with radio buttons for 'IP Access Filtering Enabled - Only allow access from IP addresses specified below' and 'IP Access Filtering Disabled - Allow access from all IP addresses' (selected). Below this are three 'Allowed Source IP' fields, each containing '0.0.0.0'.

At the bottom of the configuration area, there are two buttons: 'Save Changes' and 'Reboot'. A left-hand navigation menu is visible, showing options like Home, Configuration, Statistics, Tools, Logs, Account, PDA, Copyright, Logoff, and user information (Account: admin, Level: ADMINISTRATOR).

Figure 92: Security tab of SM, example

In the Security tab of the SM, you may set the following parameters.

Authentication Key

Only if the AP to which this SM will register requires authentication, specify the key that the SM should use when authenticating. For alpha characters in this hex key, use only upper case.

Select Key

The **Use Default Key** selection specifies the predetermined key for authentication in BAM or Prizm. See [Authentication Manager Capability](#) on Page 391.

The **Use Key above** selection specifies the 32-digit hexadecimal key that is permanently stored on both the SM and the BAM or Prizm database.



NOTE:

The SM and BAM or Prizm pad the key of any length by the addition of leading zeroes, and if the entered keys match, authentication attempts succeed. However, Motorola recommends that you enter 32 characters to achieve the maximal security from this feature.

Web, Telnet, FTP Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the SM.

Ethernet Access Control

If you want to prevent any device that is connected to the Ethernet port of the SM from accessing the management interface of the SM, select **Ethernet Access Disabled**. This selection disables access through this port to via http (the GUI), SNMP, telnet, ftp, and tftp. With this selection, management access is available through only the RF interface via either an IP address (if **Network Accessibility** is set to **Public** on the SM) or the Session Status or Remote Subscribers tab of the AP.



NOTE:

This setting does not prevent a device connected to the Ethernet port from accessing the management interface of *other SMs* in the network. To prevent this, use the **IP Access Filtering Enabled** selection in the **IP Access Control** parameter of the SMs in the network. See **IP Access Control** below.

If you want to allow management access through the Ethernet port, select **Ethernet Access Enabled**. This is the factory default setting for this parameter.

IP Access Control

You can permit access to the SM from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address, including access and management by Prizm.

Allowed Source IP 1 to 3

If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the SM from any IP address. You may populate as many as all three.

If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

The Security tab of the SM also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.2.8 VLAN Tab of the SM

An example of the VLAN tab in an SM is displayed in [Figure 93](#).

Configuration → VLAN

5.7GHz OFDM - Subscriber Module - 0a-00-3e-3f-fe-48

Save Changes

VLAN Configuration

Dynamic Learning : Enabled
 Disabled

Allow Frame Types : All Frames

VLAN Aging Timeout : 25 Minutes (Range : 5 — 1440 Minutes)

Untagged Ingress VID : 770 (Range : 1 — 4094)

Management VID : 1 (Range : 1 — 4094)

SM Management VID Pass-through : Enable
 Disable
(NOTE: If disabled, all MVID traffic ingressing or egressing at SM wired interface will be dropped.)

Active Configuration

Active Configuration Untagged Ingress VID : 770
Management VID : 1
SM Management VID Passthrough : Enabled
Dynamic Ageing Timeout : 25
Allow Learning : Yes
Allow Frame Type : All Frame Types

Current VID Member Set:

VID Number	Type	Age
1	Permanent	0
770	Permanent	0

Figure 93: VLAN tab of SM, example

In the VLAN tab of an SM, you may set the following parameters.

Dynamic Learning

Specify whether the SM should (**Enable**) or should not (**Disable**) add the VIDs of upstream frames (that enter the SM through the wired Ethernet interface) to the VID table. The default value is **Enable**.

Allow Frame Types

Select the type of arriving frames that the SM should tag, using the VID that is stored in the **Untagged Ingress VID** parameter. The default value is **All Frames**.

VLAN Aging Timeout

Specify how long the SM should keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is **25** (minutes).

**NOTE:**

VIDs that you enter for the **Untagged Ingress VID** and **Management VID** parameters do not time out.

Untagged Ingress VID

Enter the VID that the SM(s) should use to tag frames that arrive at the SM(s) untagged. The range of values is 1 to 4095. The default value is **1**.

Management VID

Enter the VID that the SM should share with the AP. The range of values is 1 to 4095. The default value is **1**.

SM Management VID Pass-through

Specify whether to allow the SM (**Enable**) or the AP (**Disable**) to control the VLAN settings of this SM. The default value is **Enable**.

When VLAN is enabled in the AP to whom this SM is registered, the Active Configuration block provides the following details as read-only information in this tab. In the Motorola fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

Active Configuration Untagged Ingress VID

Some switches refer to this parameter as the Port VLAN ID. This is the VID that the SM will use for tagging frames that it receives as untagged.

Next, the following fields simply summarize how the VLAN features are currently configured:

Management VID

This is the value of the parameter of the same name, configured above.

SM Management VID Pass-Through

This is the value of the parameter of the same name, configured above.

Dynamic Ageing Timeout

This is the value of the **VLAN Aging Timeout** parameter configured above.

Allow Learning

Yes is displayed if the value of the **Dynamic Learning** parameter above is **Enabled**.
No is displayed if the value of **Dynamic Learning** is **Disabled**.

Allow Frame Type

This displays the selection that was made from the drop-down list at the **Allow Frame Types** parameter above.

Current VID Member Set, VID Number

This column lists the ID numbers of the VLANs in which this module is a member, whether through assignment or through dynamic learning.

Current VID Member Set, Type


For each VID number in the first column, the entry in this column correlates the way in which the module became and continues to be a member:

- **Permanent**—This indicates that the module was assigned the VID number through direct configuration by the operator.
- **Dynamic**—This indicates that the module adopted the VID number through enabled dynamic learning, when a tagged packet from an SM behind it in the network, or from a customer equipment that is behind the SM in this case, was read.

Current VID Member Set, Age

For each VID number in the first column of the table, the entry in this column reflects whether or when the VID number will time out:

- for **Permanent** type—the number will never time out, and this is indicated by the digit 0.
- for **Dynamic** type—the **Age** reflects what is configured in the **VLAN Aging Timeout** parameter in the Configuration => VLAN tab of the AP or reflects a fewer number of minutes that represents the difference between what was configured and what has elapsed since the VID was learned. Each minute, the Age decreases by one until, at zero, the AP deletes the learned VID, but can it again from packets sent by elements that are beneath it in the network.



IMPORTANT!

Values in this Active Configuration block can differ from attempted values in configurations:

- A VLAN profile administered by the BAM subsystem in Prizm is capable of overriding any configured VLAN value, if the **Configuration Source** parameter in the AP is set to BAM.
- The AP can override the value that the SM has configured for **SM Management VID Pass-Through**.

The VLAN tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.2.9 VLAN Membership Tab of the SM

An example of the VLAN Membership tab in an SM is displayed in [Figure 94](#).

Account: root
Level: ADMINISTRATOR

General | IP | Radio | SNMP | Quality of Service (QoS) | Security | VLAN | **VLAN Membership** | DiffServe | Protocol
Filtering | NAT | NAT Port Mapping | Unit Settings

Configuration => VLAN Membership

2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48

VLAN Membership Configuration

VLAN Membership Table Configuration : (Range : 1 -- 4095)

VLAN Membership Table

VID Number	Type	Age
10	Static	

Figure 94: VLAN Membership tab of SM, example

In the VLAN Membership tab, you may set the following parameter.

VLAN Membership Table Configuration

For each VLAN in which you want the AP to be a member, enter the VLAN ID and then click the **Add Member** button. Similarly, for any VLAN in which you want the AP to no longer be a member, enter the VLAN ID and then click the **Remove Member** button.

18.2.10 DiffServe Tab of the SM

An example of the DiffServe tab in an SM is displayed in [Figure 95](#).

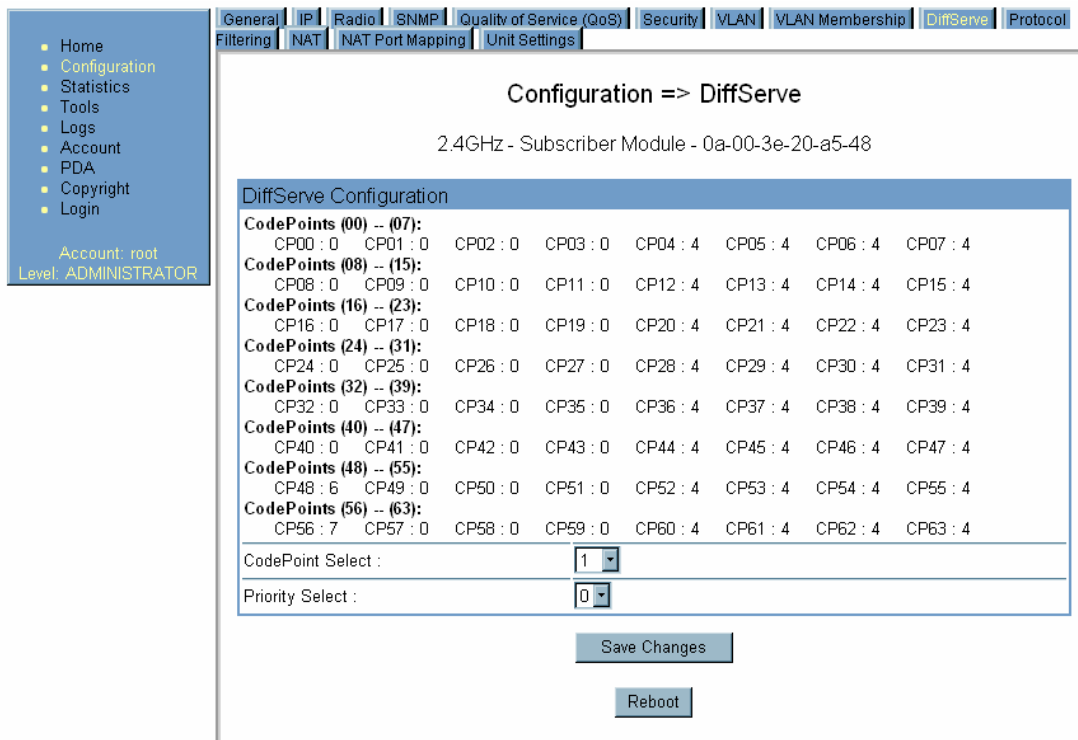


Figure 95: DiffServe tab of SM, example

In the DiffServe tab of the SM, you may set the following parameters.

CodePoint 1 through CodePoint 47

The default priority value for each settable CodePoint is shown in [Figure 115](#). Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the AP for all downlinks within the sector and in the SM for each uplink. See [DSCP Field](#) on [Page 90](#).

The DiffServe tab of the SM also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.2.11 Protocol Filtering Tab of the SM

An example of the Protocol Filtering tab in an SM is displayed in [Figure 96](#).

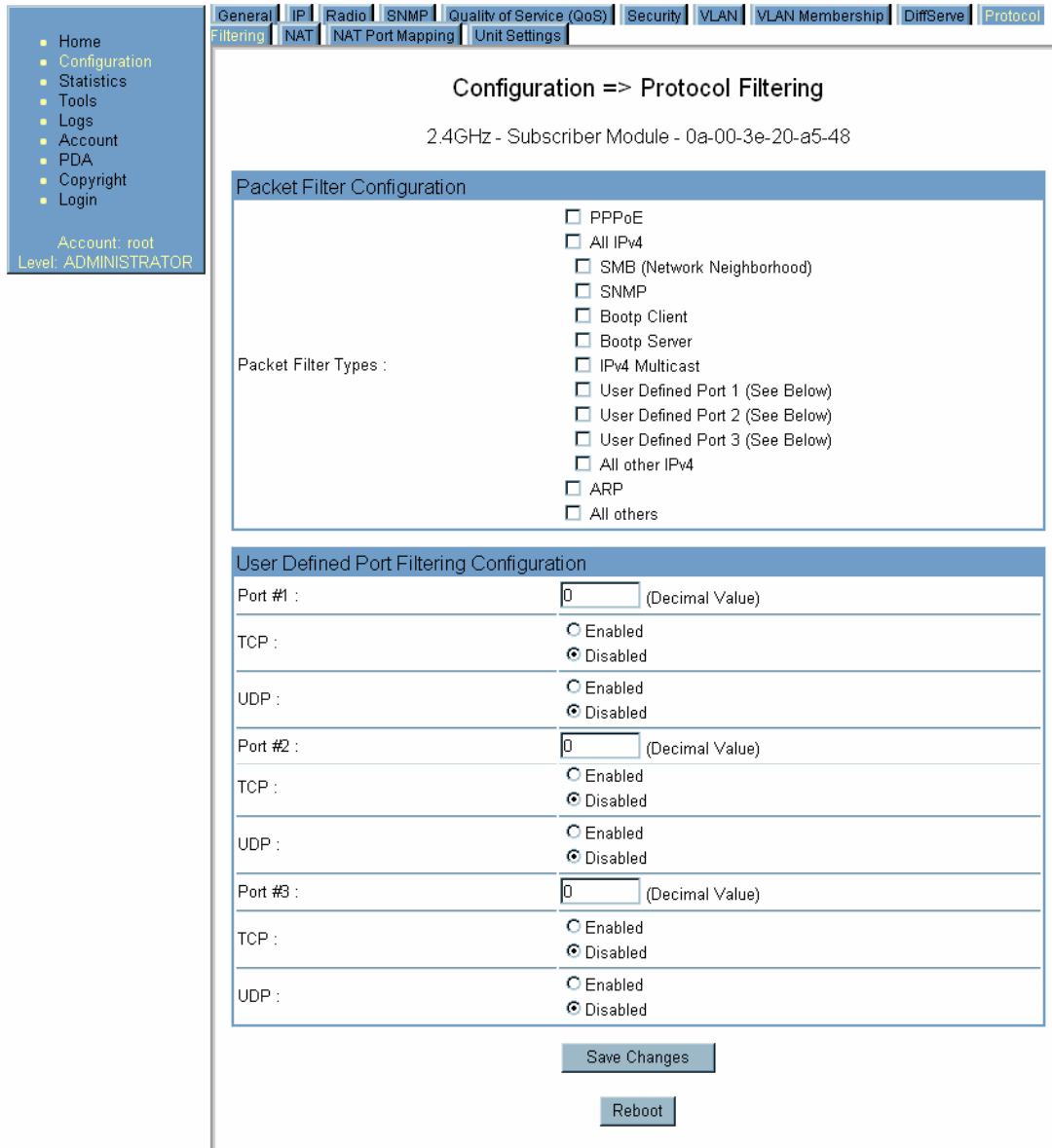


Figure 96: Protocol Filtering tab of SM, example

In the Protocol Filtering tab of the SM, you may set the following parameters.

Packet Filter Types

For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. Examples are provided in [Protocol and Port Filtering with NAT Disabled](#) on Page 385.

To filter packets in any of the user-defined ports, you must do all of the following:

- Check the box for **User Defined Port *n* (See Below)** in the **Packet Filter Types** section of this tab.
- In the **User Defined Port Filtering Configuration** section of this tab, both
 - provide a port number at **Port #*n***.
 - check **TCP, UDP**, or both.

If the **DHCP state** parameter is set to **Enabled** in the Configuration => IP tab of the SM, *do not* check the **Bootp Client** option for **Packet Filter Types** in its Protocol Filtering tab, because doing so would block the DHCP request. (Filters apply to all packets that leave the SM via its RF interface, including those that the SM itself generates.) If you want to keep DHCP enabled and avoid the blocking scenario, select the **Bootp Server** option instead. This will result in responses being appropriately filtered and discarded.

User Defined Port Filtering Configuration

You can specify ports for which to block subscriber access, regardless of whether NAT is enabled. For more information, see [Filtering Protocols and Ports](#) on Page 385.

18.2.12 PPPoE Tab of the SM

An example of the PPPoE tab of the SM is displayed in [Figure 97](#).

The screenshot shows the configuration page for PPPoE on a Subscriber Module (SM). The page title is "Configuration => PPPoE" and the device identifier is "5.4GHz - Subscriber Module - 0a-00-3e-52-14-8b". A "Save Changes" button is located below the title. The main configuration area is titled "PPPoE Configuration" and contains the following fields:

- PPPoE: Enabled, Disabled
- Access Concentrator:
- Service Name:
- Authentication Type: (dropdown menu)
- User Name: (dropdown menu)
- Password:
- MTU: (dropdown menu)
- Timer Type: (dropdown menu)
- Timer Period: (dropdown menu)
- TCP MSS Clamping: (dropdown menu)

Below the main configuration area is a section titled "PPPoE Manual Connect/Disconnect" with "Connect" and "Disconnect" buttons. At the bottom of the page are "Save Changes" and "Reboot" buttons.

Figure 97: PPPoE tab of SM, example

Point-to-Point Protocol over Ethernet (PPPoE) is a protocol that encapsulates PPP frames inside Ethernet frames (at Ethernet speeds). Benefits to the network operator may include

- Access control
- Service monitoring

- Generation of statistics about activities of the customer (see [Accessing PPPoE Statistics About Customer Activities \(SM\)](#) on Page 435)
- Re-use of infrastructure and operational practices by operators who already use PPP for other networks

18.2.13 NAT Port Mapping Tab of the SM

An example of the NAT Port Mapping tab in an SM is displayed in [Figure 98](#).

Configuration => NAT Port Mapping

2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48

Port Mapping Configuration			
Port Map 1 :	Port Number: <input type="text" value="0"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="169.254.1.1"/>
Port Map 2 :	Port Number: <input type="text" value="1"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="169.254.1.2"/>
Port Map 3 :	Port Number: <input type="text" value="2"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="169.254.1.3"/>
Port Map 4 :	Port Number: <input type="text" value="3"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="0.0.0.0"/>
Port Map 5 :	Port Number: <input type="text" value="4"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="0.0.0.0"/>
Port Map 6 :	Port Number: <input type="text" value="5"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="0.0.0.0"/>
Port Map 7 :	Port Number: <input type="text" value="6"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="0.0.0.0"/>
Port Map 8 :	Port Number: <input type="text" value="7"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="0.0.0.0"/>
Port Map 9 :	Port Number: <input type="text" value="8"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="0.0.0.0"/>
Port Map 10 :	Port Number: <input type="text" value="9"/>	Protocol: <input type="text" value="All Protocols"/>	IP: <input type="text" value="0.0.0.0"/>

Save Changes

Reboot

Figure 98: NAT Port Mapping tab of SM, example

In the NAT Port Mapping tab of the SM, you may set the following parameters.

Port Map 1 to 10

Separate parameters allow you to distinguish NAT ports from each other by assigning a unique combination of port number, protocol for traffic through the port, and IP address for access to the port.

18.2.14 Unit Settings Tab of the SM

An example of the Unit Settings tab in an SM is displayed in [Figure 99](#).

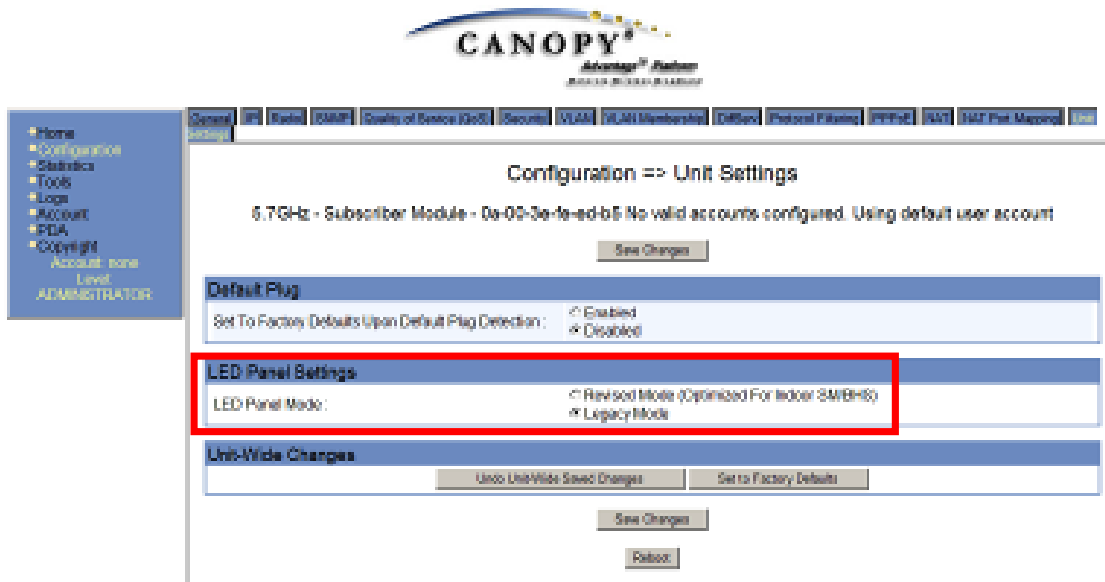


Figure 99: Unit Settings tab of SM, example

The Unit Settings tab of the SM contains an option for how the SM should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See [Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH](#) on Page 383.

LED Panel Mode

Optionally select Revised Mode for simpler use of the LEDs during alignment of the SM. See [Diagnostic LEDs](#) on Page 183.

The Unit Settings tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Unit-Wide Saved Changes

When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.3 SETTING THE CONFIGURATION SOURCE

The AP includes a **Configuration Source** parameter, which sets where SMs that register to the AP are controlled for MIR, VLAN, the high-priority channel, and CIR as follows. The **Configuration Source** parameter affects the source of

- all MIR settings:
 - **Sustained Uplink Data Rate**
 - **Uplink Burst Allocation**
 - **Sustained Downlink Data Rate**
 - **Downlink Burst Allocation**
- all SM VLAN settings:
 - **Dynamic Learning**
 - **Allow Only Tagged Frames**
 - **VLAN Ageing Timeout**
 - **Untagged Ingress VID**
 - **Management VID**
 - **VLAN Membership**
- the **Hi Priority Channel** setting
- all CIR settings
 - **Low Priority Uplink CIR**
 - **Low Priority Downlink CIR**
 - **Hi Priority Uplink CIR**
 - **Hi Priority Downlink CIR**

Most operators whose plans are typical should consult [Table 52](#).

Table 52: Recommended combined settings for typical operations

Most operators who use...	should set this parameter...	in this web page/tab...	in the AP to...
no BAM server	Authentication Mode	Configuration/ Security	Authentication Disabled
	Configuration Source	Configuration/ General	SM
Prizm with BAM server	Authentication Mode	Configuration/ Security	Authentication Required
	Configuration Source	Configuration/ General	Authentication Server

Operators whose plans are atypical should consider the results that are described in [Table 53](#) and [Table 54](#). For any SM whose **Authentication Mode** parameter is set to **Authentication Required**, the listed settings are derived as shown in [Table 53](#).

Table 53: Where feature values are obtained for an SM with authentication required

Configuration Source Setting in the AP	Values are obtained from			
	MIR Values	VLAN Values	High Priority Channel State	CIR Values
Authentication Server	BAM	BAM	BAM	BAM
SM	SM	SM	SM	SM
Authentication Server+SM	BAM	BAM, then SM	BAM, then SM	BAM, then SM

NOTES:

HPC represents the **Hi Priority Channel** (enable or disable).

Where *BAM, then SM* is the indication, parameters for which BAM does not send values are obtained from the SM. This is the case where the BAM server is operating on a BAM release that did not support the feature. This is also the case where the feature enable/disable flag in BAM is set to disabled. The values are those previously set or, if none ever were, then the default values.

Where *BAM* is the indication, values in the SM are disregarded.

Where *SM* is the indication, values that BAM sends for the SM are disregarded.

The high-priority channel is unavailable to Series P7 and P8 SMs.

For any SM whose **Authentication Mode** parameter is *not* set to **Authentication Required**, the listed settings are derived as shown in [Table 54](#).

Table 54: Where feature values are obtained for an SM with authentication disabled

Configuration Source Setting in the AP	Values are obtained from			
	MIR Values	VLAN Values	High Priority Channel State	CIR Values
Authentication Server	AP	AP	AP	AP
SM	SM	SM	SM	SM
Authentication Server+SM	SM	SM	SM	SM

BAM Release 2.0 sends only MIR values. BAM Release 2.1 and Prizm Release 2.0 and 2.1 send VLAN and high-priority channel values as well.

For the case where the **Configuration Source** parameter in the AP is set to **Authentication Server**, the SM stores a value for the **Dynamic Learning** VLAN parameter that differs from its factory default. When Prizm does not send VLAN values (because **VLAN Enable** is set to **No** in Prizm), the SM

- uses this stored **Disable** value for **Dynamic Learning**.
- shows the following in the VLAN Configuration web page:
 - *either* **Enable** or **Disable** as the value of the **Dynamic Learning** parameter.
 - **Allow Learning : No** under **Active Configuration**.

For the case where the **Configuration Source** parameter in the AP is set to **Authentication Server+SM**, and Prizm does not send VLAN values, the SM

- uses the configured value in the SM for **Dynamic Learning**. If the SM is set to factory defaults, then this value is **Enable**.
- shows under **Active Configuration** the result of the configured value in the SM. For example, if the SM is set to factory defaults, then the VLAN Configuration page shows **Allow Learning : Yes**.

This selection (**Authentication Server+SM**) *is not* recommended where Prizm manages the VLAN feature in SMs.

18.4 CONFIGURING A BH TIMING MASTER FOR THE DESTINATION



NOTE:

The PTP 400 and PTP 600 series bridges (previously known as 30/60 Mbps and 150/300 Mbps Backhubs) are described in their own dedicated user guides. See [Products Not Covered by This User Guide](#) on Page 34.

If an ADMINISTRATOR-level password has been set in the BHM, you must log into the module before you can configure its parameters. See [Managing Module Access by Passwords](#) on Page 381.

18.4.1 General Tab of the BHM

An example of the General tab in a BHM is displayed in [Figure 100](#).

The screenshot displays the 'Configuration => General' page for a BHM interface. The interface is titled '5.4GHz - Backhaul - Timing Master - 0a-00-3e-53-fa-b7'. A 'Save Changes' button is located at the top right. The configuration is organized into several sections, each with a collapse icon:

- Device Type:** Timing Mode is set to Timing Master and Timing Slave.
- Link Speeds:** Link Speed is set to 'Auto 100F/100H/10F/10H'.
- Sync Setting:** Sync Input is set to 'Sync to Received Signal (Power Port)'.
- Regional Settings:** Region Code is set to 'Europe'.
- Web Page Configuration:** Webpage Auto Update is set to '1' Seconds (0 = Disable Auto Update).
- Bridge Configuration:** Bridge Entry Timeout is set to '25' Minutes (Range : 25—1440 Minutes). Bridging Functionality is set to Enable and Disable.
- Update Application Information:** Update Application Address is set to '169.254.1.199'.
- MAC Control Parameters:** Dynamic Rate Adapt is set to '1x/2x'.
- TCP Settings:** Prioritize TCP ACK is set to Enabled and Disabled.
- Layer 2 Discovery Destination Address:** Multicast Destination Address is set to LLDP Multicast and Broadcast.

At the bottom of the page, there are two buttons: 'Save Changes' and 'Reboot'.

Figure 100: General tab of BHM, example

In the General tab of the BHM, you may set the following parameters.

Timing Mode

Select **Timing Master**. This BH will provide sync for the link. Whenever you toggle this parameter to Timing Master from Timing Slave, you should also do the following:

1. Make no other changes in this or any other interface page.
2. Save this change of timing mode.
3. Reboot the BH.

RESULT: The set of interface web pages that is unique to a BHM is made available.

Link Speed

From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

Sync Input

Specify the type of synchronization for this BH timing master to use.

- Select **Sync to Received Signal (Power Port)** to set this BHM to receive sync from a connected CMMmicro or CMM4.
- Select **Sync to Received Signal (Timing Port)** to set this BHM to receive sync from a connected CMM2, an AP in the cluster, an SM, or a BH timing slave.
- Select **Generate Sync Signal** where the BHM does not receive sync, and no AP or other BHM is active within the link range.

Region Code

From the drop-down list, select the region in which the radio is operating. Selectable regions are

- **Australia**
- **Brazil**
- **Canada**
- **Europe**
- **Russia**
- **United States**
- **Other**
- **None**

When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see [Radar Signature Detection and Shutdown](#) on Page 133.

Unlike selections in other parameters, your **Region Code** selection requires a **Save Changes** and a **Reboot** cycle before it will force the context-sensitive GUI to display related options (for example, **Alternate Frequency Carrier 1 and 2** in the Configuration => Radio tab). Thus, a proper configuration exercise in environments that are subject to DFS requirements has two imperative **Save Changes** and **Reboot** cycles: one after the **Region Code** is set, and a second after related options are set.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.



CAUTION!

An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

Bridging Functionality

Select whether you want bridge table filtering active (**Enable**) or not (**Disable**) on this BHM. Selecting **Disable** allows you to use redundant BHs without causing network addressing problems. Through a spanning tree protocol, this reduces the convergence time from 25 minutes to mere seconds. However, you should disable bridge table filtering as only a deliberate part of your overall network design. Otherwise, disabling it allows unwanted traffic across the wireless interface.

Update Application Address

For capabilities in future software releases, you can enter the address of the server to access for software updates on this BHM.

2X Rate

See [2X Operation](#) on Page 92.

Prioritize TCP ACK

To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. See [AP-SM Links](#) on Page 101.

The General tab of the BHM also provides the following buttons.

Multicast Destination Address

Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMMmicro, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the **Multicast Destination Address** parameter value in the connected device that has it populated.

In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to **LLDP Multicast**. Set this parameter in the BHM to **Broadcast**. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.

Where the AP is not behind another device, the **Broadcast** mode will allow discovery of the AP.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.2 IP Tab of the BHM

An example of an IP tab in a BHM is displayed in [Figure 101](#).

Figure 101: IP tab of BHM, example

You may set the following IP Configuration page parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to be associated with the Ethernet connection on this module. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See [Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 383](#).



RECOMMENDATION:

Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the BHM to communicate on the network. The default subnet mask is 255.255.0.0. See [Allocating Subnets on Page 166](#).

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the BHM to communicate with the network. The default gateway is 169.254.0.0.

LAN1 Network Interface Configuration, DHCP State

If you select **Enabled**, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.

LAN2 Network Interface Configuration (RF Private Interface), IP Address

Enter the IP address to be associated with this BHM for over-the-air access.

The IP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.3 Radio Tab of the BHM

An example of the Radio tab in a BHM is displayed in [Figure 102](#).

The screenshot shows the 'Radio' tab configuration page for a BHM. The page title is 'Configuration => Radio' and the device identifier is '5.4GHz - BackHaul - Timing Master - 0a-00-3e-51-60-23'. The configuration is divided into four main sections:

- Radio Configuration:**
 - Radio Frequency Carrier: 5560
 - Alternate Frequency Carrier 1: 5535
 - Alternate Frequency Carrier 2: 5510
 - Color Code: 0 (0--254)
 - Power Save Mode: Enabled, Disabled
 - Sector ID: 0
 - Downlink Data: 50 %
 - Schedule Whitening: Enable, Disable
- Power Control:**
 - External Antenna Gain: 0 dB (Range: 0 -- 35 dB)
- Scan Policy:**
 - Transmit Frame Spreading: Enabled, Disabled
- Transmitter Output Power:**
 - Transmitter Output Power: 23 dBm (Range: -3 -- 23 dBm)

At the bottom of the page, there are two buttons: 'Save Changes' and 'Reboot'.

Figure 102: Radio tab of BHM, example

In the Radio tab of the BHM, you may set the following parameters.

Radio Frequency Carrier

Specify the frequency for the BHM to transmit. The default for this parameter is **None**. (The selection labeled **Factory** requires a special software key file for implementation.) In a 5.7-GHz BHM, this parameter displays both ISM and U-NII frequencies. In a 5.2-GHz BHM, this parameter displays only ISM frequencies. For a list of channels in the band, see [Considering Frequency Band Alternatives](#) on Page 138.

Alternate Frequency Carrier 1

If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:

1. Click the General tab.
2. Set the **Region Code** parameter from its drop-down list.
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. Click the Radio tab.

From the drop-down list, select the frequency that the BHM should switch to if it detects a radar signature on the frequency configured in the **Radio Frequency Carrier** parameter. See [Radar Signature Detection and Shutdown](#) on Page 133.

Alternate Frequency Carrier 2

From the drop-down list, select the frequency that the BHM should switch to if it detects a radar signature on the frequency configured in the **Alternate Frequency Carrier 1** parameter. See [Radar Signature Detection and Shutdown](#) on Page 133.

Color Code

Specify a value from 0 to 254. For registration to occur, the color code of the BHM and the BHS *must* match. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).



RECOMMENDATION:

Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Power Save Mode

Select either

- **Enabled** (the default), to reduce module power consumption by approximately 10% without affecting the transmitter output power. This is the recommended setting.
- **Disabled**, to continue normal power consumption, but only under guidance from technical support.

Sector ID

You can optionally enter an identifier to distinguish this link.

Downlink Data

The operator specifies the percentage of the aggregate (uplink and downlink total) throughput that is needed for the downlink. The default for this parameter is 50%.

Schedule Whitening

Select either

- **Enable**, to spread the transmitted signal power to avoid peaks that modules with Dynamic Frequency Selection (DFS) configured might interpret as radar. This is the recommended setting.
- **Disable**, to allow peaks in transmitted signal power.

PTP 200 Series (OFDM) BHMs do not have this parameter.

External Antenna Gain

If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:

1. Click the **General** tab.
2. Set the **Region Code** parameter from its drop-down list.
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. Click the **Radio** tab.

Using [Table 55](#) as a guide, type in the dB value by which to reduce Dynamic Frequency Selection (DFS) sensitivity to radar signals.

Table 55: Recommended External Antenna Gain values for BHM

Module Type	Recommended Setting
PTP 100 with 9 dB Canopy LENS	9
PTP 100 with standard 18 dB reflector	18
PTP 100 connectorized with 15.5 dBi antenna and 0.5 dB cable loss	15

The value of this parameter does not affect transmitter output power. This parameter is present in only radios that support DFS.

Transmit Frame Spreading

If you select **Enable**, then a BHS between two BHMs can register in the assigned BHM (not the other BHM). Motorola *strongly recommends* that you select this option. With this selection, the BHM does not transmit a beacon in each frame, but rather transmits a beacon in only pseudo-random frames in which the BHS expects the beacon. This allows multiple BHMs to send beacons to multiple BHSs in the same range without interference.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance.
- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.
- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power. In the PTP54200 OFDM BHM, transmitter output power is settable in the range of -30 to 15 dBm. However, with only the integrated antenna, where regulation⁸ requires that EIRP is not greater than 27 dBm, compliance requires that the transmitter output power is set to 10 dBm or less. With a 12 dBi external antenna on the connectorized version of this BHM, the full range (up to 15 dBm) is acceptable.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant with national or regional regulations.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see [Adjusting Transmitter Output Power](#) on Page 330.

The Radio tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

⁸ This is the case in most regions, including the U.S.A., Europe, and Canada.

18.4.4 SNMP Tab of the BHM

An example of the SNMP tab in a BHM is displayed in [Figure 103](#).

The screenshot displays the SNMP configuration interface for a BHM. On the left is a navigation menu with the following items: Home, Configuration, Statistics, Tools, Account, Quick Start, Copyright, Logoff, Account: admin, Level: ADMINISTRATOR. The main configuration area is titled "Configuration => SNMP" and is for the device "5.7GHz - Backhaul - Timing Master - 0a-00-3e-fe-ed-d4".

The configuration is organized into several sections:

- SNMP Community Strings:** Contains two entries. "SNMP Community String 1" is set to "Canopy" with "Read Only" permissions selected. "SNMP Community String 2 (Read Only)" is set to "Canopy".
- SNMP Accessing Addresses:** A table with 10 rows, each for "Accessing IP / Subnet Mask" from 1 to 10. All values are currently "0.0.0.0 / 0".
- Trap Addresses:** A table with 10 rows, each for "Trap Address" from 1 to 10. All values are currently "0.0.0.0".
- Trap Enable:** Contains "Sync Status" and "Session Status", both with "Disabled" selected.
- Site Information:** Contains "Site Name", "Site Contact", and "Site Location", all with "No Site Name", "No Site Contact", and "No Site Location" respectively.

At the bottom of the configuration area, there are "Save Changes" and "Reboot" buttons.

Figure 103: SNMP tab of BHM, example

In the SNMP tab of the BHM, you may set the following parameters.

SNMP Community String 1

Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

SNMP Community String 1 Permissions

You can designate the **SNMP Community String 1** to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.

SNMP Community String 2 (Read Only)

Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is **Canopy2**. This password will never authenticate a user or an NMS to read/write access.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet, Trap Address**, and **Permission** parameters.

Accessing IP / Subnet Mask 1 to 10

Specify the addresses that are allowed to send SNMP requests to this BHM. Prizm or the NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the BHM, presuming that the device supplies the correct **Community String** value.



NOTE:

For more information on CIDR, execute an Internet search on "Classless Interdomain Routing."

The default treatment is to allow all networks access. You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.

Trap Address 1 to 10

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which trap information should be sent. Trap information informs Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when Prizm or an NMS attempts to access agent information but either
 - supplied an inappropriate community string or SNMP version number.
 - is associated with a subnet to which access is disallowed.

Trap Enable

Select either **Sync Status** or **Session Status** to enable SNMP traps. If you select neither, then traps are disabled.

Read Permissions

Select **Read Only** if you wish to disallow any parameter changes by Prizm or an NMS.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.5 Security Tab of the BHM

An example of the Security tab in a BHM is displayed in [Figure 104](#).

The screenshot shows the configuration interface for the Security tab of a BHM. At the top, there are navigation tabs: General, IP, Radio, SNMP, Security (selected), Time, VLAN, DiffServ, and Unit Settings. The main heading is 'Configuration => Security' with the device ID '5.7GHz - Backhaul - Timing Master - 0a-00-3e-fc-55-d9'. A 'Save Changes' button is located below the device ID.

The configuration is organized into several sections:

- Authentication Mode:**
 - Authentication Mode: Authentication Required, Authentication Disabled
 - Authentication Key: (Only Used if Authentication Required) (Using All 0xFF's Key)
- Airlink Security:**
 - Encryption: Enabled, Disabled
 - 24 Hour Encryption Refresh: Enable, Disable** (This section is highlighted with a red box in the image)
- BHM Evaluation Configuration:**
 - BHS Display of BHM Evaluation Data: Disable Display, Enable Display
- Session Timeout:**
 - Web, Telnet, FTP Session Timeout: Seconds
- IP Access Filtering:**
 - IP Access Control: IP Access Filtering Enabled - Only allow access from IP addresses specified below, IP Access Filtering Disabled - Allow access from all IP addresses
 - Allowed Source IP 1:
 - Allowed Source IP 2:
 - Allowed Source IP 3:

At the bottom of the page, there are two buttons: 'Save Changes' and 'Reboot'.

Figure 104: Security tab of BHM, example

In the Security tab of the BHM, you may set the following parameters.

Authentication Mode

Specify whether the BHM should require the BHS to authenticate.

Authentication Key

Only if you set the BHM in the previous parameter to require authentication, specify the key that the BHS should use when authenticating.

Encryption

Specify the type of air link security to apply to this BHM:

- **Encryption Disabled** provides no encryption on the air link. This is the default mode.
- **Encryption Enabled** provides encryption, using a factory-programmed secret key that is unique for each module.



NOTE:

In any BH link where encryption is enabled, the BHS briefly drops registration and re-registers in the BHM every 24 hours to change the encryption key.

24 Hour Encryption Refresh

A BHM that has encryption enabled forces its BHS to re-register once every 24 hours, during which the BHM refreshes the encryption key. This provides a level of security, but results in a brief but daily downtime. Since the refresh occurs in 24 hour increments that begin when the link is established, the only way to set a favorable the time of day (for example, 2:00 AM) for the key refresh is to reboot either the BHM or BHS at the favorable time.

When this feature is disabled, the key is refreshed upon only other re-registration events, such as a reboot. The default status of this feature is **Enable**.

The algorithm used in Advanced Encryption Standard (AES) encryption-capable radios is certified by the National Institute of Standards and Technology (NIST) to meet government Federal Information Processing Standard-197 (FIPS-197) for ensuring secure data communication. Refreshing the key at 24-hour intervals is not needed for AES radios to meet FIPS 197, but provides an level of security above the algorithm itself.

BHS Display of BHM Evaluation Data

You can use this field to suppress the display of data (**Disable Display**) about this BHM on the BHM Evaluation tab of the Tools page in the BHS.

Web, Telnet, FTP Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the BHM.

IP Access Control

You can permit access to the BHM from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address, including access and management by Prizm.

Allowed Source IP 1 to 3

If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the BHM from any IP address. You may populate as many as all three.

If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

The Security tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.6 VLAN tab of the BHM

An example of the VLAN tab in a BHM is displayed in [Figure 105](#).

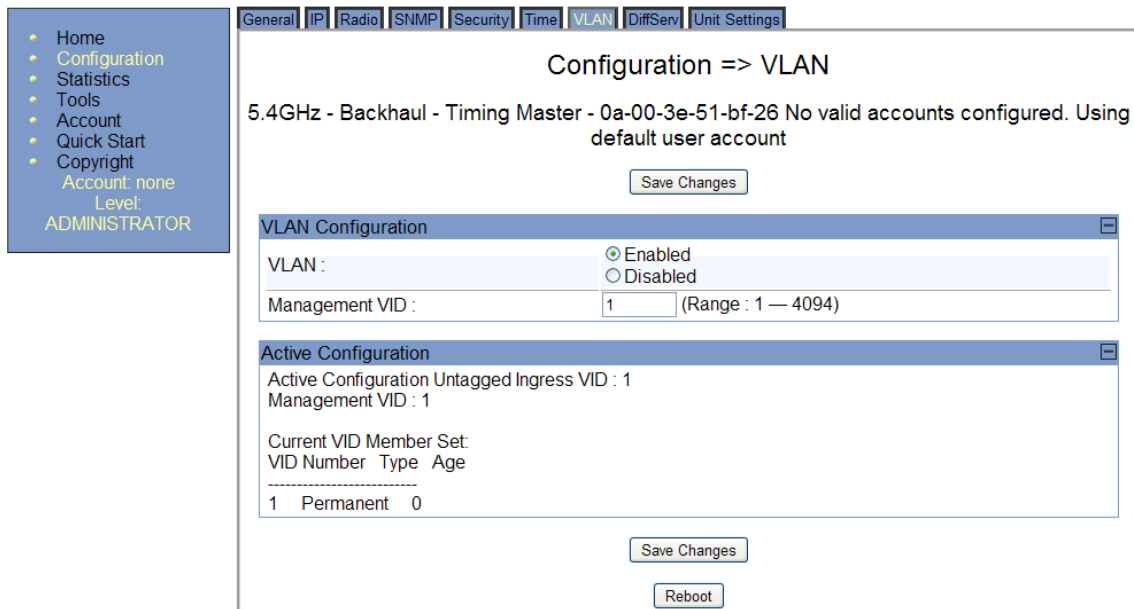


Figure 105: VLAN tab of BHM, example

In the VLAN tab of the BHM, you may set the following parameters.

VLAN

Set the **VLAN** feature to **Enabled** or **Disabled**. When the feature is disabled, the text box for the following parameter is inactive. When the **Management VID** is enabled by this parameter, the module is manageable through only packets that are tagged with the VID configured in that parameter. These parameters have no bearing on tagging in non-management traffic.

By default, **VLAN** is **Enabled** in backhaul modules. With this feature enabled, the backhaul becomes a permanent member of any VLAN VID that it reads in packets that it receives. When the backhaul reboots, it loses these memberships, but begins again to freely adopt memberships in the VIDs that will be permanent until the next reboot.

Management VID

Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4094. The default value is **1**. This text box is inactive if VLAN is set to **Disabled**. In the Motorola fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

The Active Configuration block provides the following details as read-only information in this tab.

Active Configuration Untagged Ingress VID

In a backhaul module, this value will always be 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

VID Number

In a backhaul module, this value will always be 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

Type

In a backhaul module, this value will always be Permanent, reflective of the fact that the backhaul is not capable of deleting any VID membership, regardless of whether it was learned or set.

Age

In a backhaul module, this value will always be 0, reflective of the fact that the backhaul is not capable of deleting any VID membership, regardless of whether it was learned or set.

The VLAN tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.7 DiffServe Tab of the BHM

An example of the DiffServe tab in a BHM is displayed in [Figure 106](#).

Account: root
Level: ADMINISTRATOR

General | IP | Radio | SNMP | Security | Time | **DiffServe** | Unit Settings

Configuration => DiffServe

2.4GHz - BackHaul - Timing Master - 0a-00-3e-20-71-19

DiffServe Configuration

CodePoints (00) -- (07):	CP00 : 0	CP01 : 0	CP02 : 0	CP03 : 0	CP04 : 4	CP05 : 4	CP06 : 4	CP07 : 4
CodePoints (08) -- (15):	CP08 : 0	CP09 : 0	CP10 : 0	CP11 : 0	CP12 : 4	CP13 : 4	CP14 : 4	CP15 : 4
CodePoints (16) -- (23):	CP16 : 0	CP17 : 0	CP18 : 0	CP19 : 0	CP20 : 4	CP21 : 4	CP22 : 4	CP23 : 4
CodePoints (24) -- (31):	CP24 : 0	CP25 : 0	CP26 : 0	CP27 : 0	CP28 : 4	CP29 : 4	CP30 : 4	CP31 : 4
CodePoints (32) -- (39):	CP32 : 0	CP33 : 0	CP34 : 0	CP35 : 0	CP36 : 4	CP37 : 4	CP38 : 4	CP39 : 4
CodePoints (40) -- (47):	CP40 : 0	CP41 : 0	CP42 : 0	CP43 : 0	CP44 : 4	CP45 : 4	CP46 : 4	CP47 : 4
CodePoints (48) -- (55):	CP48 : 6	CP49 : 0	CP50 : 0	CP51 : 0	CP52 : 4	CP53 : 4	CP54 : 4	CP55 : 4
CodePoints (56) -- (63):	CP56 : 7	CP57 : 0	CP58 : 0	CP59 : 0	CP60 : 4	CP61 : 4	CP62 : 4	CP63 : 4

CodePoint Select :

Priority Select :

Save Changes

Reboot

Figure 106: DiffServe tab of BHM, example

In the DiffServe tab of the BHM, you may set the following parameters.

**CodePoint 1
through
CodePoint 47**

The default priority value for each settable CodePoint is shown in [Figure 115](#). Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

**CodePoint 49
through
CodePoint 55**

Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

**CodePoint 57
through
CodePoint 63**

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the AP for all downlinks within the sector and in the SM for each uplink. See [DSCP Field](#) on Page 90.

The DiffServe tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.8 Unit Settings Tab of the BHM

An example of the Unit Settings tab of the BHM is displayed in [Figure 107](#).

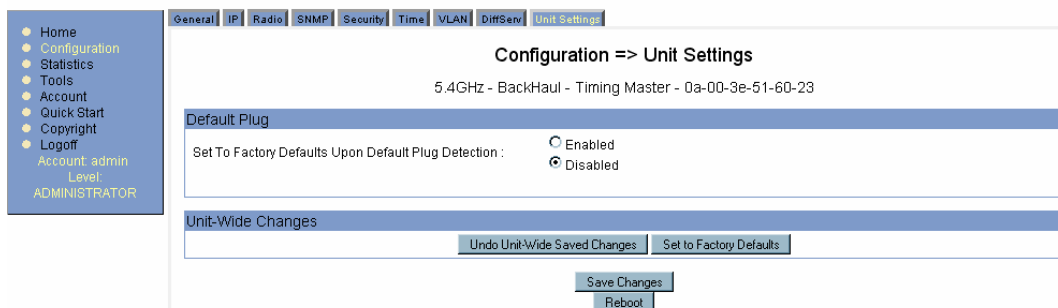


Figure 107: Unit Settings tab of BHM, example

The Unit Settings tab of the BHM contains an option for how the BHM should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults.

A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See [Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH](#) on Page 383.

The Unit Settings tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5 CONFIGURING A BH TIMING SLAVE FOR THE DESTINATION

If an ADMINISTRATOR-level password has been set in the BHS, you must log into the module before you can configure its parameters. See [Managing Module Access by Passwords](#) on Page 381.

18.5.1 General Tab of the BHS

An example of the General tab in a BHS is displayed in [Figure 108](#).

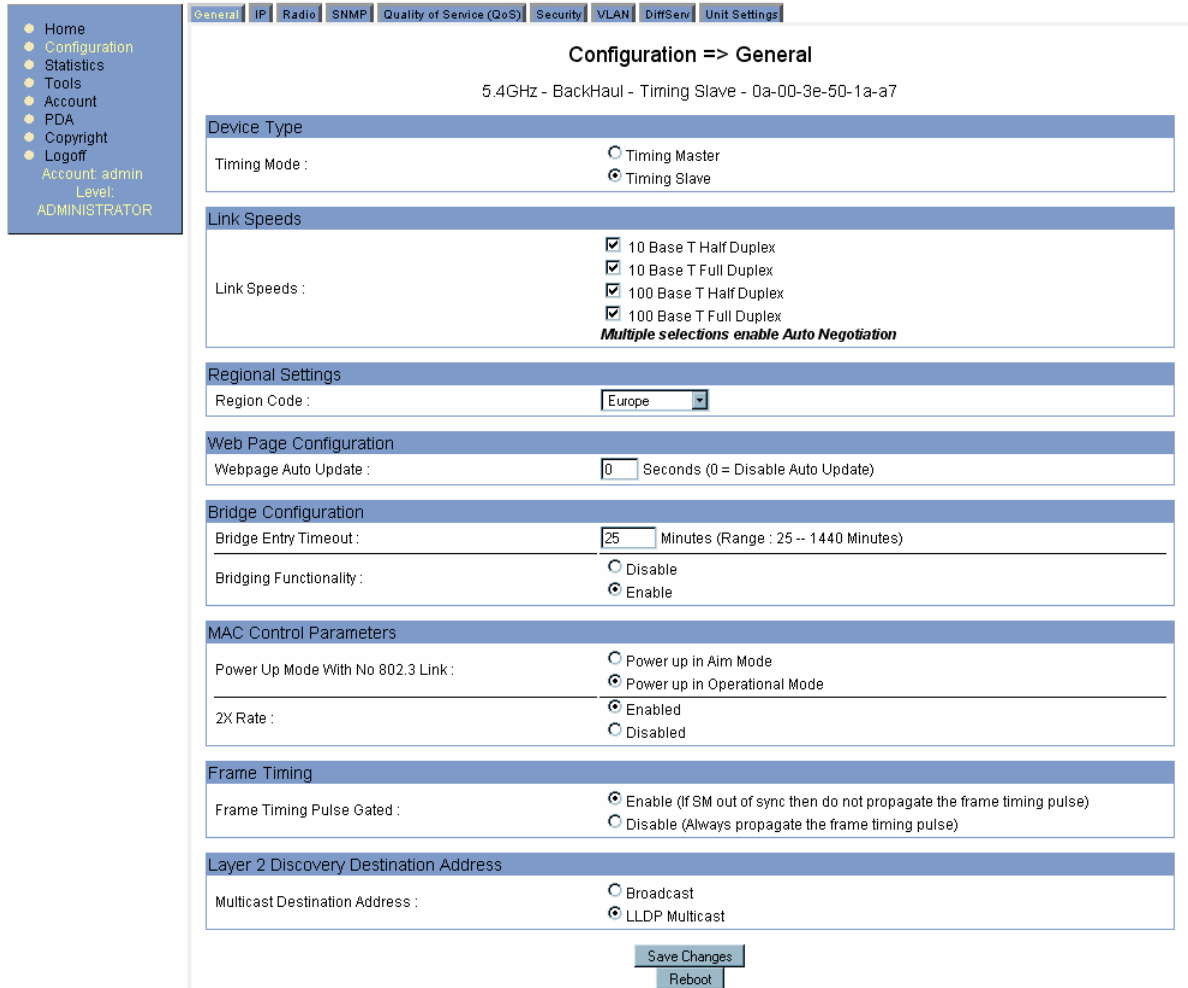


Figure 108: General tab of BHS, example


In the General tab of the BHS, you may set the following parameters.

Timing Mode

Select **Timing Slave**. This BH will receive sync from another source. Whenever you toggle this parameter to Timing Slave from Timing Master, you should also do the following:

1. Make no other changes in this or any other interface page.
2. Save this change of timing mode.
3. Reboot the BH.

RESULT: The set of interface web pages that is unique to a BHS is made available.



NOTE:
In a BHS that cannot be converted to a BHM, this parameter is not present.

Link Speeds

Specify the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHS, and SMs in the operator network.

Region Code

From the drop-down list, select the region in which the radio is operating. Selectable regions are

- **Australia**
- **Brazil**
- **Canada**
- **Europe**
- **Russia**
- **United States**
- **Other**
- **None**

When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. For further information on DFS, see [Radar Signature Detection and Shutdown](#) on Page 133.

The slave radio automatically inherits the DFS type of the master. This behavior ignores the value of the **Region Code** parameter in the slave, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), you should always set the value that corresponds to the local region.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the BHM encounters no activity with the BHS (whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is 25 minutes.



CAUTION!

An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

Bridging Functionality

Select whether you want bridge table filtering active (**Enable**) or not (**Disable**) on this BHS. Selecting **Disable** allows you to use redundant BHs without causing network addressing problems. Through a spanning tree protocol, this reduces the convergence time from 25 minutes to mere seconds. However, you should disable bridge table filtering as only a deliberate part of your overall network design. Otherwise, disabling it allows unwanted traffic across the wireless interface.

Power Up Mode With No 802.3 Link

Specify the default mode in which this BHS will power up when it senses no Ethernet link. Select either

- **Power Up in Aim Mode**—the BHS boots in an aiming mode. When the BHS senses an Ethernet link, this parameter is automatically reset to Power Up in Operational Mode. When the BHS senses no Ethernet link within 15 minutes after power up, the BHS carrier shuts off.
- **Power Up in Operational Mode**—the BHS boots in Operational mode and attempts registration. This is the default selection.

2X Rate

See [2X Operation](#) on Page 92.

Frame Timing Pulse Gated

If this BHS extends the sync pulse to a BHM or an AP behind it, select either

- **Enable**—If this BHS loses sync, then *do not* propagate a sync pulse to the BHM or AP. This setting prevents interference in the event that the BHS loses sync.
- **Disable**—If this BHS loses sync, then propagate the sync pulse anyway to the BHM or AP.

See [Wiring to Extend Network Sync](#) on Page 378.

The General tab also provides the following buttons.

Multicast Destination Address

Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMMmicro, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the **Multicast Destination Address** parameter value in the connected device that has it populated.

In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to **LLDP Multicast**. Set this parameter in the BHS to **Broadcast**. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.

Where the AP is not behind another device, the **Broadcast** mode will allow discovery of the AP.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.2 IP Tab of the BHS

An example of the IP tab in a BHS is displayed in [Figure 109](#).

The screenshot shows a web interface for configuring a BHS. On the left is a navigation menu with items: Home, Configuration, Statistics, Tools, Account, PDA, Copyright, and Login. Below the menu, it says 'Account: none' and 'Level: ADMINISTRATOR'. The main content area has a breadcrumb trail: 'General | IP | Radio | SNMP | Quality of Service (QoS) | Security | DiffServe | Unit Settings'. The current page is titled 'Configuration => IP' and shows the MAC address '2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af'. The 'LAN1 Network Interface Configuration' section includes:

- IP Address : [text input field]
- Subnet Mask : [text input field containing '255.255.0.0']
- Gateway IP Address : [text input field]
- DHCP state : Enabled, Disabled

 At the bottom of the configuration area are two buttons: 'Save Changes' and 'Reboot'.

Figure 109: IP tab of BHS, example

In the IP tab of the BHS, you may set the following parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this BHS. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See [Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH](#) on Page 383.

**RECOMMENDATION:**

Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the BHS to communicate on the network. The default subnet mask is 255.255.0.0. See [Allocating Subnets](#) on Page 166.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the BHS to communicate with the network. The default gateway is 169.254.0.0.

LAN1 Network Interface Configuration, DHCP State

If you select **Enabled**, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.

The IP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.3 Radio Tab of the BHS

An example of the Radio tab in a BHS is displayed in [Figure 110](#).

Configuration => Radio

5.4GHz - BackHaul - Timing Slave - 0a-00-3e-50-1a-a7

Radio Configuration

<input checked="" type="checkbox"/>	5495	<input checked="" type="checkbox"/>	5500	<input checked="" type="checkbox"/>	5505	<input checked="" type="checkbox"/>	5510	<input checked="" type="checkbox"/>	5515	<input checked="" type="checkbox"/>	5520	<input checked="" type="checkbox"/>	5525
<input checked="" type="checkbox"/>	5530	<input checked="" type="checkbox"/>	5535	<input checked="" type="checkbox"/>	5540	<input checked="" type="checkbox"/>	5545	<input checked="" type="checkbox"/>	5550	<input checked="" type="checkbox"/>	5555	<input checked="" type="checkbox"/>	5560
<input checked="" type="checkbox"/>	5565	<input checked="" type="checkbox"/>	5570	<input checked="" type="checkbox"/>	5575	<input checked="" type="checkbox"/>	5580	<input checked="" type="checkbox"/>	5585	<input checked="" type="checkbox"/>	5590	<input checked="" type="checkbox"/>	5595
<input checked="" type="checkbox"/>	5600	<input checked="" type="checkbox"/>	5605	<input checked="" type="checkbox"/>	5610	<input checked="" type="checkbox"/>	5615	<input checked="" type="checkbox"/>	5620	<input checked="" type="checkbox"/>	5625	<input checked="" type="checkbox"/>	5630
<input checked="" type="checkbox"/>	5635	<input checked="" type="checkbox"/>	5640	<input checked="" type="checkbox"/>	5645	<input checked="" type="checkbox"/>	5650	<input checked="" type="checkbox"/>	5655	<input checked="" type="checkbox"/>	5660	<input checked="" type="checkbox"/>	5665
<input checked="" type="checkbox"/>	5670	<input checked="" type="checkbox"/>	5675	<input checked="" type="checkbox"/>	5680	<input checked="" type="checkbox"/>	5685	<input checked="" type="checkbox"/>	5690	<input checked="" type="checkbox"/>	5695	<input checked="" type="checkbox"/>	5700
<input checked="" type="checkbox"/>	5705	<input type="checkbox"/>	None										

Color Code : (0--254)

Power Control

External Antenna Gain : dB (Range : 0 -- 35 dB)

Transmitter Output Power

Transmitter Output Power : dBm (Range: -3 -- 23 dBm)

Save Changes

Reboot

Figure 110: Radio tab of BHS, example

In the Radio tab of the BHS, you may set the following parameters.

Custom Radio Frequency Scan Selection List

Specify the frequency that the BHS should scan to find the BHM. The frequency *band* of the BHs affects what channels you select.



IMPORTANT!

In the 2.4-GHz frequency band, the BHS can register to a BHM that transmits on a frequency 2.5 MHz higher than the frequency that the BHS receiver locks when the scan terminates as successful. This establishes a poor-quality link. To prevent this, select frequencies that are at least 5 MHz apart.

In a 2.4-GHz BHS, this parameter displays all available channels, but has only three recommended channels selected by default. See [2.4-GHz AP Cluster Recommended Channels](#) on Page 139.

In a 5.2- or 5.4-GHz BHS, this parameter displays only ISM frequencies. In a 5.7-GHz BHS, this parameter displays both ISM and U-NII frequencies. If you select all frequencies that are listed (default selections), then the module scans for a signal on any channel. If you select only one, then the module limits the scan to that channel. Since the frequencies that this parameter offers for each of these two bands are 5 MHz apart, a scan of *all* channels does not risk establishment of a poor-quality link as in the 2.4-GHz band. Nevertheless, this can risk establishment of a link to the wrong BHM.

A list of channels in the band is provided in [Considering Frequency Band Alternatives](#) on Page 138.

(The selection labeled **Factory** requires a special software key file for implementation.)

Color Code

Specify a value from 0 to 254. For registration to occur, the color code of the BHM and the BHS *must* match. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).



RECOMMENDATION:

Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

External Antenna Gain

Using [Table 56](#) as a guide, type in the dB value by which to reduce Dynamic Frequency Selection (DFS) sensitivity to radar signals.

Table 56: Recommended External Antenna Gain values for BHS

Module Type	Recommended Setting
PTP 100 with 9 dB Canopy LENS	9
PTP 100 with standard 18 dB reflector	18
PTP 100 connectorized with 15.5 dBi antenna and 0.5 dB cable loss	15

The value of this parameter does not affect transmitter output power. This parameter is present in only radios that support DFS.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- Both 900-MHz and 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance.
- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.
- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.

- confirm that the initial power setting is compliant with national or regional regulations.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see [Adjusting Transmitter Output Power](#) on Page 330.

The Radio tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.4 SNMP Tab of the BHS

An example of the SNMP tab in a BHS is displayed in [Figure 111](#).

The screenshot shows the SNMP configuration interface for a BHS. The top navigation bar includes tabs for General, IP, Radio, **SNMP**, Quality of Service (QoS), Security, VLAN, DiffServ, and Unit Settings. The left sidebar contains a menu with options: Home, Configuration, Statistics, Tools, Account, PDA, Copyright, Logoff, and user information: Account: admin, Level: ADMINISTRATOR. The main content area is titled 'Configuration => SNMP' and shows the device name '5.7GHz - Backhaul - Timing Slave - 0a-00-3e-fc-56-c9'. Below the title is a 'Save Changes' button. The configuration is organized into four sections:

- SNMP Community Strings:** Contains two entries. 'SNMP Community String 1' has the value 'Canopy' and permissions set to 'Read Only' (selected) and 'Read / Write'. 'SNMP Community String 2 (Read Only)' has the value 'Canopy'.
- SNMP Accessing Addresses:** A table with 10 rows, each for 'Accessing IP / Subnet Mask' from 1 to 10. Each row has two input fields, both containing '0.0.0.0' and '0' respectively.
- Trap Addresses:** A table with 10 rows, each for 'Trap Address' from 1 to 10. Each row has one input field containing '0.0.0.0'.
- Site Information:** Contains three fields: 'Site Name', 'Site Contact', and 'Site Location', all with the value 'No Site Name/Contact/Location'.

At the bottom of the configuration area, there are 'Save Changes' and 'Reboot' buttons.

Figure 111: SNMP tab of BHS, example

In the SNMP tab of the BHS, you may set the following parameters.

SNMP Community String 1

Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

SNMP Community String 1 Permissions

You can designate the **SNMP Community String 1** to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.

SNMP Community String 2 (Read Only)

Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is **Canopy2**. This password will never authenticate a user or an NMS to read/write access.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet, Trap Address**, and **Permission** parameters.

Accessing IP / Subnet Mask 1 to 10

Specify the addresses that are allowed to send SNMP requests to this BHS. Prizm or the NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the BHS, presuming that the device supplies the correct **Community String** value.

The default treatment is to allow all networks access (set to 0). For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.” You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.

Trap Address 1 to 10

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which trap information should be sent. Trap information informs Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when Prizm or an NMS attempts to access agent information but either
 - supplied an inappropriate community string or SNMP version number.
 - is associated with a subnet to which access is disallowed.

Read Permissions

Select **Read Only** if you wish to disallow Prizm or NMS SNMP access to configurable parameters and read-only fields of the SM.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by Prizm or an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.5 Quality of Service (QoS) Tab of the BHS

An example of the Quality of Service tab of the BHS is displayed in [Figure 112](#).

The screenshot shows the configuration interface for the Quality of Service (QoS) tab. The breadcrumb trail at the top indicates the path: General > IP > Radio > SNMP > Quality of Service (QoS) > Security > DiffServe > Unit Settings. The main heading is 'Configuration => Quality of Service (QoS)' with the device identifier '2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af'. The 'CIR Bandwidth Settings' section contains two rows: 'Low Priority Uplink CIR : 0 (kbps) (Range: 0 -- 20000 kbps)' and 'Low Priority Downlink CIR : 0 (kbps) (Range: 0 -- 20000 kbps)'. At the bottom of the configuration area are two buttons: 'Save Changes' and 'Reboot'.

Figure 112: Quality of Service (QoS) tab of BHS, example

In the Quality of Service (QoS) tab of the BHS, you may set the following parameters.

Low Priority Uplink CIR

See

- [Committed Information Rate on Page 88](#)
- [Setting the Configuration Source on Page 292.](#)

Low Priority Downlink CIR

See

- [Committed Information Rate on Page 88](#)
- [Setting the Configuration Source on Page 292.](#)

18.5.6 Security Tab of the BHS

An example of the Security tab in a BHS is displayed in [Figure 113](#).

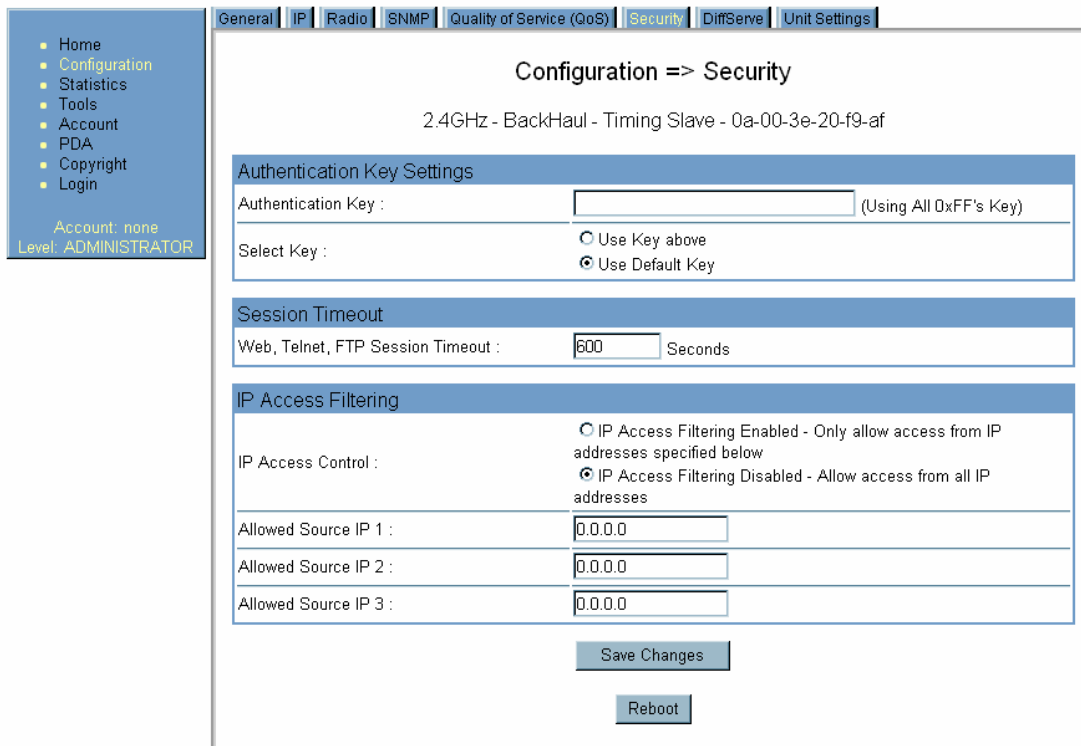


Figure 113: Security tab of BHS, example

In the Security tab of the BHS, you may set the following parameters.

Authentication Key

Only if the BHM to which this BHS will register requires authentication, specify the key that the BHS should use when authenticating. For alpha characters in this hex key, use only upper case.



NOTE:

Motorola recommends that you enter 32 characters to achieve the maximal security from this feature.

Select Key

The **Use Default Key** selection specifies that the link should continue to use the automatically generated authentication key. See [Authentication Manager Capability](#) on Page 391.

The **Use Key above** selection specifies the 32-digit hexadecimal key that is permanently stored on both the BHS and the BHM.

Web, Telnet, FTP Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the BHS.

IP Access Control

You can permit access to the BHS from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address, including access and management by Prizm.

Allowed Source IP 1 to 3

If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the BHS from any IP address. You may populate as many as all three.

If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

The Security tab of the BHS also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.7 VLAN Tab of the BHS

An example of the VLAN tab in a BHS is displayed in [Figure 114](#).

Configuration => VLAN

5.4GHz - Backhaul - Timing Slave - 0a-00-3e-51-bb-63 No valid accounts configured. Using default user account

Save Changes

VLAN Configuration

VLAN : Enabled
 Disabled

Management VID : (Range : 1 — 4094)

Active Configuration

Active Configuration Untagged Ingress VID : 1
Management VID : 10

Current VID Member Set:

VID Number	Type	Age
1	Permanent	0
10	Permanent	0

Save Changes

Reboot

Figure 114: VLAN tab of BHS, example

In the VLAN tab of the BHM, you may set the following parameters.

VLAN

Set the **VLAN** feature to **Enabled** or **Disabled**. When the feature is disabled, the text box for the following parameter is inactive. When the **Management VID** is enabled by this parameter, the module is manageable through only packets that are tagged with the VID configured in that parameter. These parameters have no bearing on tagging in non-management traffic.

By default, **VLAN** is **Enabled** in backhaul modules. With this feature enabled, the backhaul becomes a permanent member of any VLAN VID that it reads in packets that it receives. When the backhaul reboots, it loses these memberships, but begins again to freely adopt memberships in the VIDs that will be permanent until the next reboot.

Management VID

Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4094. The default value is 1. This text box is inactive if VLAN is set to **Disabled**. In the Motorola fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

The Active Configuration block provides the following details as read-only information in this tab.

Active Configuration Untagged Ingress VID

In a backhaul module, this value will always be 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

VID Number

In a backhaul module, this value will always be 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

Type

In a backhaul module, this value will always be Permanent, reflective of the fact that the backhaul is not capable of deleting any VID membership, regardless of whether it was learned or set.

Age

In a backhaul module, this value will always be 0, reflective of the fact that the backhaul is not capable of deleting any VID membership, regardless of whether it was learned or set.

The VLAN tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.8 DiffServe Tab of the BHS

An example of the DiffServe tab in a BHS is displayed in [Figure 115](#).

General | IP | Radio | SNMP | Quality of Service (QoS) | Security | **DiffServe** | Unit Settings

Configuration ==> DiffServe

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af

DiffServe Configuration							
CodePoints (00) -- (07):							
CP00 : 0	CP01 : 0	CP02 : 0	CP03 : 0	CP04 : 4	CP05 : 4	CP06 : 4	CP07 : 4
CodePoints (08) -- (15):							
CP08 : 0	CP09 : 0	CP10 : 0	CP11 : 0	CP12 : 4	CP13 : 4	CP14 : 4	CP15 : 4
CodePoints (16) -- (23):							
CP16 : 0	CP17 : 0	CP18 : 0	CP19 : 0	CP20 : 4	CP21 : 4	CP22 : 4	CP23 : 4
CodePoints (24) -- (31):							
CP24 : 0	CP25 : 0	CP26 : 0	CP27 : 0	CP28 : 4	CP29 : 4	CP30 : 4	CP31 : 4
CodePoints (32) -- (39):							
CP32 : 0	CP33 : 0	CP34 : 0	CP35 : 0	CP36 : 4	CP37 : 4	CP38 : 4	CP39 : 4
CodePoints (40) -- (47):							
CP40 : 0	CP41 : 0	CP42 : 0	CP43 : 0	CP44 : 4	CP45 : 4	CP46 : 4	CP47 : 4
CodePoints (48) -- (55):							
CP48 : 6	CP49 : 0	CP50 : 0	CP51 : 0	CP52 : 4	CP53 : 4	CP54 : 4	CP55 : 4
CodePoints (56) -- (63):							
CP56 : 7	CP57 : 0	CP58 : 0	CP59 : 0	CP60 : 4	CP61 : 4	CP62 : 4	CP63 : 4

CodePoint Select :

Priority Select :

Save Changes

Reboot

Figure 115: DiffServe tab of BHS, example

You may set the following Differentiated Services Configuration page parameters.

CodePoint 1 through CodePoint 47

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

The default priority value for each settable CodePoint is shown in [Figure 115](#). Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the BHM for the downlink and in the BHS for the uplink. See [DSCP Field](#) on Page 90.

18.5.9 Unit Settings Tab of the BHS

An example of the Unit Settings tab in a BHS is displayed in [Figure 116](#).

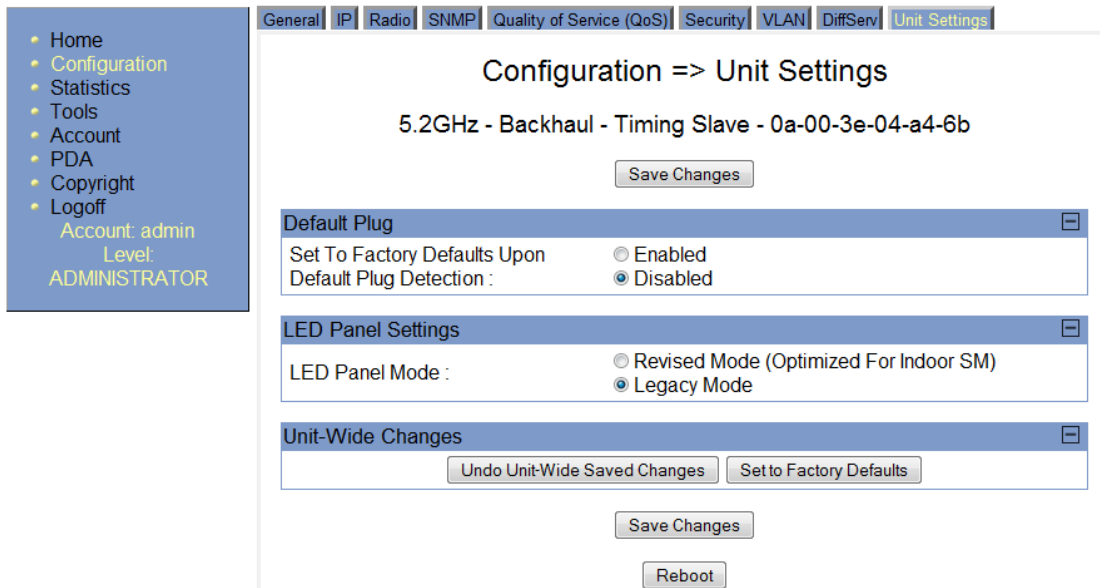


Figure 116: Unit Settings tab of BHS, example

The Unit Settings tab of the BHS contains an option for how the BHS should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults.

A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See [Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH](#) on Page 383.

The Unit Settings tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Undo Unit-Wide Saved Changes

When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

18.6 ADJUSTING TRANSMITTER OUTPUT POWER

Authorities may require transmitter output power to be adjustable and/or lower than the highest that a module produces. Adjustable power modules include a Radio tab parameter to reduce power on an infinite scale to achieve compliance. If you set this parameter to lower than the supported range extends, the value is automatically reset to the lowest supported value. The high end of the supported range does not vary from radio to radio.

Although transmitter output power is settable in the PMP Series 400 OFDM AP, this AP automatically sets the transmitter output power in its SMs through a feature named Auto-TPC. The conceptual reason for this feature is OFDM reception in the AP is more

sensitive to large differences in power levels received from its SMs than is its standard Canopy single-carrier AP counterpart. The OFDM AP sets the SM to the lesser of the following two levels:

- 10 dBm. This is the maximum allowed, because the SM operates with its integrated antenna, and regulation permits EIRP of not greater than 27 dBm.
- power level such that the power that the AP receives from the SM is not greater than 60 dBm.

See also [Procedure 3: Reducing transmitter output power](#) on Page 156.

The professional installer of the equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

The total gain per antenna in 900-MHz and 5.7-GHz radios is stated in [Table 57](#).

Table 57: Total gain per antenna

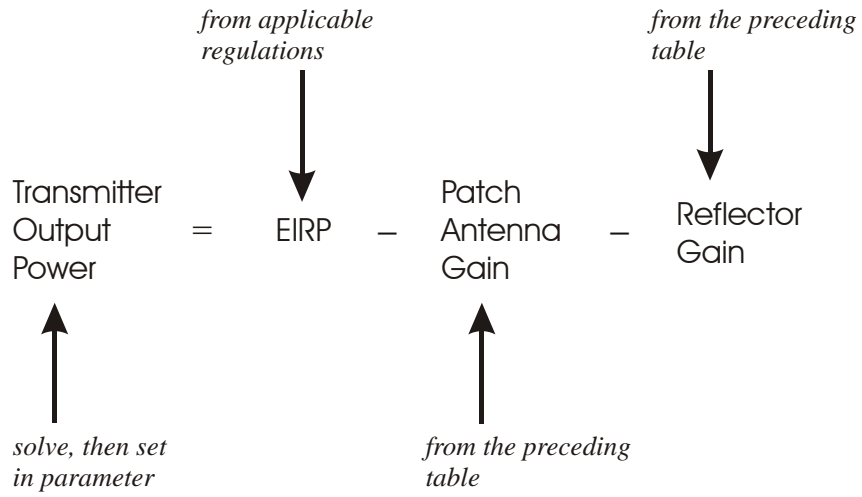
Module Type	Antenna Gain	Cable Loss ¹	Net Gain
900-MHz Integrated	12.5 dBi	0.2 dB	12 dBi
900-MHz Connectorized ²	10 to 10.5 dBi	0.3 dB	10 dBi
5.7-GHz Connectorized	settable	0.3 dB + from any additional cable	See Note 3
NOTES:			
1. Received signal measurements take this loss into account, but the transmitter output power setting cannot. Set the transmitter output power higher by this amount.			
2. With Mars, MTI, or Maxrad antenna.			
3. Antenna gain minus cable loss.			

Integrated patch antenna and reflector gains are provided in [Table 58](#).

Table 58: Patch antenna and reflector gain

Frequency Band Range	Gain	
	Patch Antenna	Reflector
2.4 GHz	8 dBi	11dBi
5.2, 5.4, or 5.7 GHz	7 dBi	18dBi

The calculation of transmitter output power is as follows:



Transmitter output power is settable as dBm on the Radio tab of the module. Example cases of transmitter output power settings are shown in [Table 59](#).

Table 59: Transmitter output power settings, example cases

Frequency Band Range and Antenna Scheme	Region	Maximum EIRP in Region	Transmitter Output Power Setting	
			AP, SM, or BH with No Reflector	SM or BH with Reflector
900-MHz Integrated	U.S.A. Canada	36 dBm (4 W)	24 dBm	
900-MHz Connectorized	U.S.A. Canada	36 dBm (4 W)	26 dBm ¹	
	Australia	30 dBm (1 W)	Depends on antenna	
2.4-GHz Integrated	U.S.A. Canada	Depends on antenna gain	25 dBm	25 dBm
	CEPT states	20 dBm (100 mW)	12 dBm	1 dBm
5.2-GHz Integrated	U.S.A. Canada	30 dBm (1 W)	23 dBm	
5.4-GHz FSK Integrated	CEPT states	30 dBm (1 W)	23 dBm	5 dBm
5.4-GHz OFDM Integrated	U.S.A. Canada Europe	27 dBm (600 mW)	-30 to 10 dBm ²	
5.4-GHz OFDM Connectorized	U.S.A. Canada Europe	27 dBm (600 mW)	-30 to 15 dBm ²	
5.7-GHz Connectorized	UK	33 dBm (2 W)	Depends on antenna	Depends on antenna

NOTES:

1. With Mars, MTI, or Maxrad antenna. This is the default setting, and 28 dBm is the highest settable value. The lower default correlates to 36 dBm EIRP where 10-dBi antennas are used. The default setting for this parameter is applied whenever **Set to Factory Defaults** is selected.
2. In a typical case, set the **Transmitter Output Power** parameter in the AP to the maximum allowed. This provides the greatest range for both overall operation and 3X operation. Where full power is not necessary, or where the OFDM network is likely to interfere with a nearby network, incrementally reduce the setting and monitor RF performance.

19 INSTALLING COMPONENTS



RECOMMENDATION:

Use *shielded* cable for all infrastructure connections associated with BHs, APs, and CMMs. The environment that these modules operate in often has significant unknown or varying RF energy. Operator experience consistently indicates that the additional cost of shielded cables is more than compensated by predictable operation and reduced costs for troubleshooting and support.

19.1 PDA ACCESS TO MODULES

For RF spectrum analysis or module aiming on a roof or tower, a personal digital assistant (PDA) is easier to carry than, and as convenient to use as, a notebook computer. The PDA is convenient to use because no scrolling is required to view

- spectrum analysis results.
- RSSI and jitter.
- master module evaluation data.
- information that identifies the module, software, and firmware.

To access this data in a format that fits a 320 x 240 pixel PDA screen, the PDA must have all of the following:

- a Compact Flash card slot.
- any of several Compact Flash wired Ethernet cards.
- a wired Ethernet connection to the module.
- a browser directed to `http://ModuleIPAddress/pda.html`.

The initial PDA tab reports link status, as shown in [Figure 117](#).

The screenshot shows a web interface with a navigation menu on the left and a main content area. The navigation menu includes: Home, Configuration, Statistics, Tools, Account, PDA (highlighted), Copyright, Logoff, Account: admin, Level: ADMINISTRATOR. The main content area has tabs for Quick Status, Spectrum Analyzer, and Spectrum Results (PDA). Under the Quick Status tab, there are sub-tabs for Information, BHM Evaluation, and AIM. The main content displays 'PDA => Quick Status' for '5.4GHz - BackHaul - Timing Slave - 0a-00-3e-50-1a-a7'. Below this is a table titled 'Link Status' with the following data:

Link Status	
RSSI :	1968
Jitter :	7
Power Level :	-34 dBm
Distance :	0.02 miles (98 feet)
Link :	No Link
AP :	0a-00-3e-51-60-23

Figure 117: PDA Quick Status tab, example

An example of the Spectrum Analyzer tab for PDAs is displayed in [Figure 118](#). For additional information about the Spectrum Analyzer feature, see [Monitoring the RF Environment](#) on Page 373.

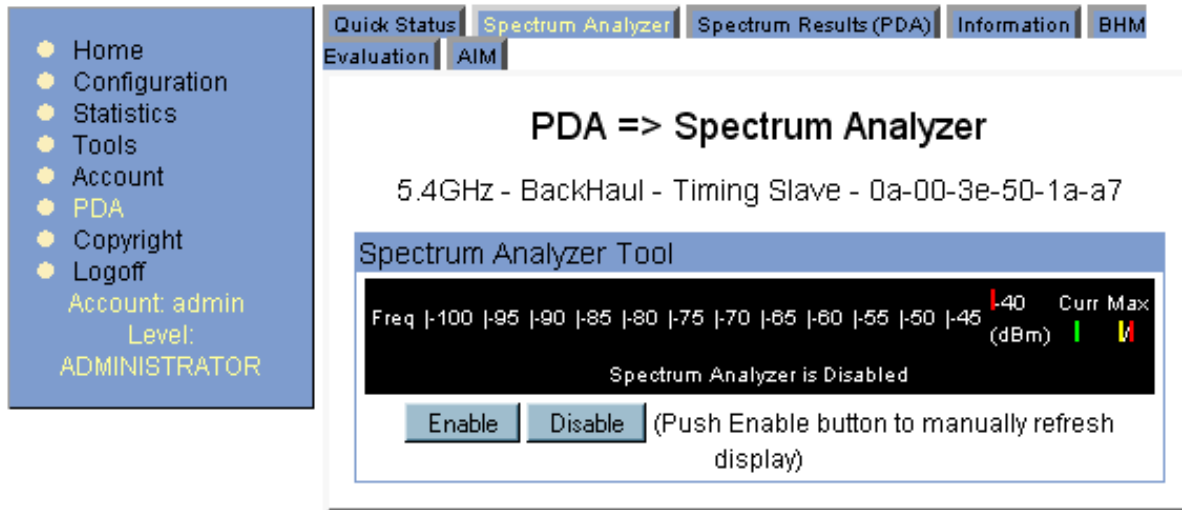


Figure 118: PDA Spectrum Analyzer tab of BHS, example

Examples of the Spectrum Results and Information tabs for PDAs are shown in [Figure 119](#) and [Figure 120](#).

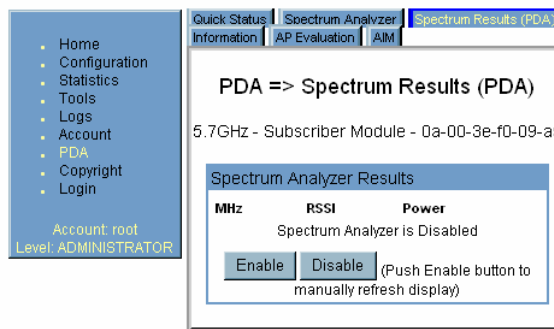


Figure 119: PDA Spectrum Results tab of SM, example

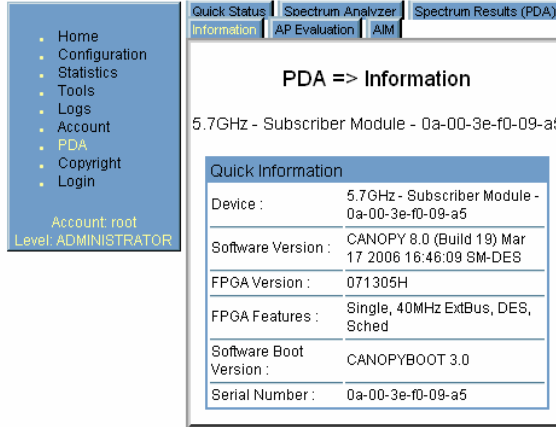


Figure 120: PDA Information tab of SM, example

Examples of the BHM Evaluation and Aim tabs for PDAs are shown in Figure 121 and Figure 122.

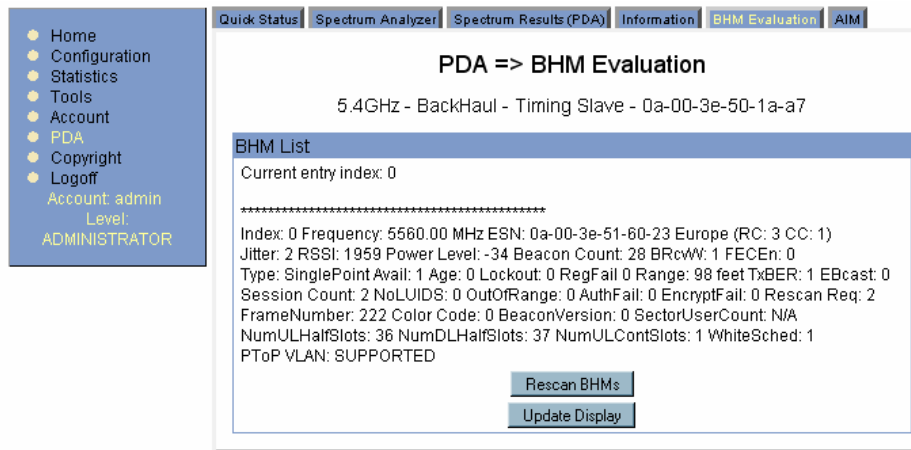


Figure 121: PDA AP Evaluation tab of BHM, example

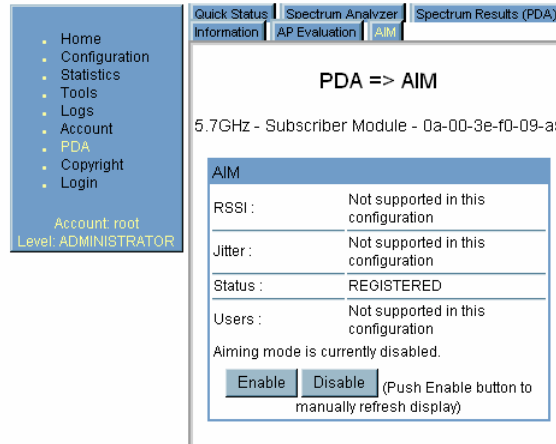


Figure 122: PDA Aim tab of SM, example

19.2 INSTALLING AN AP

19.2.1 Installing a PMP 100 Series AP

To install a PMP 100 Series (FSK) AP, perform the following steps.

Procedure 17: Installing the FSK AP

1. Begin with the AP in the powered-down state.
2. Choose the best mounting location for your particular application. Modules need not be mounted next to each other. They can be distributed throughout a given site. However, the 60° offset must be maintained. Mounting can be done with stainless steel hose clamps or another equivalent fastener.
3. Align the AP as follows:
 - a. Move the module to where the link will be unobstructed by the radio horizon and no objects penetrate the Fresnel zone. (The Canopy System Calculator page [AntennaElevationCalcPage.xls](#) automatically calculates the minimum antenna elevation that is required to extend the radio horizon to the other end of the link. The Canopy System Calculator page [FresnelZoneCalcPage.xls](#) automatically calculates the Fresnel zone clearance that is required between the visual line of sight and the top of a high-elevation object.)
 - b. Use a local map, compass, and/or GPS device as needed to determine the direction that one or more APs require to each cover the intended 60° sector.
 - c. Apply the appropriate degree of downward tilt. (The Canopy System Calculator page [DowntiltCalcPage.xls](#) automatically calculates the angle of antenna downward tilt that is required.)
 - d. Ensure that the nearest and furthest SMs that must register to this AP are within the beam coverage area. (The Canopy System Calculator page [BeamwidthRadiiCalcPage.xls](#) automatically calculates the radii of the beam coverage area for PMP 100 Series APs.)
4. Using stainless steel hose clamps or equivalent fasteners, lock the AP in the proper direction and downward tilt.
5. Remove the base cover of the AP. (See [Figure 51](#) on Page 182.)
6. Attach the cables to the AP. (See [Procedure 5](#) on Page 186.)

NOTE: When power is applied to a module or the unit is reset on the web-based interface, the module requires approximately 25 seconds to boot. During this interval, self-tests and other diagnostics are being performed. See [Table 45](#) on Page 183.

===== end of procedure =====

19.2.2 Installing a PMP 400 Series AP

To install a PMP 400 Series (OFDM) AP, perform the following steps.

Procedure 18: Installing the OFDM AP

1. Inventory the parts to ensure that you have them all before you begin.
NOTE: The full set of parts is shown in [Figure 123](#).

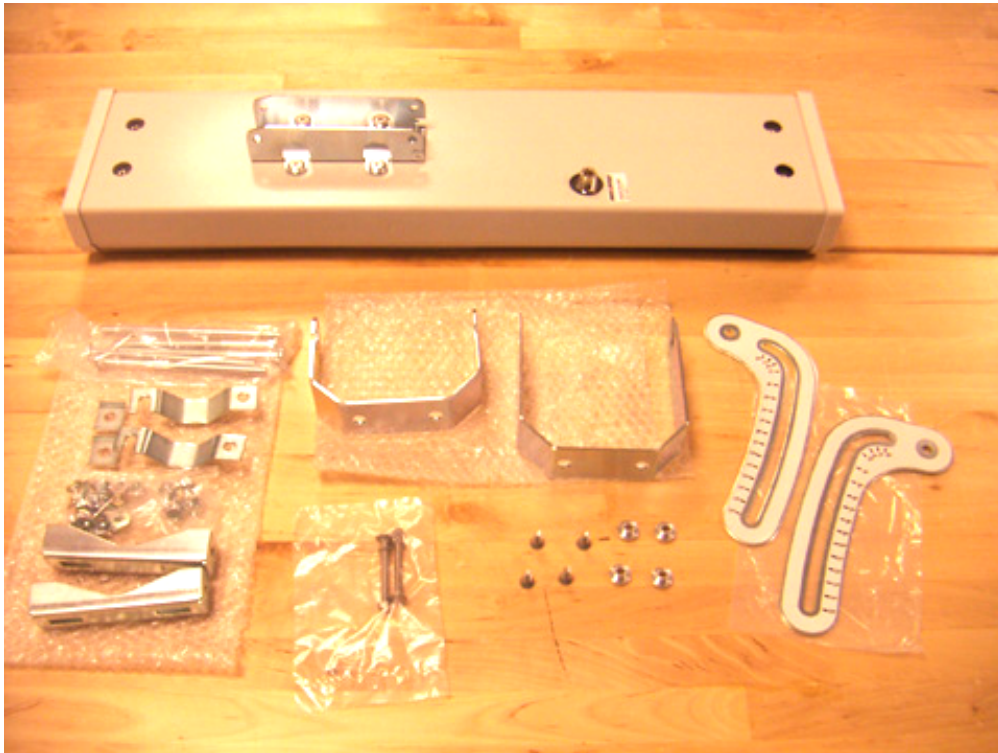


Figure 123: Parts inventory for OFDM AP installation

2. Assemble the upper bracket as shown in [Figure 124](#).



Figure 124: Assembled upper bracket for OFDM AP

3. Connect the AP to its antenna as shown in [Figure 125](#).

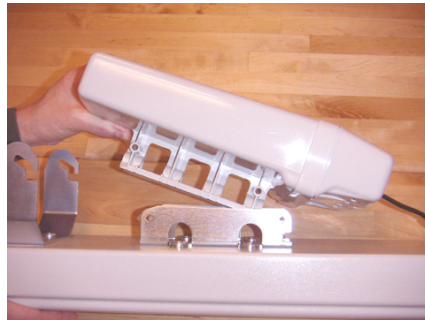


Figure 125: OFDM AP connected to its antenna

4. Attach the AP to its antenna as shown in [Figure 126](#).



Figure 126: OFDM AP mounted to its antenna

5. Attach the lower bracket to the antenna as shown in [Figure 126](#) above.
6. Use a local map, compass, and/or GPS device as needed to determine the direction that one or more APs require to each cover the 90° sector.

7. Ensure that the nearest and furthest SMs that must register to this AP are within the 3-dB beam pattern of 60° azimuth by 5° elevation with near-in null fill coverage.
8. Choose the best mounting location for your particular application.
NOTE: Use the embedded spectrum analyzer or a commercial analyzer to evaluate the frequencies present in various locations. OFDM APs need not be mounted next to each other. They can be distributed throughout a given site. However, the 90° offset must be maintained. If you want to collocate these APs with PMP 100 Series APs of the 5.4-GHz frequency band range, plan to allow at least 25 MHz of separation between their center channels.
9. Attach the upper bracket to the pole or tower as shown in [Figure 127](#).



Figure 127: OFDM AP ready for tower mount

10. Hang the AP/antenna assembly onto the upper bracket as shown in [Figure 128](#).



Figure 128: Hanging OFDM AP assembly onto upper bracket of pole mount

11. Attach the lower bracket to the pole or tower as shown in [Figure 129](#) and [Figure 130](#).

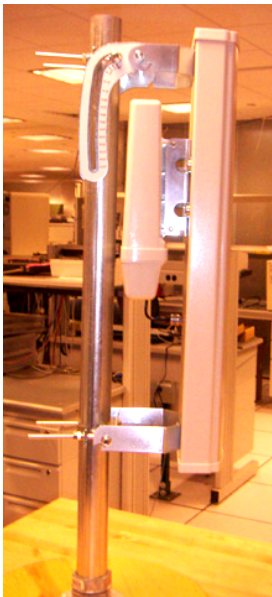


Figure 129: OFDM AP attached to pole or tower

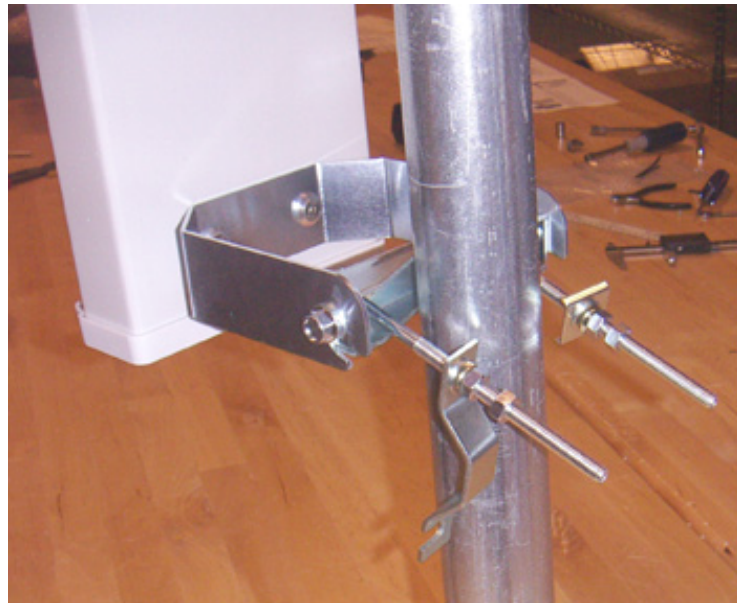


Figure 130: OFDM antenna lower bracket with quick-connect

12. Remove the cover of the 600SS Surge Suppressor.
13. With the cable openings facing downward, mount the 600SS as close as possible to the point where the Ethernet cable will penetrate the residence or building.

14. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.
15. Connect an Ethernet cable from the power adapter to either RJ-45 port of the 600SS.
16. Remove the bottom cover of the AP.
17. Secure a ground strap to the ground lug (circled in [Figure 131](#)) on the bottom of the AP.
18. Secure the ground strap to the pole, tower, or other trusted ground.

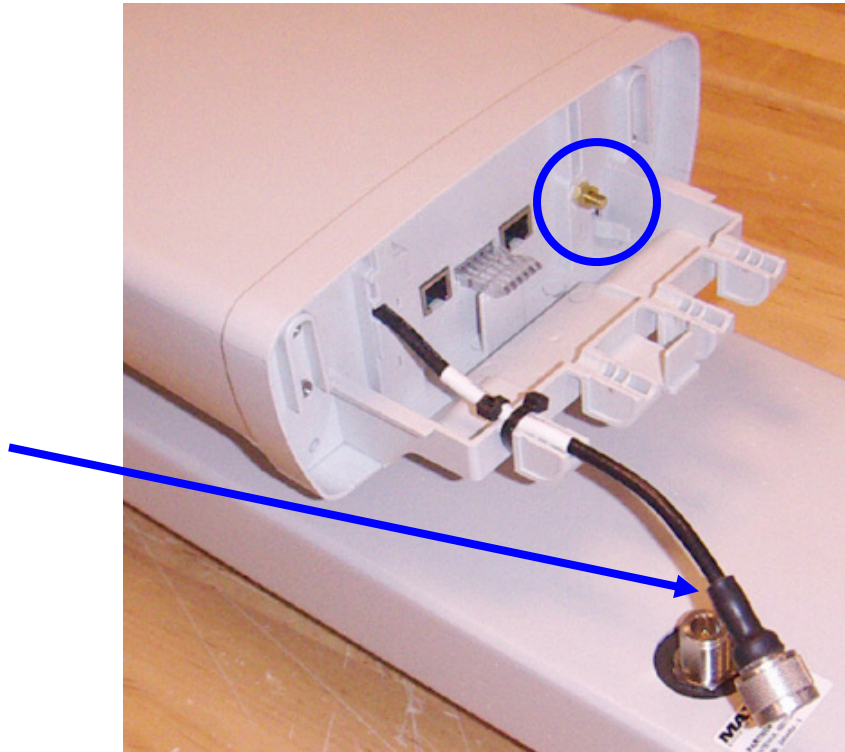


Figure 131: Ground lug and coax cable of OFDM AP

19. Connect the Ethernet cable from the AP to the other RJ-45 port of the 600SS.
 20. Wrap an AWG 10 (or 6mm²) copper wire around the Ground post of the 600SS.
 21. Tighten the Ground post locking nut in the 600SS onto the copper wire.
 22. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
 23. Replace the cover of the 600SS surge suppressor.
 24. Replace the bottom cover of the AP.
 25. Adjust the initial down tilt of the AP/antenna assembly to 5°, -3 dB beam elevation, with near-in null fill.
- NOTE:* The down tilt bracket is shown in [Figure 132](#).



Figure 132: Down tilt adjustment bracket of OFDM AP


26. Connect the coax cable to the antenna.
27. Weather-seal the connector on the coax cable (identified by arrow in [Figure 131](#) above).

===== end of procedure =====

19.3 INSTALLING A CONNECTORIZED FLAT PANEL ANTENNA

To install a connectorized flat panel antenna to a mast or structure, follow instructions that the manufacturer provides. Install the antenna safely and securely, consistent with industry practices.

The Universal Mounting Bracket available from Motorola (Part Number SMMB-1 and consisting of a mounting bracket and L-shaped aluminum tube) holds one module, but cannot hold both the module and a connectorized antenna. The SMMB-2 is a heavy duty bracket that can hold both a 900-MHz or 5.7-GHz connectorized module and its connectorized antenna. See [Module Support Brackets](#) on Page 63.



IMPORTANT!

Connectorized antennas *require* professional installation.

The professional installer is responsible for

- selection of an antenna that the regulatory agency has approved for use with the CAP 9130 AP and CAP 9130 SM.
- setting of the gain consistent with regulatory limitations and antenna specifications.
- ensuring that the polarity—horizontal or vertical—is identical on both ends of the link. (This may be less obvious where an integrated antenna is used on one end and a connectorized on the other.)
- use of moisture sealing tape or wrap to provide long-term integrity for the connection.

Although a vertically polarized signal propagates better than a horizontally polarized signal (because of the magnetic field of the earth), vertical polarization is typically better for long distance only where noise above the thermal noise floor is negligible. In some applications, cross polarization may improve signal separation, but typically to only 9 dB of separation at 900 MHz and 15 to 20 dB in the 5.7-GHz frequency band ranges.

19.4 INSTALLING A GPS ANTENNA

For instructions on GPS antenna installation, see the user guide that is dedicated to the CMM product.

19.5 INSTALLING A CLUSTER MANAGEMENT MODULE

For instructions on CMM2 (Cluster Management Module 2), CMM3 (CMMmicro), or CMM4 installation, including the outdoor temperature range in which it is acceptable to install the unit, tools required, mounting and cabling instructions, and connectivity verification, see the user guide that is dedicated to that particular product.

19.6 INSTALLING AN SM

19.6.1 Configuring the Laptop for Connection to SMs

Windows Laptop

To configure a Windows laptop for connection to SMs for installation, perform the following steps.

Procedure 19: Configuring a Windows laptop

1. Select **Start→Control Panel**.
2. Select **Network and Internet Connections** (or the similarly labeled category).
3. Select
 - **Network Connections**, if your platform is XP.
 - **Manage Network Connections**, if your platform is Vista.
4. Right click on a LAN whose status is shown as Connected and select **Properties** from the drop-down list.
5. Click to highlight **Internet Protocol (TCP/IP)**.
NOTE An example is shown in [Figure 133](#).

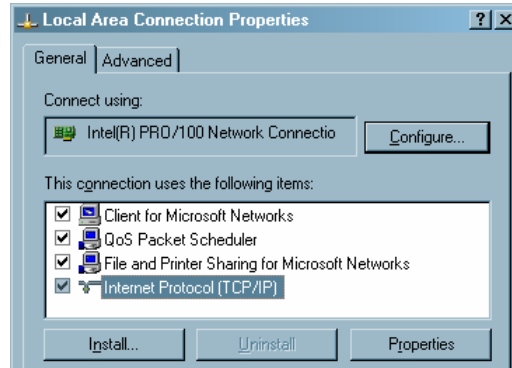


Figure 133: Example Local Area Connection Properties window

6. Click the **Properties** button.
7. In the General tab, select **Use the following IP address**.
NOTE: An example is shown in [Figure 134](#).

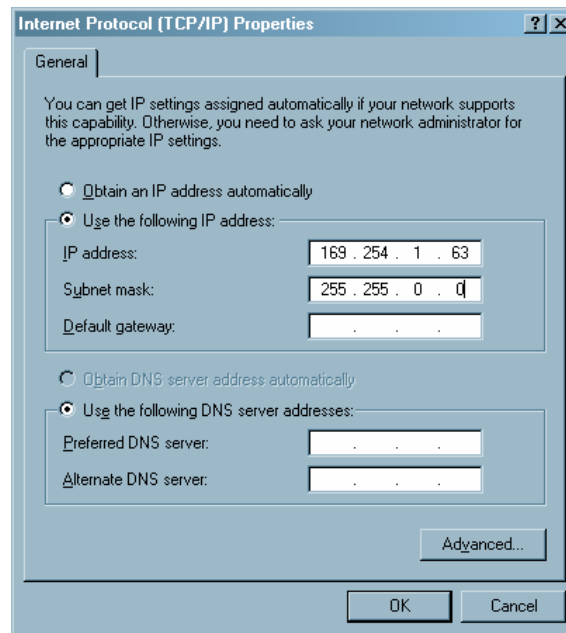


Figure 134: Example Internet Protocol (TCP/IP) Properties window

8. For IP address, type in 169.254.1.63.
9. For Subnet mask, type in 255.255.0.0.
10. In the Internet Protocol (TCP/IP) Properties window, click the **OK** button.
11. Click the **Close** button to dismiss the Local Area Connections window.
12. Close the Network Connections window.

RESULT: The laptop is now configured to reach the interfaces of SMs whose IP addresses are default from the factory. However, the current setting inhibits normal access to the Internet.

13. Whenever you want to access the Internet, reset the General tab to **Obtain an IP address automatically**, but leave the special configuration for the 169 net intact.
14. Whenever you want to use the laptop for SM installations, reset the General tab to **Use the following IP address** and the 169 net.

===== end of procedure =====

Linux Laptop

To configure a Linux laptop for connection to SMs for installation, perform the following steps.

Procedure 20: Configuring a Linux laptop

1. On your Linux console, log in as `root`.
2. Enter `ip addr show`.
3. Write down the string that is in the final position of the system response (for example, `eth0`) to use as the *NIC* in the next step.
4. Enter `ip addr add 169.254.1.63/16 dev NIC`.
RESULT: The laptop is now configured to reach the interfaces of SMs whose IP addresses are default from the factory. However, the current setting inhibits normal access to the Internet.
5. Enter `ip addr show`.
RESULT: The system response confirms the configuration.
6. Whenever you want to access the Internet, perform the following steps:
 - a. Log in as `root`.
 - b. Enter `netconfig`.
 - c. When prompted on whether to set up networking, select **Yes**.
 - d. Tab to highlight the **Use Dynamic IP Configuration** option.
 - e. Press the spacebar.
RESULT: The laptop will automatically obtain an IP address and will be able to access the Internet.
7. Whenever you want to use the laptop for SM installations, perform Steps 1 through 5 of this procedure.

===== end of procedure =====

19.6.2 Installing a PMP 100 Series SM

Installing a PMP 100 Series SM consists of two procedures:

- Physically installing the SM on a residence or other location and performing a course alignment using the alignment tone ([Procedure 21](#)).
- Verifying the AP to SM link and finalizing alignment using review of power level and jitter, link tests, and review of registration and session counts ([Procedure 23](#) on Page [355](#)).

Procedure 21: Installing the FSK SM

1. Choose the best mounting location for the SM.
2. Select the type of mounting hardware appropriate for this location.
NOTE: For mounting 2.4, 5.2, 5.4, and 5.7 GHz SMs, Motorola offers the SMMB-1 mounting bracket. For mounting 900 MHz SMs, Motorola offers the SMMB-2 mounting bracket.
3. Attach the mounting bracket to the structure.
4. Remove the base cover of the SM. (See [Figure 51](#) on Page 182.)
5. Terminate the UV outside grade Category 5 Ethernet cable with an RJ-45 connector, and connect the cable to the SM. (See [Procedure 8](#) on Page 195.)
6. Wrap a drip loop in the cable.
7. Optionally, attach the SM to the arm of the Passive Reflector dish assembly as shown in [Figure 135](#) or snap a LENS onto the SM.

**RECOMMENDATION:**

A reflector in this instance reduces the beamwidth to reduce interference. The arm is molded to receive and properly aim the module relative to the aim of the dish. Use stainless steel hose clamps for the attachment.

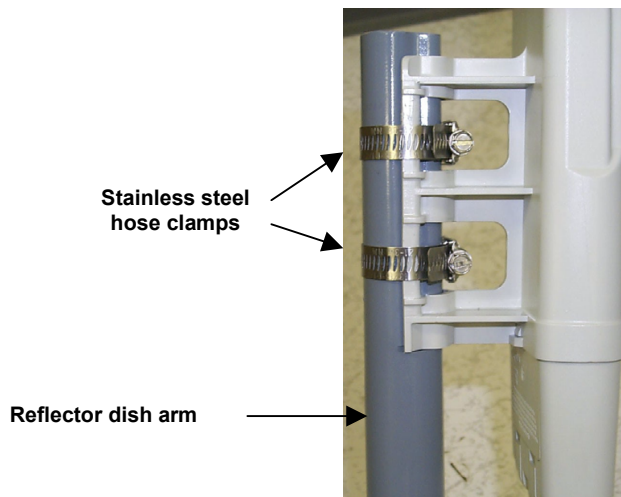


Figure 135: SM attachment to reflector arm

8. Use stainless steel hose clamps or equivalent fasteners to lock the SM into position.
NOTE: The SM grounding method is shown in [Figure 136](#).

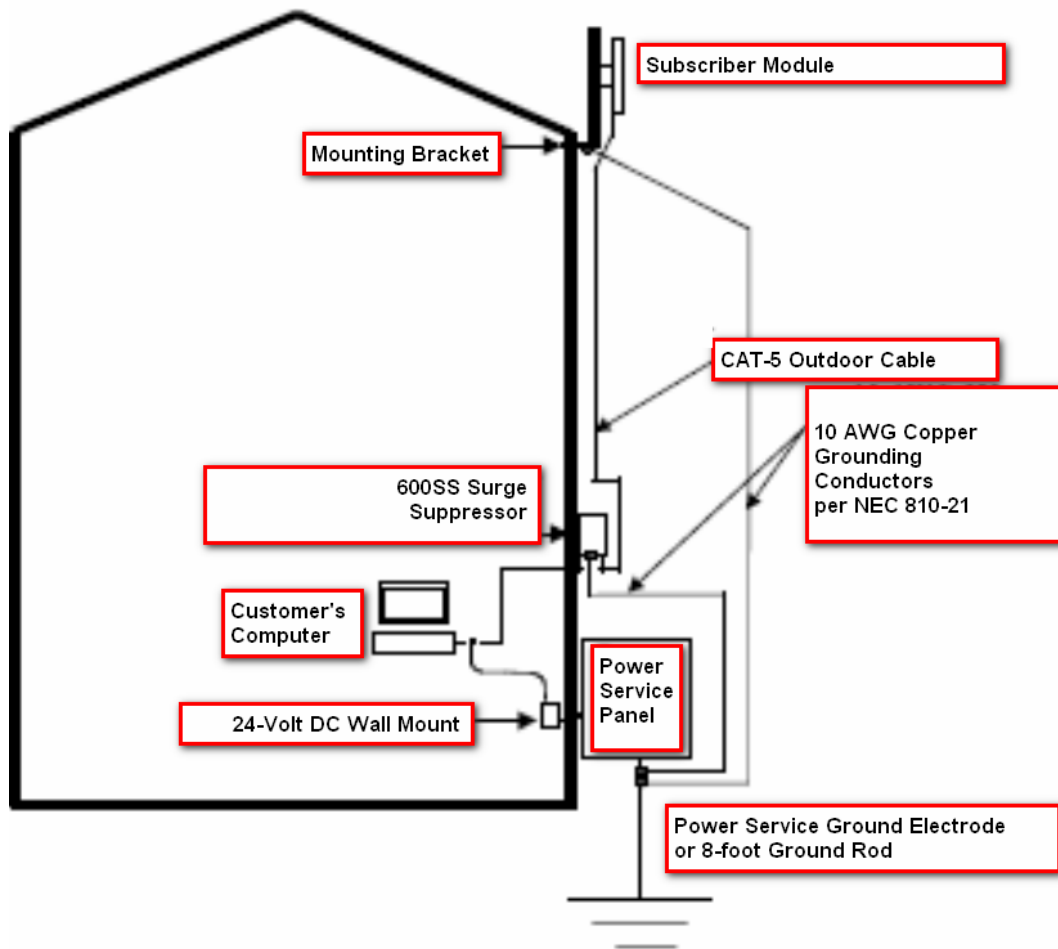
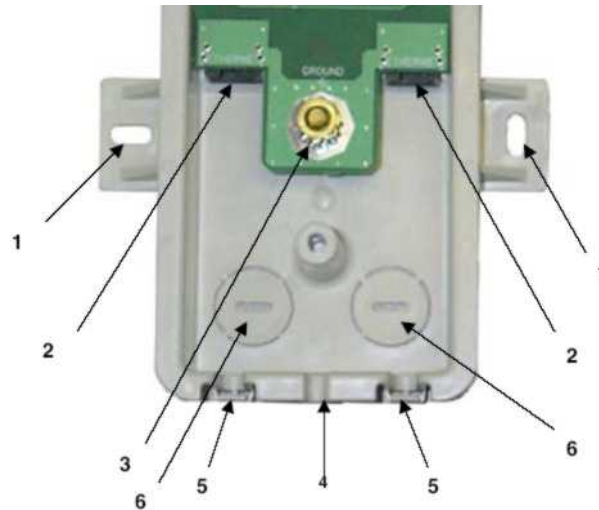


Figure 136: SM grounding per NEC specifications

9. Refer to [Grounding SMs](#) on Page 176.
10. Remove the cover of the 600SS Surge Suppressor.
NOTE: The inside of the surge suppressor is shown in [Figure 137](#).



KEY TO CALLOUTS

- 1 Holes—for mounting the Surge Suppressor to a flat surface (such as an outside wall). The distance between centers is 4.25 inches (108 mm).
- 2 RJ-45 connectors—One side (neither side is better than the other for this purpose) connects to the product (AP, SM, BHM, BHS, or cluster management module). The other connects to the AC adaptor's Ethernet connector.
- 3 Ground post—use heavy gauge (10 AWG or 6 mm²) copper wire for connection. Refer to local electrical codes for exact specifications.
- 4 Ground Cable Opening—route the 10 AWG (6 mm²) ground cable through this opening.
- 5 CAT-5 Cable Knockouts—route the two CAT-5 cables through these openings, or alternatively through the Conduit Knockouts.
- 6 Conduit Knockouts—on the back of the case, near the bottom. Available for installations where cable is routed through building conduit.

Figure 137: Internal view of Canopy 600SS Surge Suppressor

11. With the cable openings facing downward, mount the 600SS to the *outside* of the subscriber premises, as close to the point where the Ethernet cable penetrates the residence or building as possible, and as close to the grounding system (Protective Earth) as possible.
12. Wrap an AWG 10 (or 6mm²) copper wire around the Ground post of the 600SS.
13. Tighten the Ground post locking nut in the 600SS onto the copper wire.
14. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
15. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.
16. Pack both of the surge suppressor Ethernet jacks with dielectric grease.
17. Wrap a splice loop in the loose end of the Ethernet cable from the SM.
18. Connect that cable to one of the Ethernet jacks.

19. Connect an Ethernet cable to the other Ethernet jack of the 600SS and to the power adapter.
20. Replace the cover of the 600SS.
21. Connect the power supply to a power source.
22. Connect the Ethernet output from the power supply to the Ethernet port of your laptop.
23. Climb your ladder to the SM.
24. Launch your web browser.
25. In the URL address bar, enter 169.254.1.1.
26. If the browser in your laptop fails to access the interface of the SM, perform the following steps:
 - a. Insert your override plug into the RJ11 GPS utility port of the SM.
NOTE: An override plug is shown in [Figure 138](#).

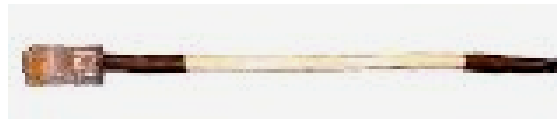


Figure 138: Override plug

- b. Remove and reinsert the RJ45 Ethernet cable connector at the SM.
NOTE: This triggers a power cycle, which causes the SM to reboot.
 - c. Wait for the reboot to conclude (about 30 seconds).
 - d. When the reboot is finished, remove the override plug.
 - e. In the left-side menu of the SM interface, click **Login**.
 - f. Consistent with local operator policy, reset both the `admin` and the `root` user passwords.
 - g. In the left-side menu, click **Configuration**.
 - h. Click the IP tab.
 - i. Consistent with local operator practices, set an
 - **IP Address**
 - **Subnet Mask**
 - **Gateway IP Address**
 - j. Click the **Save Changes** button.
 - k. Click the **Reboot** button.
27. As described under [Adding a User for Access to a Module](#) on Page 381, log in as either `admin` or `root` on the SM.
28. Configure a password for the `admin` account and a password for the `root` account.
29. Log off of the SM.
30. Log back into the SM as `admin` or `root`, using the password that you configured.

31. For coarse alignment of the SM, use the Audible Alignment Tone feature as follows:
 - a. In the left-side menu of the SM interface, click **Configuration**.
 - b. Click the General tab.
 - c. Set the **2X Rate** parameter in the SM to **Disabled**.
 - d. Connect the RJ-11 6-pin connector of the Alignment Tool Headset to the RJ-11 utility port of the SM.

Alternatively, instead of using the Alignment Tool Headset, use an earpiece or small battery-powered speaker connected to Pin 5 (alignment tone output) and Pin 6 (ground) of an RJ-11 connector.

- e. Listen to the alignment tone for
 - pitch, which indicates greater signal power (RSSI/dBm) by higher pitch.
 - volume, which indicates better signal quality (lower jitter) by higher volume.



Figure 139: Audible Alignment Tone kit, including headset and connecting cable

- f. Adjust the module slightly until you hear the highest pitch and highest volume.
 - g. In the General tab of the Configuration web page of the SM, set the **2X Rate** parameter back to **Enable**.
32. When you have achieved the best signal (highest pitch, loudest volume), lock the SM in place with the mounting hardware.
 33. Log off of the SM.
 34. Disconnect the Ethernet cable from your laptop.
 35. Replace the base cover of the SM.
 36. Connect the Ethernet cable to the computer that the subscriber will be using.

===== **end of procedure** =====

19.6.3 Installing a PMP 400 Series SM

Installing a PMP 400 Series SM consists of two procedures:

- Physically installing the SM on a residence or other location and performing a course alignment using the alignment tone.
- Verifying the AP to SM link and finalizing alignment using review of power level, link tests, and review of registration and session counts ([Procedure 23](#) on [Page 355](#)).

To install a PMP 400 Series (OFDM) SM, perform the following steps.

Procedure 22: Installing the OFDM SM

1. When gathering parts for the installation, select
 - a 29.5-V DC power supply and 328 feet (100 meters) or less of cable for the power supply.
 - an SMMB-2A mounting bracket
 - a 600SS surge suppressor
2. At the site, choose the best mounting location.
3. Mount the SMMB-2A bracket to the structure.
4. Remove the base cover of the SM.
5. Terminate the UV outside grade Category 5 Ethernet cable with an RJ-45 connector, and connect the cable to the SM.
6. Wrap a drip loop in the cable.
7. Use stainless steel hose clamps or equivalent fasteners to lock the SM into position.
8. Remove the cover of the 600SS Surge Suppressor.
9. Refer to [Grounding SMs](#) on [Page 176](#).
10. With the cable openings facing downward, mount the 600SS to the outside of the subscriber premises, as close as possible to the point where the Ethernet cable will penetrate the residence or building.
11. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.
12. Pack both of the surge suppressor Ethernet jacks with dielectric grease.
13. Connect an Ethernet cable from the power adapter to either RJ-45 port of the 600SS.
14. Remove the bottom cover of the SM.
15. Secure a ground strap to the ground lug (circled in [Figure 131](#) on [Page 343](#)) on the bottom of the SM.
16. Secure the ground strap to the power service panel of the structure.
17. Weather-seal the connector on the coax cable (identified by arrow in [Figure 131](#) on [Page 343](#)).
18. Wrap a splice loop in the loose end of the Ethernet cable from the SM.
19. Connect that cable to the other RJ-45 port of the 600SS.
20. Wrap an AWG 10 (or 6mm²) copper wire around the Ground post of the 600SS.
21. Tighten the Ground post locking nut in the 600SS onto the copper wire.

22. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
23. Replace the cover of the 600SS surge suppressor.
24. Connect the power supply to a power source.
25. Connect the Ethernet output from the power supply to the Ethernet port of your laptop.
26. Climb your ladder to the SM.
27. Launch your web browser.
28. In the URL address bar, enter 169.254.1.1.
29. As described under [Adding a User for Access to a Module](#) on Page 381, log in as either `admin` or `root` on the SM.
30. Configure a password for the `admin` account and a password for the `root` account.
31. Log off of the SM.
32. Log back into the SM as `admin` or `root`, using the password that you configured.
33. For coarse alignment of the SM, use the Audible Alignment Tone feature as follows:
 - a. In the left-side menu of the SM interface, click **Configuration**.
 - b. Click the General tab.
 - c. Set the operation rate parameter in the SM to **Disabled**.
 - d. Connect the RJ-11 6-pin connector of the Alignment Tool Headset to the RJ-11 utility port of the SM.

Alternatively, instead of using the Alignment Tool Headset, use an earpiece or small battery-powered speaker connected to Pin 5 (alignment tone output) and Pin 6 (ground) of an RJ-11 connector.
 - e. Listen to the alignment tone for pitch, which indicates greater signal power (RSSI/dBm) by higher pitch.

IMPORTANT: If you have experience in aligning FSK SMs, keep in mind that, unlike FSK SMs whose beam width is 60°, OFDM SMs have an 18 beam width. This alignment requires significantly greater precision.

Since the OFDM SM does not measure jitter, no difference in volume is heard in the headset as you move the SM.
 - f. Adjust the module slightly until you hear the highest pitch and highest volume.
 - g. In the General tab of the Configuration web page of the SM, set the operation rate parameter back to the desired operation speed (1X, 2X, or 3X).
34. When you have achieved the best signal (highest pitch, loudest volume), lock the SM in place with the mounting hardware.
35. Log off of the SM.
36. Disconnect the Ethernet cable from your laptop.
37. Replace the base cover of the SM.
38. Connect the Ethernet cable to the computer that the subscriber will be using.

===== end of procedure =====

19.7 CONFIGURING AN AP-SM LINK

To configure the AP-SM over-the-air link after the SM has been installed, perform the following steps.

Procedure 23: Configuring the AP-SM link

1. Using a computer (laptop, desktop, PDA) connected to the SM, open a browser and access the SM using the default IP address of <http://169.254.1.1> (or the IP address configured in the SM, if one has been configured.)
2. In the left-side menu, select **Configuration**.
3. Click the General tab.
4. Set the **2X Rate** parameter to **Disabled**.
5. In the left-side menu, select **Tools**.
6. Click the AP Evaluation tab.
7. Among the listed APs (each shown with a unique Index number), find the AP whose **Jitter** value is lowest and whose **Power Level** value is highest (or find the ESN of the AP to which you were instructed to establish a link).

IMPORTANT: The received **Power Level** is shown in dBm and should be maximized. **Jitter** should be minimized. However, better/lower jitter should be favored over better/higher dBm. For example, if coarse alignment gives an SM a power level of -75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to -78 dBm and the jitter to 2 or 3, the latter would be better, with the following caveats:

 - When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
 - When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

An example of the AP Evaluation tab is shown in [Figure 140](#).

```

Index: 0 Frequency: 5805.00 MHz ESN: 0a-00-3e-f0-f1-eb Brazil (RC: 4 CC: 2)
Jitter: 3 RSSI: 2439 Power Level: -19 Beacon Count: 38 BRcvW: 1 FECEn: 0
Type: Multipoint Avail: 1 Age: 0 Lockout: 0 RegFail 0 Range: 196 feet TxBER: 1 EBcast: 0
Session Count: 4 NoLUIDS: 0 OutOfRange: 0 AuthFail: 0 EncryptFail: 0 Rescan Req: 0
FrameNumber: 36 SectorID: 0 Color Code: 253 BeaconVersion: 1 SectorUserCount: 0
NumULHalfSlots: 19 NumDLHalfSlots: 57 NumULContSlots: 0
  
```

Figure 140: Example data from AP Evaluation tab

PMP 400 Series SMs do not have the **Jitter** parameter.



NOTE:

For historical reasons, **RSSI** is also shown and is the unitless measure of power. The best practice is to use **Power Level** and ignore **RSSI**, which implies more accuracy and precision than is inherent in the measurement.

8. Write down the **Frequency** and **Color Code** values of the AP in the link.

NOTE: See [Figure 140](#) on Page 355.

9. In the left-side menu of the SM interface, select **Configuration**.
10. Click the Radio tab.
11. At the **Custom Radio Frequency Scan Selection List** parameter, uncheck all frequencies except the one on which the AP in the link is broadcasting.
12. At the **Color Code** parameter, enter the code number that was shown for that AP in the AP Evaluation tab.
13. Click the **Save Changes** button.
14. Click the **Reboot** button.
15. Fine-adjust the SM mounting, if needed, to improve **Jitter** (if reported) or **Power Level** according to your company standards.

NOTE: For example, while maintaining or improving on the **Jitter** that you saw in the AP Evaluation data, and achieving ≥ 3 dB of **Power Level** separation from any other AP, fine-tune the SM mounting position for the highest **Power Level** achievable.
16. Retighten the hardware that secures the mounting.
17. In the left-side menu, select **Tools**.
18. Click the Link Capacity Test tab.

NOTE: Use of this tool is described under [Using the Link Capacity Test Tool \(All\)](#) on Page 438.

 - a. Perform several link tests of 10-second duration as follows:
 - b. Type into the **Duration** field how long (in seconds) the RF link should be tested.
 - c. Leave the **Packet Length** field (when present) set to the default of 1522 bytes or type into that field the packet length at which you want the test conducted.
 - d. Leave the **Number of Packets** field set to 0 (to flood the link).
 - e. Click the **Start Test** button.
 - f. View the results of the test.
19. If these link tests fail to consistently show 90% or greater efficiency in 1X operation or 50 to 60% efficiency in 2X, troubleshoot the link, using the data as follows:
 - If the downlink is consistently 90% efficient, but the uplink is only 40%, this indicates trouble for the SM transmitting to the AP. Have link tests performed for nearby SMs. If their results are similar, investigate a possible source of interference local at the AP.
 - If the uplink is consistently 90% efficient, but the downlink is only 40%, this indicates trouble for the AP transmitting to the SM. Investigate a possible source of interference near the SM.

If these link tests consistently show 90% or greater efficiency in 1X operation, or 50 to 60% efficiency in 2X operation, in both uplink and downlink, continue this procedure.
20. In the left-side menu, select **Configuration**.
21. In the General tab, set the **2X Rate** parameter to **Enabled**.
22. Click the **Save Changes** button.

23. If Prizm or another element management system will be used to manage the SM via SNMP, perform the following steps:
 - a. Click the SNMP tab.
 - b. At the **Read Permissions** parameter, select **Read/Write**.
 - c. Under **Site Information**, type complete data into the three parameters: **Site Name**, **Site Contact**, **Site Location**.
 - d. Click the **Save Changes** button.
24. Click the **Reboot** button.

NOTE: At 2X operation, received **Jitter** can be as great as 9 in a high-quality downlink, but should be as low as your further aiming efforts can yield. If you need to re-aim, set the SM back to 1X operation first.

===== end of procedure =====

19.8 MONITORING AN AP-SM LINK

After the SM installer has configured the link, either an operator in the network office or the SM installer in the field (if read access to the AP is available to the installer) should perform the following procedure. Who is authorized and able to do this may depend on local operator password policy, management VLAN setup, and operational practices.

Procedure 24: Monitoring the AP-SM link for performance

1. Access the interface of the AP.
2. In the left-side menu of the AP interface, select **Home**.
3. Click the Session Status tab.

NOTE: An example of this tab is shown in [Figure 141](#).

General Status
Session Status
Remote Subscribers
Event Log
Network Interface

- Home
- Configuration
- Statistics
- Tools
- Account
- Quick Start
- Copyright
- Logoff

Account: root
Level: ADMINISTRATOR

Home => Session Status

2.4GHz - Access Point - 0a-00-3e-20-a5-36

Session Status List

LUID: 002 : MAC: 0a-00-3e-20-00-32 State: IN SESSION (Encrypt Active)

Site Name : SM 10.40.14.121
 Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
 Software Boot Version : CANOPYBOOT 3.0
 FPGA Version : 071305 (DES Sched) P8
 Session Timeout: 0, AirDelay 6 (approximately 0.06 miles (294 feet))
 Session Count: 1, Reg Count 1, Re-Reg Count 0
 RSSI (Avg/Last): 2059/2062 Jitter (Avg/Last): 2/2 Power Level (Avg/Last): -37/-37
 Sustained Uplink Data Rate (APCAP): 3500 (kbit)
 Uplink Burst Allocation (APCAP): 500000 (kbit)
 Sustained Downlink Data Rate (APCAP): 3500 (kbit)
 Downlink Burst Allocation (APCAP): 500000 (kbit)
 Low Priority Uplink CIR (D): 0 (kbps) Low Priority Downlink CIR (D): 0 (kbps)
 Rate : VC 18 Rate 1X/1X

LUID: 003 : MAC: 0a-00-3e-20-a6-6f(Lite SM) State: IN SESSION (Encrypt Active)

Site Name : SM 10.40.14.147
 Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
 Software Boot Version : CANOPYBOOT 3.0
 FPGA Version : 022706 (DES Sched) P9
 Session Timeout: 0, AirDelay 3 (approximately 0.03 miles (147 feet))
 Session Count: 1, Reg Count 1, Re-Reg Count 0
 RSSI (Avg/Last): 2056/2059 Jitter (Avg/Last): 4/2 Power Level (Avg/Last): -37/-37
 Sustained Uplink Data Rate (DLCAP): 256 (kbit)
 Uplink Burst Allocation (DLCAP): 768 (kbit)
 Sustained Downlink Data Rate (DLCAP): 256 (kbit)
 Downlink Burst Allocation (DLCAP): 768 (kbit)
 Low Priority Uplink CIR (DL): 0 (kbps) Low Priority Downlink CIR (DL): 0 (kbps)
 Rate : VC 19 Rate 2X/2X

LUID: 004 : MAC: 0a-00-3e-20-a5-48 State: IN SESSION (Encrypt Active)

Site Name : Camera Client
 Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
 Software Boot Version : CANOPYBOOT 3.0
 FPGA Version : 022706 (DES Sched) P9
 Session Timeout: 0, AirDelay 4 (approximately 0.04 miles (196 feet))
 Session Count: 1, Reg Count 1, Re-Reg Count 0
 RSSI (Avg/Last): 2059/2066 Jitter (Avg/Last): 5/7 Power Level (Avg/Last): -37/-37
 Sustained Uplink Data Rate (APCAP): 20000 (kbit)
 Uplink Burst Allocation (APCAP): 500000 (kbit)
 Sustained Downlink Data Rate (APCAP): 20000 (kbit)
 Downlink Burst Allocation (APCAP): 500000 (kbit)
 Low Priority Uplink CIR (D): 0 (kbps) Low Priority Downlink CIR (D): 0 (kbps)
 Rate : VC 20 Rate 2X/2X

LUID: 005 : MAC: 0a-00-3e-20-00-2a State: IN SESSION (Encrypt Active)

Site Name : SM 10.40.14.103
 Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
 Software Boot Version : CANOPYBOOT 3.0
 FPGA Version : 071305 (DES Sched) P8
 Session Timeout: 0, AirDelay 5 (approximately 0.05 miles (245 feet))
 Session Count: 2, Reg Count 1, Re-Reg Count 1
 RSSI (Avg/Last): 2059/2068 Jitter (Avg/Last): 2/2 Power Level (Avg/Last): -37/-37
 Sustained Uplink Data Rate (APCAP): 3500 (kbit)
 Uplink Burst Allocation (APCAP): 500000 (kbit)
 Sustained Downlink Data Rate (APCAP): 3500 (kbit)
 Downlink Burst Allocation (APCAP): 500000 (kbit)
 Low Priority Uplink CIR (D): 0 (kbps) Low Priority Downlink CIR (D): 0 (kbps)
 Rate : VC 21 Rate 1X/1X

Figure 141: AP/SM link status indications in the AP Session Status tab

4. Find the **Session Count** line under the MAC address of the SM.
5. Check and note the values for **Session Count, Reg Count, and Re-Reg Count**.
6. Briefly monitor these values, occasionally refreshing this page by clicking another tab and then the Session Status tab again.

7. If these values are low (for example, 1, 1, and 0, respectively, meaning that the SM registered and started a stable session once) and are not changing
 - a. consider the installation successful.
 - b. monitor these values from the network office over the next several hours and days.

If these values are greater than 1, 1, and 0, or they increase while you are monitoring them, troubleshoot the link. (For example, recheck jitter as described in [Procedure 21: Installing the FSK SM](#) or recheck link efficiency as described in this procedure, then look for sources of RF interference or obstructions.)

===== end of procedure =====

19.9 INSTALLING A REFLECTOR DISH

The internal patch antenna of the module illuminates the Passive Reflector Dish from an offset position. The module support tube provides the proper angle for this offset.

19.9.1 Both Modules Mounted at Same Elevation

For cases where the other module in the link is mounted at the same elevation, fasten the *mounting hardware leg* of the support tube vertical for each module. When the hardware leg is in this position

- the reflector dish has an obvious downward tilt.
- the *module leg* of the support tube is *not* vertical.

For a mount to a non-vertical structure such as a tapered tower, use a plumb line to ensure that the hardware leg is vertical when fastened. Proper dish, tube, and module positions for a link in this case are illustrated in [Figure 142](#). The dish is tipped forward, not vertical, but the focus of the signal is horizontal.



Figure 142: Correct mount with reflector dish

Improper dish, tube, and module positions for this case are illustrated in [Figure 143](#).



Figure 143: Incorrect mount with reflector dish

19.9.2 Modules Mounted at Different Elevations

For cases where the other module in the link is mounted at a different elevation, the assembly hardware allows tilt adjustment. The proper angle of tilt can be calculated as a factor of both the difference in elevation and the distance that the link spans. Even in this case, a plumb line and a protractor can be helpful to ensure the proper tilt. This tilt is typically minimal.

The number of degrees to offset (from vertical) the mounting hardware leg of the support tube is equal to the angle of elevation from the lower module to the higher module (b in the example provided in [Figure 39](#) on Page 149).

19.9.3 Mounting Assembly

Both the hardware that Mounting Assembly 27RD provides for adjustment and the relationship between the offset angle of the module and the direction of the beam are illustrated in [Figure 144](#).

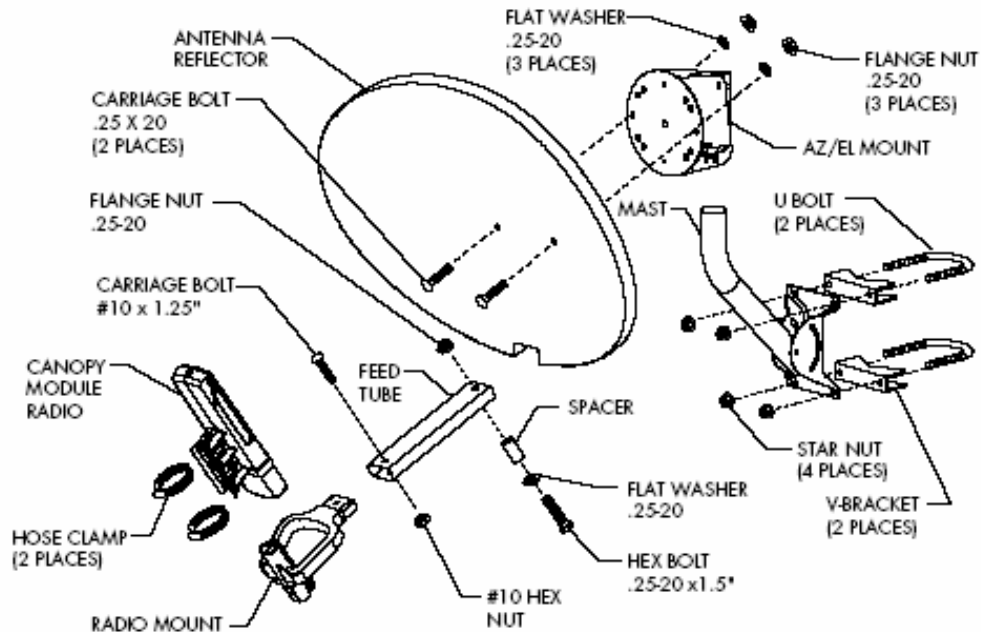


Figure 144: Mounting assembly, exploded view

19.10 INSTALLING A BH TIMING MASTER

19.10.1 Installing a PTP 100 Series BHM

To install a PTP 100 Series (FSK) BHM, perform the following steps.

Procedure 25: Installing the FSK BHM

1. Access the General tab of the Configuration page in the BHM.
2. If this is a 20-Mbps BH, set the **2X Rate** parameter to **Disabled** (temporarily for easier course aiming).
3. Click the **Save Changes** button.
4. Click the **Reboot** button.
5. After the reboot is completed, remove power from the BHM.
6. Choose the best mounting location for your particular application.
7. Attach the BHM to the arm of the Passive Reflector dish assembly as shown in [Figure 145](#) or snap a LENS into place on the BHM.



RECOMMENDATION:

The arm is molded to receive and properly aim the module relative to the aim of the dish. (See [Figure 142](#) on Page 359.) Stainless steel hose clamps should be used for the attachment.

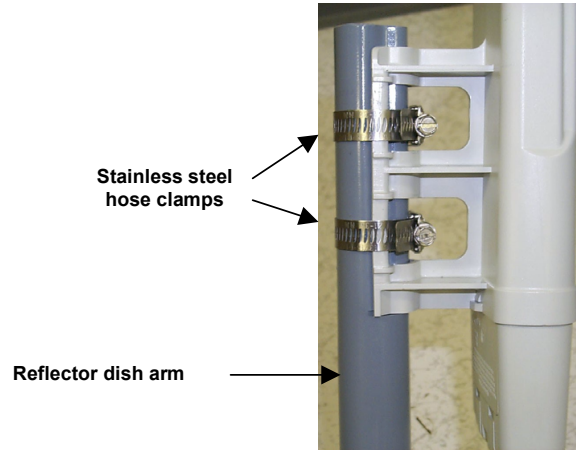


Figure 145: BH attachment to reflector arm

8. Align the BHM as follows:
 - a. Move the module to where the link will be unobstructed by the radio horizon and no objects penetrate the Fresnel zone. (The Canopy System Calculator page [AntennaElevationCalcPage.xls](#) automatically calculates the minimum antenna elevation that is required to extend the radio horizon to the other end of the link. The Canopy System Calculator page [FresnelZoneCalcPage.xls](#) automatically calculates the Fresnel zone clearance that is required between the visual line of sight and the top of a high-elevation object.)
 - b. Use a local map, compass, and/or GPS device as needed to determine the direction to the BHS.
 - c. Apply the appropriate degree of downward or upward tilt. (The Canopy System Calculator page [DowntiltCalcPage.xls](#) automatically calculates the angle of antenna downward tilt that is required.)
 - d. Ensure that the BHS is within the beam coverage area. (The Canopy System Calculator page [BeamwidthRadiiCalcPage.xls](#) automatically calculates the radii of the beam coverage area.)
9. Using stainless steel hose clamps or equivalent fasteners, lock the BHM into position.
10. Remove the base cover of the BHM. (See [Figure 51](#) on Page 182.)
11. If this BHM *will not* be connected to a CMM, optionally connect a utility cable to a GPS timing source and then to the RJ-11 port of the BHM.
12. Either connect the BHM to the CMM or connect the DC power converter to the BHM and then to an AC power source.
RESULT: When power is applied to a module or the unit is reset on the web-based interface, the module requires approximately 25 seconds to boot. During this interval, self-tests and other diagnostics are being performed.
13. Access the General tab of the Configuration page of this BHM.
14. If a CMMmicro or CMM4 is connected, set the **Sync Input** parameter to the **Sync to Received Signal (Power Port)** selection.
 If a CMM2 is connected, set the **Sync Input** parameter to the **Sync to Received Signal (Timing Port)** selection.

===== end of procedure =====

19.10.2 Installing a PTP 200 Series BHM

To install a PTP 200 Series (OFDM) BHM, use the procedure provided under [Installing a PMP 400 Series AP](#) on Page 339, with the following additional treatment for a setting that is unique to PTP 200 Series wireless Ethernet bridges.

OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol (slot) to allow multipathing to settle before receiving the desired data. A 1/4 cyclic prefix means that for every 4 bits of throughput data transmitted, an additional bit is used, A 1/8 cyclic prefix means that for every 8 bits of throughput data transmitted, an additional bit is used.

PTP 200 Series modules (OFDM BHs) are settable for either 1/8 or 1/4 cyclic prefix. The use of 1/8 cyclic prefix provides about 11% higher maximum throughput and is recommended for most cases.

The **Cyclic Prefix** is set on the Configuration => Radio page of the BHM. The default on a new unit or after the unit has been reset to factory defaults is 1/4 Cyclic Prefix. In most deployments, 1/8 Cyclic Prefix will provide a high quality, higher throughput link. In cases with severe multipathing or obstructions, 1/4 Cyclic Prefix may yield better overall results.

Procedure 26: Setting the Cyclic Prefix in a PTP 200 Series wireless Ethernet bridge

1. Before deployment, set the **Cyclic Prefix** on the Configuration => Radio page of both the BHM and the BHS to 1/8.
IMPORTANT: The **Cyclic Prefix** setting must be identical in both the BHM and the BHS. If the settings do not match, then the BHS will not register in the BHM.
2. During installation, use Link Tests to confirm link quality per standard installation and alignment procedures.
3. If a Link Test shows low throughput or efficiency, consider changing the **Cyclic Prefix** setting to 1/4 on both the BHM and the BHS along with other standard installation troubleshooting procedures such as re-aiming, off-axis aiming, changing location, raising or lowering the height of the radio, and adjusting the **Transmitter Output Power** setting.

19.11 INSTALLING A BH TIMING SLAVE

19.11.1 Installing a PTP 100 Series BHS

Installing a PTP 100 Series (FSK) BHS consists of two procedures:

- Physically installing the BHS and performing a course alignment using the alignment tone ([Procedure 27](#)).
- Verifying the BH link and finalizing alignment using review of power level and jitter, link tests, and review of registration and session counts ([Procedure 28](#) on Page 365).

Procedure 27: Installing the FSK BHS

1. Choose the best mounting location for the BHS.
2. Remove the base cover of the BHS. (See [Figure 51](#) on Page 182.)
3. Terminate the UV outside grade Category 5 Ethernet cable with an RJ-45 connector, and connect the cable to the BHS. (See [Procedure 8](#) on Page 195.)
4. Attach the BHS to the arm of the Passive Reflector dish assembly as shown in [Figure 135](#) on Page 348 or snap a LENS onto the BHS.

**RECOMMENDATION:**

The arm is molded to receive and properly aim the BH relative to the aim of the dish. Use stainless steel hose clamps for the attachment.

5. Use stainless steel hose clamps or equivalent fasteners to lock the BHS into position.
6. Remove the cover of the 600SS Surge Suppressor.
7. With the cable openings facing downward, mount the 600SS as close to the grounding system (Protective Earth) as possible.
8. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.
9. Connect an Ethernet cable from the power adapter to either RJ-45 port of the 600SS.
10. Connect another Ethernet cable from the other RJ-45 port of the 600SS to the Ethernet port of the BHS.
11. Refer to [Grounding SMs](#) on Page 176.
12. Wrap an AWG 10 (or 6mm²) copper wire around the Ground post of the 600SS.
13. Tighten the Ground post locking nut in the 600SS onto the copper wire.
14. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
15. Connect a ground wire to the 600SS.
16. Replace the cover of the 600SS surge suppressor.
17. For coarse alignment of the BHS, use the Audible Alignment Tone feature as follows:
18. If the Configuration web page of the BHS contains a **2X Rate** parameter, set it to **Disable**.
 - a. At the BHS, connect the RJ-11 6-pin connector of the Alignment Tool Headset (shown in [Figure 139](#) on Page 352) to the RJ-11 utility port of the SM.

Alternatively, instead of using the Alignment Tool Headset, use an earpiece or small battery-powered speaker connected to Pin 5 (alignment tone output) and Pin 6 (ground) of an RJ-11 connector.
 - b. Listen to the alignment tone for
 - pitch, which indicates greater signal power (RSSI/dBm) by higher pitch.
 - volume, which indicates better signal quality (lower jitter) by higher volume.
 - c. Adjust the module slightly until you hear the highest pitch and highest volume.
 - d. If the Configuration web page of the BHS contains a **2X Rate** parameter, set it back to **Enable**.

19. When you have achieved the best signal (highest pitch, loudest volume), lock the BHS in place with the mounting hardware.

===== end of procedure =====

19.11.2 Installing a PTP 200 Series BHS

To install a PTP 200 Series (OFDM) BHM, use the procedure provided under [Installing a PMP 400 Series SM](#) on Page 353, with the following additional treatment for a setting that is unique to PTP 200 Series wireless Ethernet bridges.

OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol (slot) to allow multipathing to settle before receiving the desired data. A 1/4 cyclic prefix means that for every 4 bits of throughput data transmitted, an additional bit is used, A 1/8 cyclic prefix means that for every 8 bits of throughput data transmitted, an additional bit is used.

PTP 200 Series modules (OFDM BHs) are settable for either 1/8 or 1/4 cyclic prefix. The use of 1/8 cyclic prefix provides about 11% higher maximum throughput and is recommended for most cases.

The **Cyclic Prefix** is set on the Configuration => Radio page of the BHM. The default on a new unit or after the unit has been reset to factory defaults is 1/4 Cyclic Prefix. In most deployments, 1/8 Cyclic Prefix will provide a high quality, higher throughput link. In cases with severe multipathing or obstructions, 1/4 Cyclic Prefix may yield better overall results.

To perform and possibly adjust the setting, use [Procedure 26: Setting the Cyclic Prefix in a PTP 200 Series wireless Ethernet bridge](#) on Page 363.

19.12 UPGRADING A BH LINK TO BH20

To replace a pair of 10-Mbps BHs with 20-Mbps BHs, you can minimize downtime by temporarily using the 10-Mbps capability in the faster modules. However, both interference and differences in receiver sensitivity can make alignment and link maintenance more difficult than in the previous 10-Mbps link. The effects of these factors are greater at greater link distances, particularly at 5 miles or more.

In shorter spans, these factors may not be prohibitive. For these cases, set the first replacement module to **1X Rate** and establish the link to the 10-Mbps BH on the far end. Similarly, set the second replacement module to **1X Rate** and re-establish the link. With both of the faster modules in place and with an operational link having been achieved, reset their modulation to **2X Rate** (20 Mbps).

19.13 VERIFYING A BH LINK

To verify the backhaul link after the BHS has been installed, perform the following steps.

Procedure 28: Verifying performance for a BH link

1. Using a computer (laptop, desktop, PDA) connected to the BHS, open a browser and access the BHS using the default IP address of <http://169.254.1.1> (or the IP address configured in the BHS, if one has been configured.)
2. On the General Status tab of the Home page in the BHS (shown in [Figure 71](#) on Page 216), look for **Power Level** and **Jitter**.

IMPORTANT: The received **Power Level** is shown in dBm and should be maximized. **Jitter** should be minimized. However, better/lower jitter should be

avored over better/higher dBm. For example, if coarse alignment gives a BHS a power level of -75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to -78 dBm and the jitter to 2 or 3, the latter would be better, with the following caveats:

- When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
- When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

PTP 200 Series BHSs do not have this parameter.



NOTE:

For historical reasons, **RSSI** is also shown and is the unitless measure of power. The best practice is to use **Power Level** and ignore **RSSI**, which implies more accuracy and precision than is inherent in its measurement.

3. Fine-adjust the BHS mounting, if needed, to improve **Jitter** or **Power Level**.
4. Click the Link Capacity Test tab of the Tools web page in the BHS.
NOTE: Use of this tool is described under [Using the Link Capacity Test Tool \(All\)](#) on Page 438.
5. Perform several link tests of 10-second duration as follows:
 - a. Type into the **Duration** field how long (in seconds) the RF link should be tested.
 - b. Leave the **Packet Length** field (when present) set to the default of 1522 bytes or type into that field the packet length at which you want the test conducted.
 - c. Leave the **Number of Packets** field set to 0 (to flood the link).
 - d. Click the **Start Test** button.
 - e. View the results of the test.
6. If these link tests fail to consistently show 90% or greater efficiency in 1X operation or 50 to 60% efficiency in 2X, troubleshoot the link, using the data as follows:
 - If the downlink is consistently 90% efficient, but the uplink is only 40%, this indicates trouble for the BHS transmitting to the BHM. Investigate a possible source of interference near the BHM.
 - If the uplink is consistently 90% efficient, but the downlink is only 40%, this indicates trouble for the BHM transmitting to the BHS. Investigate a possible source of interference near the BHS.

If these link tests consistently show 90% or greater efficiency in 1X operation, or 50 to 60% efficiency in 2X operation, in both uplink and downlink, continue this procedure.
7. Open the Session Status tab in the Home page of the BHM.
NOTE: An example of this page is shown in [Figure 146](#).

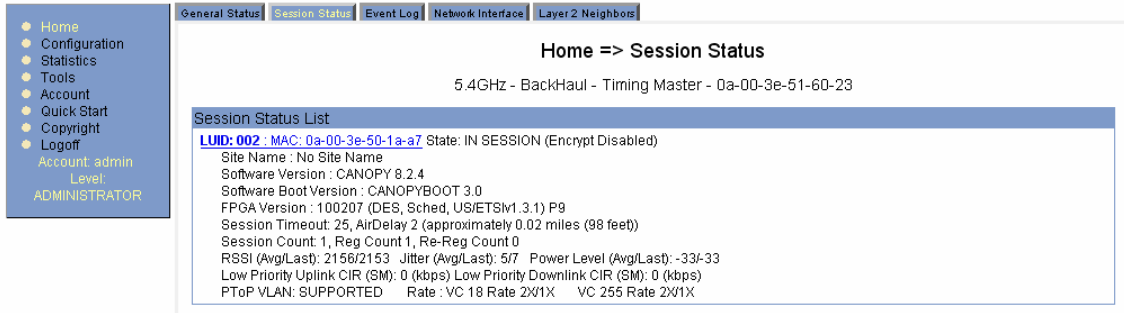


Figure 146: Session Status tab of BHM

8. Find the **Session Count** line under the MAC address of the BHS.
9. Check and note the values for **Session Count**, **Reg Count**, and **Re-Reg Count**.
10. Briefly monitor these values, occasionally refreshing this page by clicking another tab and then the Session Status tab again.
11. If these values are low (for example, 1, 1, and 0, respectively, meaning that the BHS registered and started a stable session once) and not changing
 - a. consider the installation successful.
 - b. monitor these values from the network office over the next several hours and days.

If these values are greater than 1, 1, and 0, or they increase while you are monitoring them, troubleshoot the link. (For example, recheck jitter as described in [Procedure 21: Installing the FSK SM](#) or recheck link efficiency as described in this procedure, then look for sources of RF interference or obstructions.)

===== end of procedure =====

20 VERIFYING SYSTEM FUNCTIONALITY

To verify system functionality after the APs and or BHs have been installed, perform the following steps.

Procedure 29: Verifying system functionality

1. For each installed AP, use a computer or PDA connected to an SM set to a compatible configuration (frequency and color code, for example) and verify link functionality.
2. For each BH installed, use a notebook computer connected to a BH (BHM or BHS, as appropriate) set to a compatible configuration and verify link functionality.
3. If a network data feed is present and operational, use an SM or BHS to verify network functionality.

===== **end of procedure** =====

OPERATIONS GUIDE

21 GROWING YOUR NETWORK

Keys to successfully growing your network include

- monitoring the RF environment.
- considering software release compatibility.
- redeploying modules appropriately and quickly.

21.1 MONITORING THE RF ENVIRONMENT

Regardless of whether you are maintaining or growing your network, you may encounter new RF traffic that can interfere with your current or planned equipment. Regularly measuring *over a period of time* and logging the RF environment, as you did before you installed your first equipment in an area, enables you to recognize and react to changes.

21.1.1 Spectrum Analyzer

In both an FSK and an OFDM module, the spectrum analyzer measures and displays the detected *peak* power level. This is consistent with the received Power Level that various tabs in the FSK modules report. However, it is inconsistent with received Power Level indications in OFDM modules, which use this parameter to report the detected *average* power level. For this reason, you will observe a difference in how the spectrum analyzer and the Power Level field separately report on the same OFDM signal at the same time.

The integrated spectrum analyzer can be very useful as a tool for troubleshooting and RF planning, but is not intended to replicate the accuracy and programmability of a high-end spectrum analyzer, which you may sometime need for other purposes.



IMPORTANT!

When you enable the Spectrum Analyzer on a module, it enters a scan mode and drops any RF connection it may have had. Scanning mode ends when either you click **Disable** on the Spectrum Analyzer page, or it times out after 15 minutes and returns to operational mode.

For this reason

- *do not* enable the spectrum analyzer on a module you are connected to via RF. The connection will drop for 15 minutes, and when the connection is re-established no readings will be displayed.
- be advised that, if you enable the spectrum analyzer by Ethernet connection, the RF connection to that module drops.

You can use any module to see the frequency and power level of any detectable signal that is within, just above, or just below the frequency band range of the module.



RECOMMENDATION:

Vary the days and times when you analyze the spectrum in an area. The RF environment can change throughout the day or throughout the week.

Temporarily deploy an SM or BHS for *each* frequency band range that you need to monitor and access the Spectrum Analyzer tab in the Tools web page of the module. (For access from a PDA, see [PDA Access to Modules](#) on Page 335.) To enter the scan mode and view readings, click **Enable**.

After clicking the **Enable** button on the Spectrum Analyzer page, the first “painting” may not display bars for all frequencies, especially on frequency bands with a large number of center channels, like the 5.4 GHz band. Clicking **Enable** again will display the entire spectrum bar graph. Alternatively, you can set the “Auto Refresh” time on the Configuration => General page to a few seconds to have the Spectrum Analyzer automatically fully displayed and refreshed. (Setting the “Auto Refresh” time back to 0 will disable refresh.)

21.1.2 Graphical Spectrum Analyzer Display

An SM/BHS displays the graphical spectrum analyzer. An example of the Spectrum Analyzer tab is shown in [Figure 147](#).

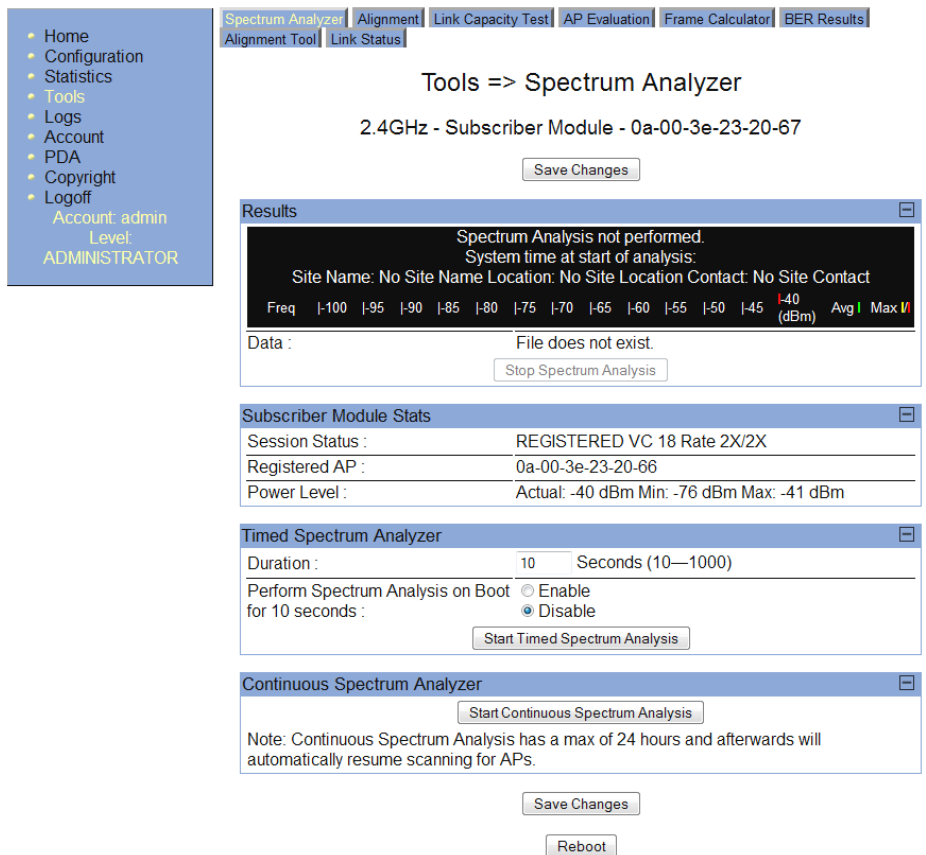


Figure 147: Spectrum Analyzer tab of SM, example

Colors in the display have the following meanings:

- Green bars show the most recent measurements.
- Yellow ticks show the maximum measurements from the current spectrum analysis session.
- Red ticks show measurements of -40 dBm or stronger.

To keep the displayed data current, either set “Auto Refresh” on the module’s Configuration => General page to a few seconds, or repeatedly click the **Enable** button. When you are finished analyzing the spectrum, click the **Disable** button to return the module to normal operation.

21.1.3 Using the AP as a Spectrum Analyzer

You can temporarily change an AP into an SM and thereby use the spectrum analyzer functionality. This is the only purpose supported for the transformation.



CAUTION!

When you change an AP into an SM, any connections to SMs off that AP are lost. Therefore, you should ensure you are connected to the AP through its *Ethernet* side (not RF side) before changing it into an SM.

For example, if you are connected to an AP through one of its SMs and mistakenly change the AP into an SM, you will lose connectivity and will need to gain access to the Ethernet side of the AP through another part of your network to change it back into an AP.

To transform a VLAN-disabled AP into an SM for spectrum analysis and then return the device to an AP, perform the following steps.

Procedure 30: Using the Spectrum Analyzer in AP feature, VLAN disabled

1. Connect to the wired Ethernet interface of the AP.
2. Access the General tab of the Configuration page in the AP.
3. Set the **Device Setting** parameter to **SM**.
4. Click the **Save Changes** button.
5. Click the **Reboot** button.
6. When the module has rebooted as an SM, click the Tools navigation link on the left side of the Home page.
7. Click the Spectrum Analyzer tab.
NOTE: If you simply click the **Enable** button on the Spectrum Analyzer tab, the display may include fewer than all frequencies that are detectable, especially in a band, such as 5.4 GHz, where the number of available center channels is great. If you then click the **Enable** button a second time or set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds, the display includes the entire spectrum. You can later reset **Webpage Auto Update** to 0, to disable refresh.
8. Either set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds or repeatedly click the **Enable** button.
RESULT: The module enters the scan mode.
9. When you are finished analyzing the spectrum, click the **Disable** button.
10. In the left-side navigation links, click Configuration.
11. Click the General tab.
12. Set the **Device Setting** parameter to **AP**.
13. Click the **Save Changes** button.

14. Click the **Reboot** button.

RESULT: The AP boots with its previous frequency setting.

===== end of procedure =====

If you reboot an AP that has a configured **Management VID** parameter and **Device Type** parameter set to **SM**, you are automatically removing the AP from the Management VLAN. The following procedure enables you to successfully analyze the spectrum and return to management via the VLAN feature. In many cases, it is advisable to use this procedure to

1. transform all APs in a cluster into SMs.
2. perform spectrum analysis without Management VLAN, one sector at a time.
3. return all APs in the cluster to their Management VLAN for access.

To transform a VLAN-enabled AP into an SM for spectrum analysis and then return the device to an AP, perform the following steps.

Procedure 31: Using the Spectrum Analyzer in AP feature, VLAN enabled

1. Access the VLAN-enabled AP through its Management VLAN.
NOTE: How you do this depends on your local configuration.
2. Access the General tab of the Configuration page in the AP.
3. Set the **Device Setting** parameter to **SM**.
4. Click the **Save Changes** button.
5. Click the **Reboot** button.
RESULT: Connectivity to the module is lost.
6. Access the module without using the Management VLAN.
NOTE: How you do this depends on your local configuration. You may need to connect to a different, non-tagging port of the VLAN switch in your NOC.
7. Click the Tools navigation link on the left side of the Home page.
8. Click the Spectrum Analyzer tab.
NOTE: If you simply click the **Enable** button on the Spectrum Analyzer tab, the display may include fewer than all frequencies that are detectable, especially in a band, such as 5.4 GHz, where the number of available center channels is great. If you then click the **Enable** button a second time or set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds, then the display will include the entire spectrum.
9. Either set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds or repeatedly click the **Enable** button.
RESULT: The module enters the scan mode.
10. When you are finished analyzing the spectrum, click the **Disable** button.
11. In the left-side navigation links, click Configuration.
12. Click the General tab.
13. Set the **Device Setting** parameter to AP.
14. Click the **Save Changes** button.
15. Click the **Reboot** button.
RESULT: Connectivity to the module is lost.

16. Access the AP through its Management VLAN.

NOTE: How you do this depends on your local configuration. You may need to connect to the appropriate tagging port of the VLAN switch in your NOC.

===== **end of procedure** =====

21.2 CONSIDERING SOFTWARE RELEASE COMPATIBILITY

Within the same network, modules can operate on multiple software releases. However, the features that can be enabled are limited to those that the earliest software supports.

21.2.1 Designations for Hardware in Radios

Documentation refers to hardware series (for example, Series P9). Releases 8 and later requires APs, BHs, and AES SMs to be Series P9 or later hardware. The correlation between hardware series and the MAC addresses of the radio modules is provided in [Table 60](#).

Table 60: Hardware series by MAC address

Radio Frequency Band Range	Hardware Series	
	P7 or P8 in These MAC Addresses	P9 or Later in These MAC Addresses
900	None	All
2.4	≤ 0A003E20672B	≥ 0A003E20672C
5.2	≤ 0A003E00F4E3	≥ 0A003E00F4E4
5.4	None	All
5.7	≤ 0A003EF12AFE	≥ 0A003EF12AFF

Differences in capabilities among these hardware series are summarized in [Table 61](#).

Table 61: Hardware series differences

Capability	Availability per Hardware Series		
	P7	P8	P9, P10, or P11
Auto-sense Ethernet cable scheme	no	yes	yes
Support CMMmicro	no	yes	yes
Support CMM4	no	yes	yes
Support hardware scheduling in APs	no	no	yes
Support 2X operation in APs and SMs	no	no	yes
<i>NOTES:</i> An SM of P7 or P8 series requires an FPGA load through CNUT for access to hardware scheduling, and then only at 1X operation. An AP of P7 or P8 series cannot perform hardware scheduling.			

CAP 130 P9 APs provide higher throughput and lower latency than earlier series APs and support configuring the high-priority channel per SM. CAP 120 APs *do not* provide the higher throughput and lower latency, but they do support configuring the high-priority channel per SM.

21.2.2 MIB File Set Compatibility

Although MIB files are text files (not software), they define objects associated with configurable parameters and indicators for the module and its links. In each release, some of these parameters and indicators are not carried forward from the previous release, and some parameters and indicators are introduced or changed.

For this reason, use the MIB files from your download to replace previous MIB files in conjunction with your software upgrades, even if the file names are identical to those of your previous files. Date stamps on the MIB files distinguish the later set.

21.3 REDEPLOYING MODULES

Successfully redeploying a module may involve

- maintaining full and accurate records of modules being redeployed from warehouse stock.
- exercising caution about
 - software compatibility. For example, whether desired features can be enabled with the redeployed module in the network.
 - procedural handling of the module. For example
 - whether to align the SM or BHS by power level and jitter or by only jitter.
 - whether the module auto-senses the Ethernet cable connector scheme.
 - hardware compatibility; for example, where a CMMmicro is deployed.
 - the value of each configurable parameter. Whether all are compatible in the new destination.
- remembering to use auto discovery to add the redeployed SM to the network in Prizm.

21.3.1 Wiring to Extend Network Sync

The following procedure can be used to extend network sync by one additional hop, as described under [Passing Sync in an Additional Hop](#) on Page 99. Where a collocated module receives sync over the air, the collocated modules can be wired to pass the sync as follows:

Procedure 32: Extending network sync

1. Connect the GPS Utility ports of the collocated modules using a sync cable with RJ-11 connectors.
2. Set the **Sync Input** parameter on the Configuration page of the collocated AP or BH timing master to **Sync to Received Signal (Timing Port)**.
3. Set the **Frame Timing Pulse Gated** parameter on the Configuration page of the collocated SM or BH timing slave to **Enable**.
NOTE: This setting prevents interference in the event that the SM or BH timing slave loses sync.

===== end of procedure =====

22 SECURING YOUR NETWORK

22.1 ISOLATING APs FROM THE INTERNET

Ensure that the IP addresses of the APs in your network

- are not routable over the Internet.
- do not share the subnet of the IP address of your user.

RFC 1918, *Address Allocation for Private Subnets*, reserves for private IP networks three blocks of IP addresses that are not routable over the Internet:

- /8 subnets have one reserved network, 10.0.0.0 to 10.255.255.255.
- /16 subnets have 16 reserved networks, 172.16.0.0 to 172.31.255.255.
- /24 subnets have 256 reserved networks, 192.168.0.0 to 192.168.255.255.

22.2 ENCRYPTING RADIO TRANSMISSIONS

Motorola fixed wireless broadband IP systems employ the following forms of encryption for security of the wireless link:

- BRAID—a security scheme that the cellular industry uses to authenticate wireless devices.
- DES—Data Encryption Standard, an over-the-air link option that uses secret 56-bit keys and 8 parity bits.
- AES—Advanced Encryption Standard, an extra-cost over-the-air link option that provides extremely secure wireless connections. AES uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.

BRAID is a stream cipher that the TIA (Telecommunications Industry Association) has standardized. Standard APs and SMs use BRAID encryption to

- calculate the per-session encryption key (independently) on each end of a link.
- provide the digital signature for authentication challenges.

22.2.1 DES Encryption

Standard modules provide DES encryption. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES Encryption does not affect the performance or throughput of the system.

22.2.2 AES Encryption

Motorola also offers fixed wireless broadband IP network products that provide AES encryption. AES uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. Because of this higher level of security, the government of the U.S.A. controls the export of communications products that use AES (among which the AES feature activation key is one) to ensure that these products are available in only certain regions and by special permit.

The distributor or reseller can advise service providers about current regional availability. AES products are certified as compliant with the Federal Information Processing Standards (FIPS) in the U.S.A. The National Institute of Standards and Technology (NIST) in the U.S.A. has specified AES for significantly greater security than that which DES provides. NIST selected the AES algorithm for providing the best combination of security, performance, efficiency, implementation, and flexibility. NIST collaborates with industry to develop and apply technology, measurements, and standards.

22.2.3 AES-DES Operability Comparisons

This section describes the similarities and differences between DES and AES products, and the extent to which they may interoperate.

The DES AP and the DES BHM modules are factory-programmed to enable or disable *DES* encryption. Similarly, the AES AP and the AES BHM modules are factory-programmed to enable or disable *AES* encryption. In either case, the authentication key entered in the Configuration page establishes the encryption key. For this reason, the authentication key must be the same on each end of the link. See [Authentication Key](#) on Page 280.

Feature Availability

AES products run the same software as DES products. Thus feature availability and functionality are and will continue to be the same, regardless of whether AES encryption is enabled. All interface screens are identical. However, when encryption is enabled on the Configuration screen

- the AES product provides AES encryption.
- the DES product provides DES encryption.

AES and DES products use different FPGA (field-programmable gate array) loads. However, the AES FPGA will be upgraded as needed to provide new features or services similar to those available for DES products.

Canopy DES products cannot be upgraded to AES. To have the option of AES encryption, the operator must purchase AES products.

Interoperability

AES and DES products do not interoperate when enabled for encryption. For example, An AES AP with encryption enabled cannot communicate with DES SMs. Similarly, an AES Backhaul timing master module with encryption enabled cannot communicate with a DES Backhaul timing slave module.

However, if encryption is disabled, AES modules can communicate with DES modules.

22.3 MANAGING MODULE ACCESS BY PASSWORDS

22.3.1 Adding a User for Access to a Module

From the factory, each module has a preconfigured administrator-level account in the name `root`, which initially requires no associated password. This is the same `root` account that you may have used for access to the module by `telnet` or `ftp`. When you upgrade a module

- an account is created in the name `admin`.
- both `admin` and `root` inherit the password that was previously used for access to the module:
 - the **Full Access** password, if one was set.
 - the **Display-Only Access** password, if one was set and no Full Access password was set.



IMPORTANT!

If you use Prizm, *do not* delete the `root` account from any module. If you use an NMS that communicates with modules through SNMP, *do not* delete the `root` account from any module unless you first can confirm that the NMS does not rely on the `root` account for access to the modules.

Each module supports four or fewer user accounts, regardless of account levels. The available levels are

- ADMINISTRATOR, who has full read and write permissions. This is the level of the `root` and `admin` users, as well as any other administrator accounts that one of them creates.
- INSTALLER, who has permissions identical to those of ADMINISTRATOR except that the installer cannot add or delete users or change the password of any other user.
- GUEST, who has no write permissions and only a limited view of General Status tab, as shown in [Figure 148](#), and can log in as a user.

From the factory default state, configure passwords for both the `root` and `admin` account at the ADMINISTRATOR permission level, using the Account => Change Users Password tab. (If you configure only one of these, then the other will still require no password for access into it and thus remain a security risk.) If you are intent on configuring only one of them, delete the `admin` account. The `root` account is the only account that CNUT uses to update and Prizm uses to manage the module.

General Status

Home => General Status

5.7GHz - Access Point - 0a-00-3e-d5-b9-97

Device Information	
Device Type :	5.7GHz - Access Point - 0a-00-3e-d5-b9-97
Software Version :	CANOPY 9.4.2 AP-DES
Software BOOT Version :	CANOPYBOOT 1.0
Board Type :	P11
FPGA Version :	021909
FPGA Type :	C40
PLD Version :	1
Uptime :	01:38:17
System Time :	01:38:17 01/01/2001
Last NTP Time Update :	00:00:00 00/00/0000
Ethernet Interface :	100Base-TX Full Duplex
Regulatory :	Passed
DFS :	Normal Transmit
Antenna :	Vertical

Access Point Stats	
Registered SM Count :	1
GPS Sync Pulse Status :	Receiving Sync
Max Registered SM Count :	1

Site Information	
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Figure 148: General Status tab view for GUEST-level account

An example of the Add User tab is displayed in Figure 149.

Change Users Password | Add User | Delete User

Account => Add User

5.7GHz - Subscriber Module - 0a-00-3e-f0-25-d9

Add User	
User Name :	<input type="text"/>
Level :	INSTALLER
New Password :	<input type="password"/>
Confirm Password :	<input type="password"/>
<input type="button" value="Add"/>	

Account Status	

Figure 149: Add User tab of SM, example

After a password has been set for any ADMINISTRATOR-level account, initial access to the module GUI opens the view of GUEST level (Figure 148).

22.3.2 Deleting a User from Access to a Module

The Account => Delete User tab provides a drop-down list of configured users from which to select the user you want to delete.

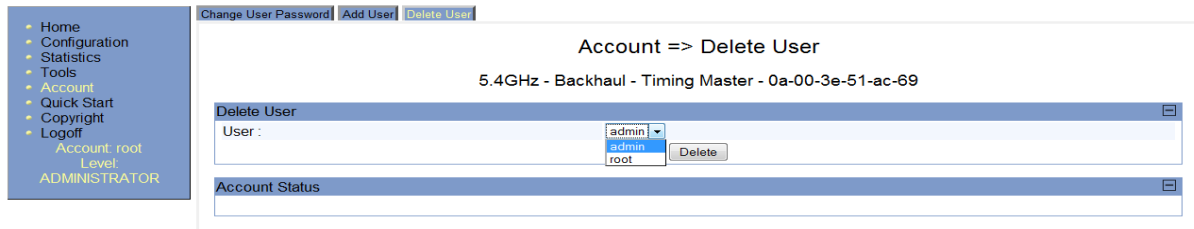


Figure 150: Delete User tab of SM, example

Accounts that cannot be deleted are

- the current user's own account.
- the last remaining account of ADMINISTRATOR level.

22.3.3 Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH

A small adjunctive product allows you to temporarily override some AP/SM/BH settings and thereby regain control of the module. This override plug is needed for access to the module in any of the following cases:

- You have forgotten either
 - the IP address assigned to the module.
 - the password that provides access to the module.
- The module has been locked by the No Remote Access feature. (See [Denying All Remote Access](#) on Page 467 and [Reinstating Remote Access Capability](#) on Page 467.)
- You want local access to a module that has had the 802.3 link disabled in the Configuration page.

You can configure the module such that, when it senses the override plug, it responds by either

- resetting the LAN1 IP address to 169.254.1.1, allowing access through the default configuration without *changing* the configuration, whereupon you will be able to view and reset any non-default values as you wish.
- resetting all configurable parameters to their factory default values.

Acquiring the Override Plug

You can either purchase or fabricate an override plug as follows. To purchase an override plug for a nominal fee, order the plug at <http://www.best-tronics.com/motorola.htm>. To fabricate an override plug, perform the following steps.

Procedure 33: Fabricating an override plug

1. Install an RJ-11 6-pin connector onto a 6-inch length of CAT 5 cable.
2. Pin out all 6-pins.
3. Short (solder together) Pins 4 and 6 on the other end. Do not connect any other wires to anything. The result should be as shown in [Figure 151](#).

===== end of procedure =====

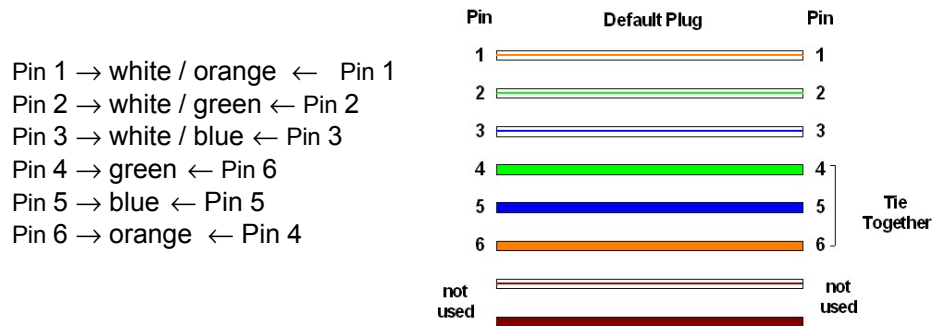



Figure 151: RJ-11 pinout for the override plug

Using the Override Plug



IMPORTANT!

While the override plug is connected to a module, the module can neither register nor allow registration of another module.

To regain access to the module, perform the following steps.

Procedure 34: Regaining access to a module

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power cycle by removing, then re-inserting, the Ethernet cable.
RESULT: The module boots with the default IP address of 169.254.1.1, password fields blank, and all other configuration values as previously set.
3. Wait approximately 30 seconds for the boot to complete.
4. Remove the override plug.
5. Set passwords and IP address as desired.
6. Change configuration values if desired.
7. Click the **Save Changes** button.
8. Click the **Reboot** button.

===== end of procedure =====

22.4 REQUIRING SM AUTHENTICATION

Through the use of Prizm Release 2.0 or later, or BAM Release 2.1, you can enhance network security by requiring SMs to authenticate when they register. Three keys and a random number are involved in authentication as follows:

- factory-set key in each SM. Neither the subscriber nor the network operator can view or change this key.
- authentication key, also known as authorization key and skey. This key matches in the SM and AP as the **Authentication Key** parameter, and in the Prizm database.
- random number, generated by Prizm or BAM and used in each attempt by an SM to register and authenticate. The network operator can view this number.
- session key, calculated separately by the SM and Prizm or BAM, based on both the authentication key (or, by default, the factory-set key) and the random number. Prizm or BAM sends the session key to the AP. The network operator cannot view this key.

None of the above keys is ever sent in an over-the-air link during an SM registration attempt. However, with the assumed security risk, the operator can create and configure the **Authentication Key** parameter. See [Authentication Key](#) on Page 280.

22.5 FILTERING PROTOCOLS AND PORTS

You can filter (block) specified protocols and ports from leaving the SM and entering the network. This protects the network from both intended and inadvertent packet loading or probing by network users. By keeping the specified protocols or ports off the network, this feature also provides a level of protection to users from each other.

Protocol and port filtering is set per SM. Except for filtering of SNMP ports, filtering occurs as packets leave the SM. If an SM is configured to filter SNMP, then SNMP packets are blocked from entering the SM and, thereby, from interacting with the SNMP portion of the protocol stack on the SM.

22.5.1 Port Filtering with NAT Enabled

Where NAT is enabled, you can filter only the three user-defined ports. The following are example situations in which you can configure port filtering where NAT is enabled.

- To block a subscriber from using FTP, you can filter Ports 20 and 21 (the FTP ports) for both the TCP and UDP protocols.
- To block a subscriber from access to SNMP, you can filter Ports 161 and 162 (the SNMP ports) for both the TCP and UDP protocols.
NOTE: In only the SNMP case, filtering occurs before the packet interacts with the protocol stack.

22.5.2 Protocol and Port Filtering with NAT Disabled

Where NAT is disabled, you can filter both protocols and the three user-defined ports. Using the check boxes on the interface, you can either

- allow all protocols except those that you wish to block.
- block all protocols except those that you wish to allow.

You can allow or block any of the following protocols:

- PPPoE (Point to Point Protocol over Ethernet)
- Any or all of the following IPv4 (Internet Protocol version 4) protocols:
 - SMB (Network Neighborhood)
 - SNMP
 - Up to 3 user-defined ports
 - All other IPv4 traffic (see [Figure 152](#))
- Uplink Broadcast
- ARP (Address Resolution Protocol)
- All others (see [Figure 152](#))

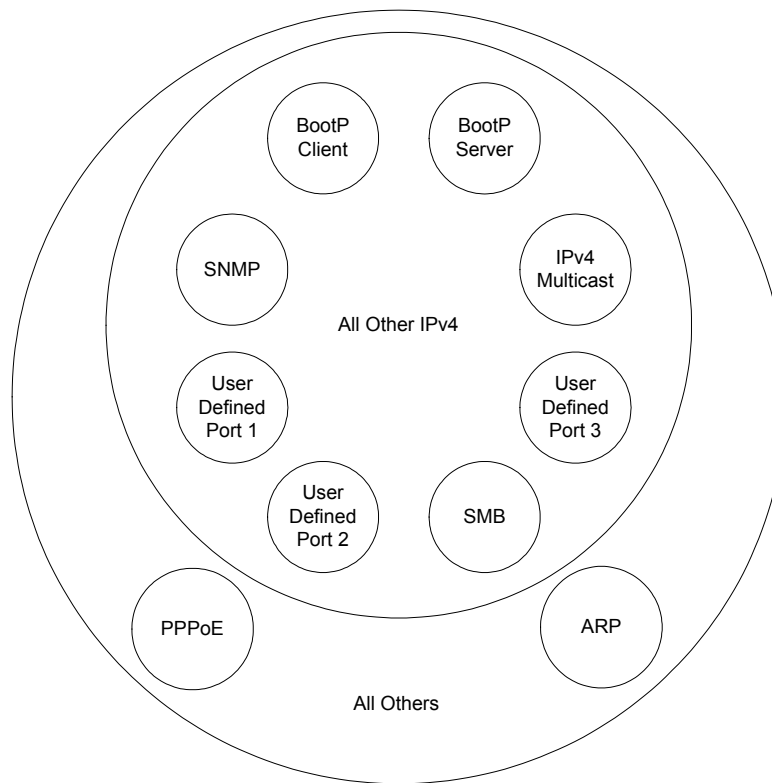


Figure 152: Categorical protocol filtering

The following are example situations in which you can configure protocol filtering where NAT is disabled:

- If you block a subscriber from only PPOE and SNMP, then the subscriber retains access to all other protocols and all ports.
- If you block PPOE, IPv4, and Uplink Broadcast, and you also check the **All others** selection, then only Address Resolution Protocol is not filtered.

The ports that are filtered as a result of protocol selections in the Protocol Filtering tab of the SM are listed in [Table 62](#). Further information is provided under [Protocol Filtering Tab of the SM](#) on Page 288.

Table 62: Ports filtered per protocol selections

Protocol Selected	Port Filtered (Blocked)
SMB	Destination Ports 137 TCP and UDP, 138 UDP, 139 TCP, 445 TCP
SNMP	Destination Ports 161 TCP and UDP, 162 TCP and UDP
Bootp Client	Source Port 68 UDP
Bootp Server	Source Port 67 UDP

22.6 ENCRYPTING DOWNLINK BROADCASTS

An AP can be enabled to encrypt downlink broadcast packets such as the following:

- ARP
- NetBIOS
- broadcast packets containing video data on UDP.

The encryption used is DES for a DES module, and AES for an AES module. Before the Encrypt Downlink Broadcast feature is enabled on the AP, air link security should be enabled on the AP.

22.7 ISOLATING SMs

In an AP, you can prevent SMs in the sector from directly communicating with each other. In CMMmicro Release 2.2 or later and the CMM4, you can prevent connected APs from directly communicating with each other, which prevents SMs that are in different sectors of a cluster from communicating with each other.

In the AP, the **SM Isolation** parameter is available in the General tab of the Configuration web page. In the drop-down menu for that parameter, you can configure the SM Isolation feature by any of the following selections:

- **Disable SM Isolation** (the default selection). This allows full communication between SMs.
- **Block SM Packets from being forwarded**. This prevents both multicast/broadcast and unicast SM-to-SM communication.
- **Block and Forward SM Packets to Backbone**. This not only prevents multicast/broadcast and unicast SM-to-SM communication but also sends the packets, which otherwise would have been handled SM to SM, through the Ethernet port of the AP.

In the CMMmicro and the CMM4, SM isolation treatment is the result of how you choose to manage the port-based VLAN feature of the embedded switch, where you can switch all traffic from any AP or BH to an uplink port that you specify. However, this is not packet level switching. It is not based on VLAN IDs. See the **VLAN Port Configuration** parameter in the dedicated user guide that supports the CMM product that you are deploying.

22.8 FILTERING MANAGEMENT THROUGH ETHERNET

You can configure the SM to disallow any device that is connected to its Ethernet port from accessing the IP address of the SM. If you set the **Ethernet Access Control** parameter to **Enabled**, then

- no attempt to access the SM management interface (by http, SNMP, telnet, ftp, or tftp) through Ethernet can succeed.
- any attempt to access the SM management interface over the air (by IP address, presuming that **LAN1 Network Interface Configuration, Network Accessibility** is set to **Public**, or by link from the Session Status or Remote Subscribers tab in the AP) is unaffected.

22.9 ALLOWING MANAGEMENT FROM ONLY SPECIFIED IP ADDRESSES

The Security tab of the Configuration web page in the AP, SM, and BH includes the **IP Access Control** parameter. You can specify one, two, or three IP addresses that should be allowed to access the management interface (by http, SNMP, telnet, ftp, or tftp).

If you select

- **IP Access Filtering Disabled**, then management access is allowed from any IP address, even if the **Allowed Source IP 1 to 3** parameters are populated.
- **IP Access Filtering Enabled**, and specify at least one address in the **Allowed Source IP 1 to 3** parameter, then management access is limited to the specified address(es). If you intend to use Prizm to manage the element, then you must ensure that the IP address of the Prizm server is listed here.

22.10 CONFIGURING MANAGEMENT IP BY DHCP

The IP tab in the Configuration web page of every radio contains a **LAN1 Network Interface Configuration, DHCP State** parameter that, if enabled, causes the IP configuration (IP address, subnet mask, and gateway IP address) to be obtained through DHCP instead of the values of those individual parameters. The setting of this DHCP state parameter is also viewable, but is not settable, in the Network Interface tab of the Home page.

In the SM, this parameter is settable

- in the NAT tab of the Configuration web page, but only if NAT is enabled.
- in the IP tab of the Configuration web page, but only if the **Network Accessibility** parameter in the IP tab is set to **Public**.

23 MANAGING BANDWIDTH AND AUTHENTICATION

This section provides a high-level description of bandwidth and authentication management in a network. For more specific information, see the *Motorola Canopy Prizm Release 3.2 User Guide*.

23.1 MANAGING BANDWIDTH WITHOUT BAM

Unless Prizm or BAM is deployed and is configured in the AP, bandwidth management is limited to applying a single sustained data rate value (for uplink and for downlink) and a single burst allocation value (for uplink and for downlink) to every SM that registers in the AP.

23.2 BANDWIDTH AND AUTHENTICATION MANAGER (BAM) SERVICES AND FEATURES

Prizm or BAM enables you to perform the following management operations on SMs:

- Change the key that the SMs need for authenticating.
- Temporarily suspend or reinstate a subscriber.
- Set burst size and data transfer rate caps for an SM or group of SMs.
- Use licensing to uncap an SM or group of SMs.
- List all ESNs that are associated with a specified VLAN ID.
- Associate or dissociate an SM or group of SMs with a specified VLAN ID.
- Set VLAN parameters.
- Toggle whether to send those VLAN parameters to the SMs.
- Set CIR parameters for low-priority and high-priority channel rates.
- Toggle whether to send those CIR parameters to the SMs.
- Toggle whether to enable the high-priority channel in the SMs.

23.2.1 Bandwidth Manager Capability

Prizm or BAM allows you to set bandwidth per SM for sustained rates and burst rates. With this capability, the system allows both

- burst rates beyond those of many other broadband access solutions.
- control of average bandwidth allocation to prevent excessive bandwidth usage by a subscriber.

All packet throttling occurs in the SMs and APs based on Quality of Service (QoS) data that the Prizm or BAM server provides. No server processing power or network messages are needed for packet throttling.

QoS management also supports marketing of broadband connections at various data rates, for operator-defined groups of subscribers, and at various price points. This allows you to meet customer needs at a price that the customer deems reasonable and affordable.

When **Authentication Required** is selected in the Security tab of the AP Configuration web page and one or more **Authentication Server** is specified by IP address, bandwidth management is expanded to apply uniquely specified sustained data rate and burst allocation values to each SM registered in the AP. So, you can define differently priced tiers of subscriber service.

Designing Tiered Subscriber Service Levels

Examples of levels of service that vary by bandwidth capability are provided in [Table 63](#) and [Table 64](#).



NOTE:

The speeds that these tables correlate to service levels are comparative examples. Actual download times may be greater due to use of the bandwidth by other SMs, congestion on the local network, congestion on the Internet, capacity of the serving computer, or other network limitations.

Table 63: Example times to download for typical tiers of service with CAP 120

Equipment	AP	CAP 120		
	SM	CSM 120		
	Operation	1X		
	Max burst speed	4.4 Mbps		
Example Settings	Service Type	Premium	Regular	Basic
	Sustained Downlink Data Rate	5250 Kbps	1000 Kbps	256 Kbps
	Sustained Uplink Data Rate	1750 Kbps	500 Kbps	128 Kbps
	Downlink and Uplink Burst Allocations	500000 Kb	80000 Kb	40000 Kb
Download (sec)	Web page	<1	<1	<1
	5 MB	9	9	9
	20 MB	36	80	470
	50 MB	91	320	1400
	300 MB	545	2320	9220

Table 64: Example times to download for typical tiers of service with CAP 130

Equipment	AP	CAP 130						
	SM	CSM 130						
	Operation	1X			2X			2X
	Max burst speed	5 Mbps			10 Mbps			10 Mbps
Example Settings	Service Type	Premium	Regular	Basic	Premium	Regular	Basic	Premium
	Sustained Downlink Data Rate	5250 Kbps	1000 Kbps	256 Kbps	5250 Kbps	1000 Kbps	256 Kbps	2000 Kbps
	Sustained Uplink Data Rate	1750 Kbps	500 Kbps	128 Kbps	1750 Kbps	500 Kbps	128 Kbps	20000 Kbps
	Downlink and Uplink Burst Allocations	500000 Kb	80000 Kb	40000 Kb	500000 Kb	80000 Kb	40000 Kb	500000 Kb
Download (sec)	Web page	<1	<1	<1	<1	<1	<1	<1
	5 MB	8	8	8	4	4	4	4
	20 MB	32	80	470	16	80	470	16
	50 MB	80	320	1400	40	320	1400	40
	300 MB	480	2320	9220	362	2320	9220	240

23.2.2 Authentication Manager Capability

Prizm or BAM allows you to set per AP a requirement that each SM registering to the AP must authenticate. When **Authentication Required** is selected in the Security tab of the AP Configuration web page and one or more **Authentication Server** is specified by IP address, any SM that attempts to register to the AP is denied service if authentication fails, such as (but not limited to) when no Prizm or BAM server is operating or when the SM is not listed in the database.

If a Prizm or BAM server drops out of service where no redundant server exists

- an SM that attempts to register is denied service.
- an SM that is already in session remains in session

In a typical network, some SMs re-register daily (when subscribers power down the SMs, for example), and others do not re-register in a period of several weeks. Whenever an authentication attempt fails, the SM locks out of any other attempt to register itself to the same AP for the next 15 minutes.

24 MANAGING THE NETWORK FROM A MANAGEMENT STATION (NMS)

SNMPv2 (Simple Network Management Protocol Version 2) can be used to manage and monitor the modules under SMI (Structure of Management Information) specifications. SMI specifies management information definitions in ASN.1 (Abstract Syntax Notation One) language. SNMPv2 supports both 32-bit and 64-bit counters. The SMI for SNMPv2 is defined in RFC 1902 at <http://www.fags.org/rfc/rfc1902.html>.

24.1 ROLES OF HARDWARE AND SOFTWARE ELEMENTS

24.1.1 Role of the Agent

In SNMP, software on each managed device acts as the *agent*. The agent collects and stores management information in ASN.1 format, in a structure that a MIB (management information base) defines. The agent responds to commands to

- send information about the managed device.
- modify specific data on the managed device.

24.1.2 Role of the Managed Device

In SNMP, the managed device is the network element that operates on the agent software. In the fixed wireless broadband IP network, this managed device is the module (AP, SM, or BH). With the agent software, the managed device has the role of server in the context of network management.

24.1.3 Role of the NMS

In SNMP, the NMS (network management station) has the role of client. An application (manager software) operates on the NMS to manage and monitor the modules in the network through interface with the agents.

24.1.4 Dual Roles for the NMS

The NMS can simultaneously act as an agent. In such an implementation, the NMS acts as

- client to the agents in the modules, when polling for the agents for information and sending modification data to the agents.
- server to another NMS, when being polled for information gathered from the agents and receiving modification data to send to the agents.

24.1.5 Simple Network Management Protocol (SNMP) Commands

To manage a module, SNMPv2 supports the `set` command, which instructs the agent to change the data that manages the module.

To monitor a network element, SNMPv2 supports

- the `get` command, which instructs the agent to send information about the module to the manager in the NMS.
- traversal operations, which the manager uses to identify supported objects and to format information about those objects into relational tables.

In a typical network, the manager issues these commands to the agents of more than one module (to all SMs in the operator network, for example).

24.1.6 Traps from the Agent

When a specified event occurs in the module, the agent initiates a trap, for which the agent sends an unsolicited asynchronous message to the manager.

24.1.7 AP SNMP Proxy to SMs

When the AP receives from Prizm or an NMS an SNMP request for an SM, it is capable of sending that request via proxy to the SM. In this case, the SM responds directly to Prizm or the NMS. (The AP performs no processing on the response.)

24.2 MANAGEMENT INFORMATION BASE (MIB)

The MIB, the SNMP-defined data structure, is a tree of standard branches that lead to optional, non-standard positions in the data hierarchy. The MIB contains both

- objects that SNMP is allowed to control (bandwidth allocation or access, for example)
- objects that SNMP is allowed to monitor (packet transfer, bit rate, and error data, for example).

The path to each object in the MIB is unique to the object. The endpoint of the path is the object identifier.

24.2.1 Cascading Path to the MIB

The standard MIB hierarchy includes the following cascading branch structures:

- the top (standard body) level:
 - ccitt (0)
 - **iso (1)**
 - iso-ccitt (2)
- under iso (1) above:
 - standard (0)
 - registration-authority (1)
 - member-body (2)
 - **identified-organization (3)**
- under identified-organization (3) above:
 - dod (6)
 - other branches
- under dod (6) above:
 - internet (1)
 - other branches

- under internet (1) above:
 - mgmt (2)
 - private (4)
 - other branches
- under mgmt (2) above: **mib-2 (1)** and other branches. (See MIB-II below.)

under private (4) above: **enterprise (1)** and other branches. (See Canopy Enterprise MIB below.)

Beneath this level are non-standard branches that the enterprise may define.

Thus, the path to an object that is managed under MIB-II begins with the decimal string **1.3.6.1.2.1** and ends with the object identifier and instance(s), and the path to an object that is managed under the Canopy Enterprise MIB begins with **1.3.6.1.4.1**, and ends with the object identifier and instance(s).

24.2.2 Object Instances

An object in the MIB can have either only a single instance or multiple instances, as follows:

- a scalar object has only a single instance. A reference to this instance is designated by . 0, following the object identifier.
- a tabular object has multiple instances that are related to each other. Tables in the MIB associate these instances. References to these instances typically are designated by . 1, . 2, and so forth, following the object identifier.

24.2.3 Management Information Base Systems and Interface (MIB-II)

The standard MIB-II (Management Information Base systems and interface) objects are programmed into the modules. To read this MIB, see *Management Information Base for Network Management of TCP/IP-based Internets: MIB II*, RFC 1213 at <http://www.faqs.org/rfcs/rfc1213.html>.

The MIB-II standard categorizes each object as one of the types defined in [Table 65](#).

Table 65: Categories of MIB-II objects

Objects in category...	Control or identify the status of...
system	system operations in the module.
interfaces	the network interfaces for which the module is configured.
ip	Internet Protocol information in the module.
icmp	Internet Control Message Protocol information in the module. (These messages flag IP problems and allow IP links to be tested.)
tcp	Transport Control Protocol information in the module (to control and ensure the flow of data on the Internet).
udp	User Datagram Protocol information in the module (for checksum and address).

24.2.4 Canopy Enterprise MIB

The Canopy Enterprise MIB provides additional reporting and control, extending the objects for any NMS that uses SNMP interaction. This MIB comprises five text files that are formatted in standard ASN.1 (Abstract Syntax Notation One) language.

The installation tool for Prizm places this MIB into the `C:\...\PrizmInstallationDirectory\modules\mibs` directory. The Prizm server software expects to find its contents there.

To use this MIB with an NMS, perform the following steps.

Procedure 35: Installing the Canopy Enterprise MIB files

1. On the NMS, immediately beneath the `root` directory, create directory `mibviewer`.
2. Immediately beneath the `mibviewer` directory, create directory `canopymibs`.
3. Download the following three standard MIB files from the Internet Engineering Task Force at <http://www.simpleweb.org/ietf/mibs> into the `mibviewer/canopymibs` directory on the NMS:
 - `SNMPv2-SMI.txt`, which defines the Structure of Management Information specifications.
 - `SNMPv2-CONF.txt`, which allows macros to be defined for object group, notification group, module compliance, and agent capabilities.
 - `SNMPv2-TC.txt`, which defines general textual conventions.
4. Move the following files or the subset of these files from your software release package directory into the `mibviewer/canopymibs` directory on the NMS (if necessary, first download the software package from <http://motorola.wirelessbroadbandsupport.com/support> by selecting the Software Updates link on that web page:

```

CMM3-MIB.txt
CMM4-MIB.txt
Etherwan.txt
IANAifType-MIB.txt
IF-MIB.txt
ITU-ALARM-TC-MIB.txt
miblist.txt
motorola-canopy-45-mib.txt
motorola-ptp400-v2.txt
motorola-ptp500-v2.txt
motorola-ptp600-v2.txt
PRIZM-ELEMENT-MIB.txt
PRIZM-EMS-MIB.txt
PRIZM-EVENT-MIB.txt
RFC1155-SMI.txt
RFC1158-MIB.txt
RFC1213-MIB.txt
RFC-1212.txt
RFC-1215.txt
SNMPv2-CONF.txt
SNMPv2-MIB.txt
SNMPv2-SMI.txt
SNMPv2-TC.txt
WHISP-APS-MIB.txt
WHISP-BOX-MIBV2-MIB.txt
WHISP-GLOBAL-REG-MIB.txt
WHISP-PLV-GATEWAY-MIB.txt
WHISP-PLV-MIB.txt
WHISP-PLV-MODEM-MIB.txt
WHISP-SM-MIB.txt
whisp-tcv2-mib.txt

```



IMPORTANT!

Do not edit these MIB files in ASN.1. These files are intended for manipulation by only the NMS. However, you can view these files through a commercially available MIB viewer. Such viewers are listed under [MIB Viewers](#) on Page 410.

5. Download a selected MIB viewer into directory *mibviewer*.
6. As instructed by the user documentation that supports your NMS, import the eight MIB files that are listed above.

===== **end of procedure** =====

24.3 CONFIGURING MODULES FOR SNMP ACCESS

Canopy modules provide the following Configuration web page parameters in the SNMP tab. These govern SNMP access from the manager to the agent:

- **Community String**, which specifies the password for security between managers and the agent.
- **Accessing Subnet**, which specifies the subnet mask that allows managers to poll the agents.

Canopy modules can also be configured to send traps to specified IP addresses, which can be those of Prizm or NMS servers, for example. The parameter for this address is named **Trap Address**.

24.4 OBJECTS DEFINED IN THE CANOPY ENTERPRISE MIB

The Canopy Enterprise MIB defines separate sets of objects for

- all radio modules
- APs and BH timing masters
- SMs and BH timing slaves
- CMMmicros
- CMM4s



NOTE:

The PTP 300, 400, 500, and 600 series wireless Ethernet bridges do not support these objects.

24.4.1 AP, SM, and BH Objects

The objects that the Canopy Enterprise MIB defines for all APs, SMs, and BHs are listed in [Table 66](#).

Table 66: Canopy Enterprise MIB objects for APs, SMs, and BHs

AP, SM, BH Object Name	Value Syntax	Operation Allowed
addFreqList	Integer	manage
addVlanMember	Integer	manage
agingTimeout	Integer	manage
allowColocation	Integer	manage
allowVIDAccess	Integer	manage
antennaGain ¹	Integer	manage
bhModulation	Integer	manage
bhTimingMode	Integer	manage
bHvlanEnable	Integer	manage
bridgeEnable	Integer	manage
bridgeEntryTimeout	Integer	manage
changeUsrPwd	DisplayString	manage
clearEventLog	Integer	manage
codePoint ^{r2}	Integer	manage

AP, SM, BH Object Name	Value Syntax	Operation Allowed
colorCode	Integer	manage
commStringROnly	DisplayString	manage
commStringRWrite	DisplayString	manage
deleteUser	DisplayString	manage
dfsEnable ³	Integer	manage
displayOnlyAccess	DisplayString	manage
dynamicLearning	Integer	manage
eirp ³	Integer	manage
extFilterDelay	Integer	manage
fecEnable	Integer	manage
frameType	Integer	manage
fullAccess	DisplayString	manage
gpsInput	Integer	manage
hiPriority	Integer	manage
hwsCompatibility ³	Integer	manage
ism	Integer	manage
lanDhcpState	Integer	manage
linkNegoSpeed	DisplayString	manage
ILDPBroadcastEnable	Integer	manage
managementVID	Integer	manage
mngtIPn ⁵	IpAddress	manage
powerControl	Integer	manage
reboot	Integer	manage
rebootIfRequired	Integer	manage
regionCode	Integer	manage
removeFreqList	Integer	manage
removeVlanMember	Integer	manage
russiaRegion	Integer	manage
saveFlash	Integer	manage
scheduling	Integer	manage
sessionTimeout	Integer	manage
setDefaultPlug	Integer	manage
snmpMibPerm	Integer	manage
subnetMaskn ⁵	Integer	manage

AP, SM, BH Object Name	Value Syntax	Operation Allowed
taggedFrame ⁴	Integer	manage
transmitterOP	Integer	manage
trapIP ⁵	IpAddress	manage
twoXRate	Integer	manage
userAccessLevel	Integer	manage
userName	DisplayString	manage
userPassword	DisplayString	manage
vlanMemberSource	Integer	manage
webAutoUpdate	Integer	manage
accessLevel	Integer	monitor
antPolarization	DisplayString	monitor
boxDeviceType	DisplayString	monitor
boxDeviceTypeID	DisplayString	monitor
boxEncryption	DisplayString	monitor
boxFrequency	DisplayString	monitor
boxTemperature ⁶	DisplayString	monitor
dhcpLanIP	IpAddress	monitor
dhcpLanGateway	IpAddress	monitor
dhcpLanSubnetMask	IpAddress	monitor
dhcpRfPublicIP	IpAddress	monitor
dhcpRfPublicGateway	IpAddress	monitor
dhcpRfPublicSubnetMask	IpAddress	monitor
entryIndex	Integer	monitor
entryL2Index	Integer	monitor
etherLinkStatus	DisplayString	monitor
inSyncCount	Integer	monitor
lanDhcpStatus	DisplayString	monitor
neighborIndex	Integer	monitor
neighborIP	DisplayString	monitor
neighborMAC	DisplayString	monitor
neighborSiteName	DisplayString	monitor
outSyncCount	Integer	monitor
packetOverloadCounter	DisplayString	monitor
pass1Status	DisplayString	monitor

AP, SM, BH Object Name	Value Syntax	Operation Allowed
pass2Status	DisplayString	monitor
platformInfo	DisplayString	monitor
platformType	Integer	monitor
platformVer	Integer	monitor
pldVersion	DisplayString	monitor
pllOutLockCount	Integer	monitor
rfPublicDhcpStatus	DisplayString	monitor
swVersion	DisplayString	monitor
txCalFailure	Integer	monitor
userLoginName	DisplayString	monitor
userPswd	DisplayString	monitor
whispBoxBoot	DisplayString	monitor
whispBoxEsn	WhispMACAddress	monitor
whispBoxEvtLog	EventString	monitor
whispBoxFPGAVer	DisplayString	monitor
whispBoxSoftwareVer	DisplayString	monitor
whispBridgeAge	Integer	monitor
whispBridgeDesLuid	WhispLUID	monitor
whispBridgeCAM ³	Integer	monitor
whispBridgeExt	Integer	monitor
whispBridgeHash	Integer	monitor
whispBridgeMacAddr	MacAddress	monitor
whispBridgeTbErr	Integer	monitor
whispBridgeTbFree	Integer	monitor
whispBridgeTbUsed	Integer	monitor
whispVAge	Integer	monitor

AP, SM, BH Object Name	Value Syntax	Operation Allowed
whispVID	Integer	monitor
whispVType	DisplayString	monitor
<p>NOTES:</p> <ol style="list-style-type: none"> For only DFS-capable radios. Where <i>n</i> is any number, 0 through 63. codePoint0, codePoint48, and codePoint56 can be only monitored. Deprecated. Replaced by frameType. Where <i>n</i> is any number, 1 through 10. The value of this object <i>does not</i> accurately reflect the temperature inside the module for comparison with the operating range. However, it can be helpful as one of many troubleshooting indicators. Although modules no longer report the Temperature field in the GUI, the agent in the modules continues to support this object. 		

24.4.2 AP and BH Timing Master Objects

The objects that the Canopy Enterprise MIB defines for each AP and BH Timing Master are listed in [Table 67](#). The traps provided in this set of objects are listed under [Traps Provided in the Canopy Enterprise MIB](#) on [Page 410](#).

Table 67: Canopy Enterprise MIB objects for APs and BH timing masters

AP, BHM Object Name	Value Syntax	Operation Allowed
allowedIPAccess1	IpAddress	manage
allowedIPAccess2	IpAddress	manage
allowedIPAccess3	IpAddress	manage
apBeaconInfo	Integer	manage
apTwoXRate	Integer	manage
asIP1	IpAddress	manage
asIP2	IpAddress	manage
asIP3	IpAddress	manage
authKey	DisplayString	manage
authMode	Integer	manage
configSource	Integer	manage
dAcksReservHigh	Integer	manage
defaultGw	IpAddress	manage
dfsConfig ¹	Integer	manage
dwnLnkData	Integer	manage

AP, BHM Object Name	Value Syntax	Operation Allowed
dwnLnkDataRate	Integer	manage
dwnLnkLimit	Integer	manage
encryptDwBroadcast	Integer	manage
encryptionMode	Integer	manage
gpsInput	Integer	manage
gpsTrap	Integer	manage
highPriorityUpLnkPct	Integer	manage
ipAccessFilterEnable	Integer	manage
lanIp	IpAddress	manage
lanMask	IpAddress	manage
limitFreqBand900	Integer	manage
linkTestAction ²	Integer	manage
linkTestDuration	Integer	manage
linkTestLUID	Integer	manage
maxRange	Integer	manage
ntpServerIP	IpAddress	manage
numCtlSlots	Integer	manage
numCtlSlotsHW	Integer	manage
numCtlSlotsReserveHigh	Integer	manage
numDAckSlots	Integer	manage
numUAckSlots	Integer	manage
privateIp	IpAddress	manage
regTrap	Integer	manage
rfFreqCarrier	Integer	manage
rfFreqCaralt1	Integer	manage
rfFreqCaralt2	Integer	manage
scheduleWhitening	Integer	manage
sectorID	Integer	manage
sesHiDownCIR	Integer	manage
sesHiUpCIR	Integer	manage
sesLoDownCIR	Integer	manage
sesHiDownCIR	Integer	manage
smlIsolation	Integer	manage
tslBridging	Integer	manage

AP, BHM Object Name	Value Syntax	Operation Allowed
txSpreading	Integer	manage
uAcksReservHigh	Integer	manage
untranslatedArp	Integer	manage
updateAppAddress	IpAddress	manage
upLnkDataRate	Integer	manage
upLnkLimit	Integer	manage
vlanEnable	Integer	manage
actDwnFragCount	Gauge32	monitor
actDwnLinkIndex	Integer	monitor
actUpFragCount	Gauge32	monitor
actUpLinkIndex	Integer	monitor
adaptRate	DisplayString	monitor
avgPowerLevel	DisplayString	monitor
dataSlotDwn	Integer	monitor
dataSlotUp	Integer	monitor
dataSlotUpHi	Integer	monitor
dfsStatus	DisplayString	monitor
dfsStatusPrimary	DisplayString	monitor
dfsStatusAlt1	DisplayString	monitor
dfsStatusAlt2	DisplayString	monitor
downLinkEff	Integer	monitor
downLinkRate	Integer	monitor
dwnLnkAckSlot	Integer	monitor
dwnLnkAckSlotHi	Integer	monitor
expDwnFragCount	Gauge32	monitor
expUpFragCount	Gauge32	monitor
fpgaVersion	DisplayString	monitor
gpsStatus	DisplayString	monitor
lastPowerLevel	DisplayString	monitor
linkAirDelay	Integer	monitor
linkAveJitter	Integer	monitor
linkDescr	DisplayString	monitor
linkESN	PhysAddress	monitor
linkInDiscards	Counter32	monitor

AP, BHM Object Name	Value Syntax	Operation Allowed
linkInError	Counter32	monitor
linkInNUcastPkts	Counter32	monitor
linkInOctets	Counter32	monitor
linkInUcastPkts	Counter32	monitor
linkInUnknownProtos	Counter32	monitor
linkLastJitter	Integer	monitor
linkLastRSSI	Integer	monitor
linkLUID	Integer	monitor
linkMtu	Integer	monitor
linkOutDiscards	Counter32	monitor
linkOutError	Counter32	monitor
linkOutNUcastPkts	Counter32	monitor
linkOutOctets	Counter32	monitor
linkOutQLen	Gauge32	monitor
linkOutUcastPkts	Counter32	monitor
linkRegCount	Integer	monitor
linkReRegCount	Integer	monitor
linkRSSI	Integer	monitor
linkSessState	Integer	monitor
linkSiteName	DisplayString	monitor
linkSpeed	Gauge32	monitor
linkTestError	DisplayString	monitor
linkTestStatus	DisplayString	monitor
linkTimeOut	Integer	monitor
maxDwnLinkIndex	Integer	monitor
maxUpLinkIndex	Integer	monitor
numCtrSlot	Integer	monitor
numCtrSlotHi	Integer	monitor
PhysAddress	PhysAddress	monitor
radioSlicingAp ¹	Integer	monitor
radioTxGain	Integer	monitor
regCount	Integer	monitor
sesDownlinkLimit	Integer	monitor
sesDownlinkRate	Integer	monitor

AP, BHM Object Name	Value Syntax	Operation Allowed
sesUplinkLimit	Integer	monitor
sesUplinkRate	Integer	monitor
sessionCount	Integer	monitor
softwareBootVersion	DisplayString	monitor
softwareVersion	DisplayString	monitor
testDuration	Integer	monitor
testLUID	Integer	monitor
upLinkEff	Integer	monitor
upLinkRate	Integer	monitor
upLnkAckSlot	Integer	monitor
upLnkAckSlotHi	Integer	monitor
whispGPSStats	Integer	monitor
NOTES: 1. Deprecated in Release 8.2 and later. 2. You can set to 1 to initiate a link test, but not 0 to stop. The value 0 is only an indication of the idle link test state.		

24.4.3 SM and BH Timing Slave Objects

The objects that the Canopy Enterprise MIB defines for each SM and BH Timing Slave are listed in [Table 68](#).

Table 68: Canopy Enterprise MIB objects for SMs and BH timing slaves

SM, BHS Object Name	Value Syntax	Operation Allowed
allOtherIPFilter	Integer	manage
allOthersFilter	Integer	manage
allowedIPAccess1	IpAddress	manage
allowedIPAccess2	IpAddress	manage
allowedIPAccess3	IpAddress	manage
alternateDNSIP	IpAddress	manage
arpCacheTimeout	Integer	manage
arpFilter	Integer	manage
authKey	DisplayString	manage
authKeyOption	Integer	manage
bCastMIR	Integer	manage
bootpcFilter	Integer	manage

SM, BHS Object Name	Value Syntax	Operation Allowed
bootpsFilter	Integer	manage
defaultGw	IpAddress	manage
dfsConfig ¹	Integer	manage
dhcpClientEnable	Integer	manage
dhcpIPStart	IpAddress	manage
dhcpNumIPsToLease	Integer	manage
dhcpServerEnable	Integer	manage
dhcpServerLeaseTime	Integer	manage
dmzEnable	Integer	manage
dmzIP	IpAddress	manage
dnsAutomatic	Integer	manage
enable8023link	Integer	manage
ethAccessFilterEnable	Integer	manage
hiPriorityChannel	Integer	manage
hiPriorityDownlinkCIR	Integer	manage
hiPriorityUplinkCIR	Integer	manage
ingressVID	Integer	manage
ip4MultFilter	Integer	manage
ipAccessFilterEnable	Integer	manage
lanIp	IpAddress	manage
lanMask	IpAddress	manage
localIP	IpAddress	manage
lowPriorityDownlinkCIR	Integer	manage
lowPriorityUplinkCIR	Integer	manage
naptEnable	Integer	manage
naptPrivateIP	IpAddress	manage
naptPrivateSubnetMask	IpAddress	manage
naptPublicGatewayIP	IpAddress	manage
naptPublicIP	IpAddress	manage
naptPublicSubnetMask	IpAddress	manage
naptRFPublicGateway	IpAddress	manage
naptRFPublicIP	IpAddress	manage
naptRFPublicSubnetMask	IpAddress	manage
networkAccess	Integer	manage

SM, BHS Object Name	Value Syntax	Operation Allowed
port	Integer	manage
port1TCPFilter	Integer	manage
port2TCPFilter	Integer	manage
port3TCPFilter	Integer	manage
port1UDPFilter	Integer	manage
port2UDPFilter	Integer	manage
port3UDPFilter	Integer	manage
powerUpMode	Integer	manage
pppoeFilter	Integer	manage
prefferedDNSIP	IpAddress	manage
protocol	Integer	manage
radioDbmInt	Integer	manage
rfDhcpState	Integer	manage
rfScanList	DisplayString	manage
smbFilter	Integer	manage
snmpFilter	Integer	manage
tcpGarbageCollectTmout	Integer	manage
timingPulseGated	Integer	manage
twoXRate	Integer	manage
udpGarbageCollectTmout	Integer	manage
uplinkBCastFilter	Integer	manage
userDefinedPort1	Integer	manage
userDefinedPort2	Integer	manage
userDefinedPort3	Integer	manage
userP1Filter	Integer	manage
userP2Filter	Integer	manage
userP3Filter	Integer	manage
activeRegion	DisplayString	monitor
adaptRate	DisplayString	monitor
airDelay	Integer	monitor
calibrationStatus	DisplayString	monitor
dhcpcdns1	IpAddress	monitor
dhcpcdns2	IpAddress	monitor
dhcpcdns3	IpAddress	monitor

SM, BHS Object Name	Value Syntax	Operation Allowed
dhcpCip	IpAddress	monitor
dhcpClientLease	TimeTicks	monitor
dhcpCSMask	IpAddress	monitor
dhcpDfltRterIP	IpAddress	monitor
dhcpDomName	DisplayString	monitor
dhcpServerTable	DhcpServerEntry	monitor
dhcpSip	IpAddress	monitor
hostIp	IpAddress	monitor
hostLease	TimeTicks	monitor
hostMacAddress	PhysAddress	monitor
jitter	Integer	monitor
radioDbm	DisplayString	monitor
radioSlicingSm ¹	Integer	monitor
radioTxGain	Integer	monitor
radioTxPwr	DisplayString	monitor
registeredToAp	DisplayString	monitor
rssi	Integer	monitor
sessionStatus	DisplayString	monitor
NOTES:		
1. Deprecated in Release 8.2 and later.		

24.5 INTERFACE DESIGNATIONS IN SNMP

SNMP identifies the ports of the module as follows:

- Interface 1 represents the Ethernet interface of the module. To monitor the status of Interface 1 is to monitor the traffic on the Ethernet interface.
- Interface 2 represents the RF interface of the module. To monitor the status of Interface 2 is to monitor the traffic on the RF interface.

These interfaces can be viewed on the NMS through definitions that are provided in the standard MIB files.

24.6 TRAPS PROVIDED IN THE CANOPY ENTERPRISE MIB

Canopy modules provide the following SNMP traps for automatic notifications to the NMS:

- coldStart, which signals that the SNMPv2 element is reinitializing itself and that its configuration may have been altered.
- warmStart, which signals that the SNMPv2 element is reinitializing such that its configuration is unaltered.
- authenticationFailure, which signals that the SNMPv2 element has received a protocol message that is not properly authenticated (contingent on the snmpEnableAuthenTraps object setting).
- linkDown, as defined in RFC 1573
- linkUp, as defined in RFC 1573
- egpNeighborLoss, as defined in RFC 1213
- whispGPSInSync, which signals a transition from not synchronized to synchronized.
- whispGPSOutSync, which signals a transition from synchronized to not synchronized.
- whispRegComplete, which signals registration completed.
- whispRegLost, which signals registration lost.
- whispRadarDetected, which signals that the one-minute scan has been completed, radar has been detected, and the radio will shutdown.
- whispRadarEnd, which signals that the one-minute scan has been completed, radar *has not* been detected, and the radio will resume normal operation.



NOTE:

The PTP 300, 400, 500 600 series wireless Ethernet bridges do not support the traps listed above.

24.7 MIB VIEWERS

Any of several commercially available MIB viewers can facilitate management of these objects through SNMP. Some are available as open source software. Motorola does not endorse, support, or discourage the use of any these viewers.

To assist end users in this area, Motorola offers a starter guide for one of these viewers—MRTG (Multi Router Traffic Grapher). This starter guide is titled *Canopy Network Management with MRTG: Application Note*, and is available in the Document Library section under Support at <http://motorola.wirelessbroadbandsupport.com/support>. MRTG software is available at <http://mrtg.hdl.com>.

Other MIB viewers are available and/or described at the following web sites:

<http://ns3.ndgsoftware.com/Products/NetBoy30/mibbrowser.html>
<http://www.adventnet.com/products/snmputilities/>
<http://www.dart.com/samples/mib.asp>
<http://www.edge-technologies.com/webFiles/products/nvision/index.cfm>
<http://www.ipswitch.com/products/whatsup/monitoring.html>
<http://www.koshna.com/products/KMB/index.asp>
<http://www.mg-soft.si/mgMibBrowserPE.html>
<http://www.mibexplorer.com>
<http://www.netmechanica.com/mibbrowser.html>
<http://www.networkview.com>
<http://www.newfreeware.com/search.php3?q=MIB+browser>
<http://www.nudesignteam.com/walker.html>
<http://www.oidview.com/oidview.html>
<http://www.solarwinds.net/Tools>
<http://www.stargus.com/solutions/xray.html>
<http://www.totilities.com/Products/MibSurfer/MibSurfer.htm>

25 USING THE CANOPY NETWORK UPDATER TOOL (CNUT)

The Canopy Network Updater Tool (CNUT) manages and automates the software and firmware upgrade process for a Canopy radio, CMMmicro, or CMM4 (but not its 14-port switch) across the network. This eliminates the need for an administrator to visit each radio in the network (or each AP while using the Autoupdate feature) to upgrade the modules.

25.1 CNUT FUNCTIONS

The Canopy Network Updater Tool

- automatically discovers all network elements
- executes a UDP command that initiates and terminates the Autoupdate mode within APs. This command is both secure and convenient:
 - For security, the AP accepts this command from only the IP address that you specify in the Configuration page of the AP.
 - For convenience, Network Updater automatically sets this Configuration parameter in the APs to the IP address of the Network Updater server when the server performs any of the update commands.
- allows you to choose among updating
 - your entire network.
 - only elements that you select.
 - only network branches that you select.
- provides a Script Engine that you can use with any script that
 - you define.
 - Motorola supplies.

25.2 NETWORK ELEMENT GROUPS

With the Canopy Network Updater Tool, you can identify element groups composed of network elements that you select. Identifying these element groups

- organizes the display of elements (for example, by region or by AP cluster).
- allows you to
 - perform an operation on all elements in the group simultaneously.
 - set group-level defaults for telnet or ftp password access and SNMP Community String (defaults that can be overridden in an individual element when necessary).

If you have both FSK and OFDM modules in your network, then you must either ensure that they all run Release 9.4.2 or that you select these two types of modules into separate element groups because they are not running on the same software.

25.3 NETWORK LAYERS

A typical network contains multiple layers of elements, each layer lying farther from the Point of Presence. For example, SMs are behind an AP and thus, in this context, at a lower layer than the AP. Correctly portraying these layers in Network Updater is essential so that Network Updater can perform radio and AP cluster upgrades in an appropriate order.



IMPORTANT!

Correct layer information ensures that Network Updater does not command an AP that is behind another AP/SM pair (such as in a remote AP installation) to perform an upgrade at the same time as the SM that is feeding the AP. If this occurs, then the remote AP loses network connection during the upgrade (when the SM in front of the AP completes its upgrade and reboots).

25.4 SCRIPT ENGINE

Script Engine is the capability in Network Updater that executes any user-defined script against any network element or element group. This capability is useful for network management, especially for scripts that you repetitively execute across your network.

The Autodiscovery capability in Network Updater finds all of your network elements. This comprehensive discovery

- ensures that, when you intend to execute a script against *all* elements, the script is indeed executed against *all* elements.
- maintains master lists of elements (element groups) against which you selectively execute scripts.

The following scripts are included with CNUT:

- AP Data Import from BAM
- AP Data Export to BAM
- Set Autoupdate Address on APs
- Set SNMP Accessibility
- Reset Unit

25.5 SOFTWARE DEPENDENCIES FOR CNUT

CNUT functionality requires

- one of the following operating systems
 - Windows® 2000
 - Windows Server 2003
 - Windows XP
 - Red Hat Enterprise Linux Version 4
- Java™ Runtime Version 2.0 or later (installed by the CNUT installation tool)

25.6 CNUT DOWNLOAD

CNUT can be downloaded together with each system release that supports CNUT. Software for these system releases is available from <http://motorola.wirelessbroadbandsupport.com/support/> as either

- a .zip file for use without the CNUT application.
- a .pkg file that the CNUT application can open.

26 USING INFORMATIONAL TABS IN THE GUI

26.1 VIEWING GENERAL STATUS (ALL)

See

- [General Status Tab of the AP](#) on Page 206.
- [General Status Tab of the SM](#) on Page 202.
- [General Status Tab of the BHM](#) on Page 221.
- [Beginning the Test of Point-to-Point Links](#) on Page 216.

26.2 VIEWING SESSION STATUS (AP, BHM)

The Session Status tab in the Home page provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a system. This tab also includes the current active values on each SM for MIR, CIR, and VLAN, as well as the source of these values, representing the SM itself, BAM, or the AP and cap.

An example of the Session Status tab is displayed in [Figure 153](#).

General Status | **Session Status** | Remote Subscribers | Event Log | Network Interface

Home => Session Status

5.7GHz - Access Point - 0a-00-3e-f0-f1-eb

Session Status List

LUID: 002 : MAC: [0a-00-3e-f2-51-5d](#)(Lite SM) State: IN SESSION (Encrypt Active)

Site Name : No Site Name
 Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
 Software Boot Version : CANOPYBOOT 3.0
 FPGA Version : 022706 (DES Sched) P9
 Session Timeout: 0, AirDelay 4 (approximately 0.04 miles (196 feet))
 Session Count: 309, Reg Count 2097, Re-Reg Count 1918
 RSSI (Avg/Last): **2485/2449** Jitter (Avg/Last): 12/12 Power Level (Avg/Last): NAVNA
 Sustained Uplink Data Rate (BAM): 785 (kbit)
 Uplink Burst Allocation (BAM): 5000 (kbit)
 Sustained Downlink Data Rate (BAM): 5500 (kbit)
 Downlink Burst Allocation (BAM): 7000 (kbit)
 Low Priority Uplink CIR (BAM): 0 (kbps) Low Priority Downlink CIR (BAM): 0 (kbps)
 Rate : VC 18 Rate 2X1X

LUID: 003 : MAC: [0a-00-3e-f2-55-5a](#) State: IN SESSION (Encrypt Active)

Site Name : No Site Name
 Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
 Software Boot Version : CANOPYBOOT 3.0
 FPGA Version : 022706 (DES Sched) P9
 Session Timeout: 0, AirDelay 3 (approximately 0.03 miles (147 feet))
 Session Count: 1, Reg Count 1, Re-Reg Count 1
 RSSI (Avg/Last): **2596/2606** Jitter (Avg/Last): 8/3 Power Level (Avg/Last): NAVNA
 Sustained Uplink Data Rate (BAM): 785 (kbit)
 Uplink Burst Allocation (BAM): 5000 (kbit)
 Sustained Downlink Data Rate (BAM): 5500 (kbit)
 Downlink Burst Allocation (BAM): 50000 (kbit)
 Low Priority Uplink CIR (BAM): 0 (kbps) Low Priority Downlink CIR (BAM): 0 (kbps)
 Rate : VC 19 Rate 2X2X

LUID: 004 : MAC: [0a-00-3e-f2-54-08](#)(Lite SM) State: IN SESSION (Encrypt Active)

Site Name : No Site Name
 Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09

Figure 153: Session Status tab data, example

An additional example and explanations of the fields on this tab are provided in [Session Status Tab of the AP](#) on Page 196.

26.3 VIEWING REMOTE SUBSCRIBERS (AP, BHM)

See

- [Remote Subscribers Tab of the AP](#) on Page 201.
- [Continuing the Test of Point-to-Point Links](#) on Page 220.

26.4 INTERPRETING MESSAGES IN THE EVENT LOG (ALL)

Each line in the Event Log of a module Home page begins with a time and date stamp. However, some of these lines wrap as a combined result of window width, browser preferences, and line length. You may find this tab easiest to use if you widen the window until all lines are shown as beginning with the time and date stamp.

26.4.1 Time and Date Stamp

The time and date stamp reflect either

- GPS time and date directly or indirectly received from the CMM.
- the running time and date that you have set in the Time & Date web page.

NOTE:



In the Time & Date web page, if you have left any time field or date field unset and clicked the **Set Time and Date** button, then the time and date default to 00:00:00 UT : 01/01/00.

A reboot causes the preset time to pause or, in some cases, to run in reverse. Additionally, a power cycle resets the running time and date to the default 00:00:00 UT : 01/01/00. Thus, whenever either a reboot or a power cycle has occurred, you should reset the time and date in the Time & Date web page of any module that is not set to receive sync.

26.4.2 Event Log Data Collection

The collection of event data continues through reboots and power cycles. When the buffer allowance for event log data is reached, the system adds new data into the log and discards an identical amount of the oldest data.

Each line that contains the expression WatchDog flags an event that was both

- considered by the system software to have been an exception
- recorded in the *preceding* line.

Conversely, a Fatal Error() message flags an event that is recorded in the *next* line. Some exceptions and fatal errors may be significant and require either operator action or technical support.

An example portion of Event Log data is displayed in [Figure 154](#). In this figure (unlike in the Event Log web page)

- lines are alternately highlighted to show the varying length of wrapped lines.
- the types of event messages (which follow the time and date stamps and the file and line references) are underscored as quoted in [Table 69](#) and [Table 70](#).



General Status
Session Status
Remote Subscribers
Event Log
Network Interface

Home => Event Log

2.4GHz - Access Point - 0a-00-3e-20-a5-36

System Event Log

```

09:19:13 UT : 01/07/03 : File src/syslog.c : Line 568 System Log Cleared
09:28:32 UT : 01/07/03 : File box.c : Line 1185 Reboot from SNMP.
09:27:05 UT : 01/07/03 : File src/syslog.c : Line 1116 Time set
09:27:05 UT : 01/07/03 : File src/syslog.c : Line 966 System Reset Exception -- External Hard Reset WatchDog
09:27:05 UT : 01/07/03 : File src/root.c : Line 521 *****System Startup*****
09:27:05 UT : 01/07/03 : File src/root.c : Line 526 Software Version : CANOPY 8.0 (Build 17) Feb 16 2006 17:56:21 AP-DES
09:27:05 UT : 01/07/03 : File src/root.c : Line 530 Software Boot Version : CANOPYBOOT 3.0
09:27:05 UT : 01/07/03 : File src/root.c : Line 536 FPGA Version : 020206H
09:27:05 UT : 01/07/03 : File src/root.c : Line 540 FPGA Features : DES Sched
09:29:34 UT : 01/07/03 : File box.c : Line 1185 Reboot from SNMP.
09:29:25 UT : 01/07/03 : File src/syslog.c : Line 1116 Time set
09:29:25 UT : 01/07/03 : File src/syslog.c : Line 966 System Reset Exception -- External Hard Reset WatchDog
09:29:25 UT : 01/07/03 : File src/root.c : Line 521 *****System Startup*****
09:29:25 UT : 01/07/03 : File src/root.c : Line 526 Software Version : CANOPY 8.0 (Build 17) Feb 16 2006 17:56:21 AP-DES
09:29:25 UT : 01/07/03 : File src/root.c : Line 530 Software Boot Version : CANOPYBOOT 3.0
09:29:25 UT : 01/07/03 : File src/root.c : Line 536 FPGA Version : 020206H
09:29:25 UT : 01/07/03 : File src/root.c : Line 540 FPGA Features : DES Sched
09:31:31 UT : 01/07/03 : File box.c : Line 1185 Reboot from SNMP.
09:29:37 UT : 01/07/03 : File src/syslog.c : Line 1116 Time set
09:29:37 UT : 01/07/03 : File src/syslog.c : Line 966 System Reset Exception -- External Hard Reset WatchDog
09:29:37 UT : 01/07/03 : File src/root.c : Line 521 *****System Startup*****
09:29:37 UT : 01/07/03 : File src/root.c : Line 526 Software Version : CANOPY 8.0 (Build 17) Feb 16 2006 17:56:21 AP-DES
09:29:37 UT : 01/07/03 : File src/root.c : Line 530 Software Boot Version : CANOPYBOOT 3.0
09:29:37 UT : 01/07/03 : File src/root.c : Line 536 FPGA Version : 020206H
09:29:37 UT : 01/07/03 : File src/root.c : Line 540 FPGA Features : DES Sched
09:40:45 UT : 01/07/03 : File box.c : Line 1185 Reboot from SNMP.
09:39:31 UT : 01/07/03 : File src/syslog.c : Line 1116 Time set
09:39:31 UT : 01/07/03 : File src/syslog.c : Line 966 System Reset Exception -- External Hard Reset WatchDog
09:39:31 UT : 01/07/03 : File src/root.c : Line 521 *****System Startup*****
09:39:31 UT : 01/07/03 : File src/root.c : Line 526 Software Version : CANOPY 8.0 (Build 17) Feb 16 2006 17:56:21 AP-DES
09:39:31 UT : 01/07/03 : File src/root.c : Line 530 Software Boot Version : CANOPYBOOT 3.0
09:39:31 UT : 01/07/03 : File src/root.c : Line 536 FPGA Version : 020206H
09:39:31 UT : 01/07/03 : File src/root.c : Line 540 FPGA Features : DES Sched
15:22:54 UT : 01/07/03 : File box.c : Line 1185 Reboot from SNMP.
15:21:17 UT : 01/07/03 : File src/syslog.c : Line 1116 Time set
15:21:17 UT : 01/07/03 : File src/syslog.c : Line 966 System Reset Exception -- External Hard Reset WatchDog
15:21:17 UT : 01/07/03 : File src/root.c : Line 521 *****System Startup*****
15:21:17 UT : 01/07/03 : File src/root.c : Line 526 Software Version : CANOPY 8.0 (Build 17) Feb 16 2006 17:56:21 AP-DES
15:21:17 UT : 01/07/03 : File src/root.c : Line 530 Software Boot Version : CANOPYBOOT 3.0
15:21:17 UT : 01/07/03 : File src/root.c : Line 536 FPGA Version : 020206H
15:21:17 UT : 01/07/03 : File src/root.c : Line 540 FPGA Features : DES Sched
06:31:11 UT : 01/08/03 : File src/httptask.c : Line 814 Reboot from Webpage.
06:31:03 UT : 01/08/03 : File src/syslog.c : Line 1116 Time set
06:31:03 UT : 01/08/03 : File src/syslog.c : Line 966 System Reset Exception -- External Hard Reset WatchDog
06:31:03 UT : 01/08/03 : File src/root.c : Line 521 *****System Startup*****
06:31:03 UT : 01/08/03 : File src/root.c : Line 526 Software Version : CANOPY 8.0 (Build 17) Feb 16 2006 17:56:21 AP-DES
06:31:03 UT : 01/08/03 : File src/root.c : Line 530 Software Boot Version : CANOPYBOOT 3.0
06:31:03 UT : 01/08/03 : File src/root.c : Line 536 FPGA Version : 020206H
06:31:03 UT : 01/08/03 : File src/root.c : Line 540 FPGA Features : DES Sched
15:52:09 UT : 01/08/03 : File src/httptask.c : Line 814 Reboot from Webpage.
15:51:20 UT : 01/08/03 : File src/syslog.c : Line 1116 Time set
15:51:20 UT : 01/08/03 : File src/syslog.c : Line 966 System Reset Exception -- External Hard Reset WatchDog
15:51:20 UT : 01/08/03 : File src/root.c : Line 521 *****System Startup*****
15:51:20 UT : 01/08/03 : File src/root.c : Line 526 Software Version : CANOPY 8.0 (Build 17) Feb 16 2006 17:56:21 AP-DES
15:51:20 UT : 01/08/03 : File src/root.c : Line 530 Software Boot Version : CANOPYBOOT 3.0
15:51:20 UT : 01/08/03 : File src/root.c : Line 536 FPGA Version : 020206H
15:51:20 UT : 01/08/03 : File src/root.c : Line 540 FPGA Features : DES Sched

```

Figure 154: Event Log tab data, example

26.4.3 Messages that Flag Abnormal Events

The messages listed in [Table 69](#) flag abnormal events and, case by case, may signal the need for corrective action or technical support. See [Troubleshooting](#) on Page 479.

Table 69: Event Log messages for abnormal events

Event Message	Meaning
Expected LUID = 6 Actual LUID = 7	Something is interfering with the control messaging of the module. Also ensure that you are using shielded cables to minimize interference. Consider trying different frequency options to eliminate or reduce interference.
FatalError()	The event recorded on the line immediately beneath this message triggered the Fatal Error().
Loss of GPS Sync Pulse	Module has lost GPS sync signal.
Machine Check Exception	This is a symptom of a possible hardware failure. If this is a recurring message, begin the RMA process for the module.
RcvFrmNum = 0x00066d ExpFrmNum = 0x000799	Something is interfering with the control messaging of the module. Also ensure that you are using shielded cables to minimize interference. Consider trying different frequency options to eliminate or reduce interference.
System Reset Exception -- External Hard Reset	The unit lost power or was power cycled.
System Reset Exception -- External Hard Reset WatchDog	The event recorded on the preceding line triggered this WatchDog message.

26.4.4 Messages that Flag Normal Events

The messages listed in [Table 70](#) record normal events and typically *do not* signal a need for any corrective action or technical support.

Table 70: Event Log messages for normal events

Event Message	Meaning
Acquired GPS Sync Pulse.	Module has acquired GPS sync signal.
FPGA Features	Type of encryption.
FPGA Version	FPGA (JBC) version in the module.
GPS Date/Time Set	Module is now on GPS time.
PowerOn reset from Telnet command line	Reset command was issued from a telnet session.
Reboot from Webpage	Module was rebooted from management interface.
Software Boot Version	Boot version in the module.
Software Version	The software release and authentication method for the unit.
System Log Cleared	Event log was manually cleared.

26.5 VIEWING THE NETWORK INTERFACE TAB (ALL)

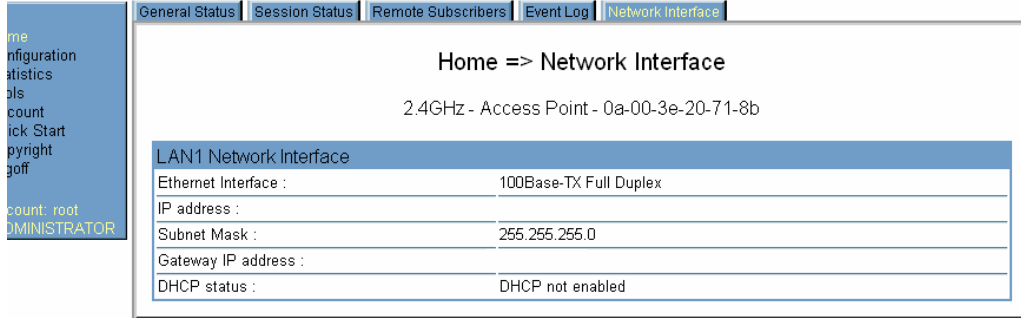


Figure 155: Network Interface tab of AP, example

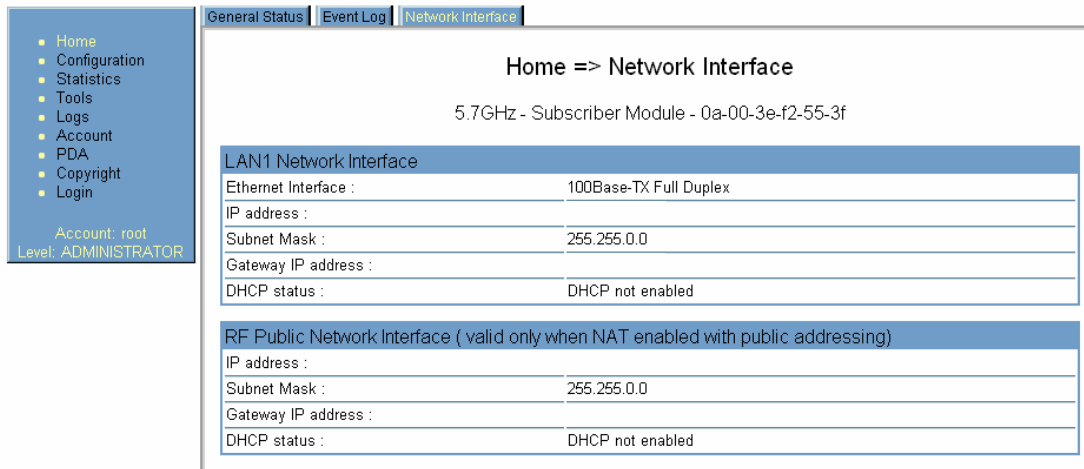


Figure 156: Network Interface tab of SM, example

In any module, the LAN1 Network Interface section of this tab displays the defined Internet Protocol scheme for the Ethernet interface to the module. In slave devices, this tab also provides an RF Public Network Interface section, which displays the Internet Protocol scheme defined for network access through the master device (AP or BHM).

26.6 VIEWING THE LAYER 2 NEIGHBORS TAB (ALL)

An example of the Layer 2 Neighbors tab is shown in [Figure 157](#).

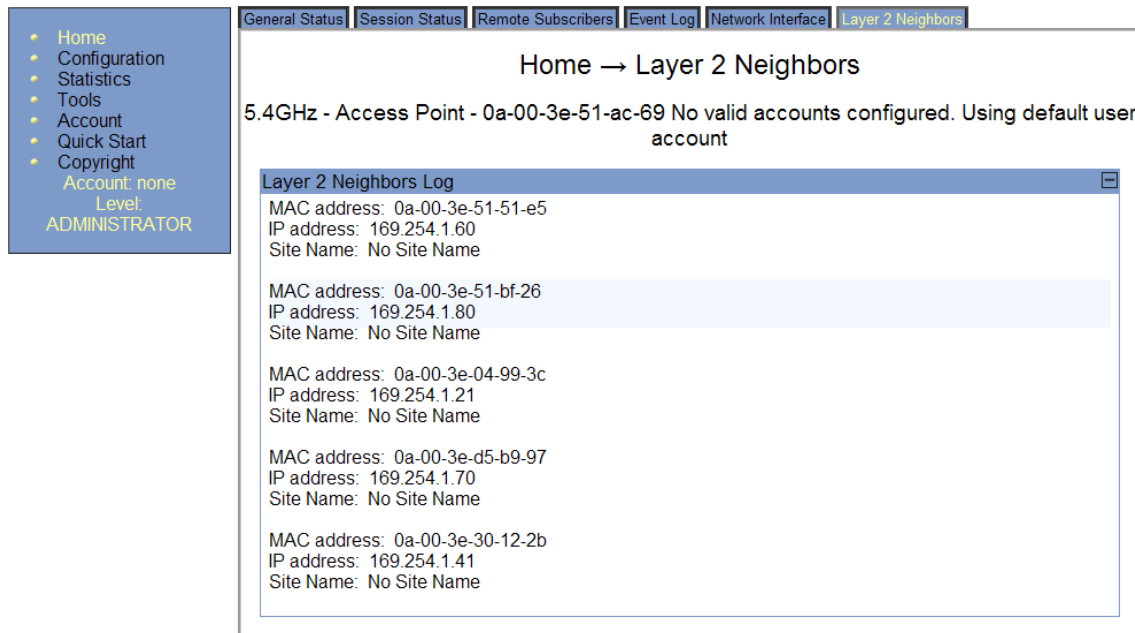


Figure 157: Layer 2 Neighbors tab, example

In the Layer 2 Neighbors tab, a module reports any device from which it has received a message in Link Layer Discovery Protocol within the previous two minutes. Given the frequency of LLDP messaging, this means that the connected device will appear in this tab 30 seconds after it is booted and remain until two minutes after its shutdown. This tab in the SM provides an efficient view of whether a connected remote AP is still discoverable by Prizm (still reporting its multicast address to the SM). See also [Multicast Destination Address](#) on Page 259.

26.7 INTERPRETING RADIO STATISTICS IN THE SCHEDULER TAB (ALL)

Statistics for the Scheduler are displayed as shown in [Figure 158](#).

The screenshot shows the Scheduler tab of the BHM interface. The left sidebar contains a navigation menu with options: Home, Configuration, Statistics (highlighted), Tools, Account, Quick Start, Copyright, Logoff, Account: admin, Level: ADMINISTRATOR. The main content area displays the following statistics:

Radio Statistics	
Transmit Unicast Data Count :	978
Transmit Broadcast Data Count :	0
Receive Unicast Data Count :	1110
Receive Broadcast Data Count :	1172
Transmit Control Count :	474
Receive Control Count :	474
In Sync Count :	0
Out of Sync Count :	0
Overrun Count :	0
Underrun Count :	0
Receive Corrupt Data Count :	0
Receive Bad Broadcast Control Count :	0
PLL Out of Lock Count :	0
Old Version Beacon Received :	0
Wrong Frequency Beacon Received :	0
Non Lite Beacon Received :	0
Unsupported Feature Beacon Received :	0
Unknown Feature Beacon Received :	0
TX Calibration Failures :	0
Bad In Sync ID Received :	0
Temperature Out of Range :	0
RSSI Out of Range :	0
Range Cap Enforced :	0
Rcv LT Start :	1
Rcv LT Start HS :	1
Rcv LT Result :	1
Xmt LT Result :	1

Figure 158: Scheduler tab of BHM, example

26.8 VIEWING THE LIST OF REGISTRATION FAILURES (AP, BHM)

An example of the SM Registration Failures tab is displayed in [Figure 159](#).

Scheduler | **SM Registration Failures** | Bridging Table | Ethernet | Radio | VLAN | Data VC

Statistics => SM Registration Failures

5.7GHz - Access Point - 0a-00-3e-f0-f1-eb

Most Recent Registration Failure List

MAC : 0a-00-3e-f0-18-87	Auth Fail	18:46:55	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	18:35:21	UT	(01/13/01)
MAC : 0a-00-3e-f0-18-87	Auth Fail	18:32:04	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	18:20:29	UT	(01/13/01)
MAC : 0a-00-3e-f0-18-87	Auth Fail	18:17:13	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	18:05:40	UT	(01/13/01)
MAC : 0a-00-3e-f0-18-87	Auth Fail	18:02:22	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	17:50:48	UT	(01/13/01)
MAC : 0a-00-3e-f0-18-87	Auth Fail	17:47:31	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	17:35:59	UT	(01/13/01)
MAC : 0a-00-3e-f0-18-87	Auth Fail	17:32:40	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	17:21:06	UT	(01/13/01)
MAC : 0a-00-3e-f0-18-87	Auth Fail	17:17:49	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	17:06:14	UT	(01/13/01)
MAC : 0a-00-3e-f0-18-87	Auth Fail	17:02:57	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	16:51:25	UT	(01/13/01)
MAC : 0a-00-3e-f0-18-87	Auth Fail	16:48:07	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	16:36:33	UT	(01/13/01)
MAC : 0a-00-3e-f0-18-87	Auth Fail	16:33:15	UT	(01/13/01)
MAC : 0a-00-3e-f0-0e-54	Auth Fail	16:21:40	UT	(01/13/01)

Account: root
Level: ADMINISTRATOR

Figure 159: SM Registration Failures tab of AP, example

The SM/BHS Registration Failures tab identifies SMs (or BHSs) that have recently attempted and failed to register to this AP (or BHM). With its time stamps, these instances may suggest that a new or transient source of interference exists.

26.9 INTERPRETING DATA IN THE BRIDGING TABLE (ALL)

An example of the Bridging Table tab is displayed in [Figure 160](#).

Screenshot of the Bridging Table tab in a network management interface. The interface shows a sidebar with navigation options like Home, Configuration, Statistics, Tools, Account, Quick Start, Copyright, and Logoff. The main content area displays "Statistics => Bridging Table" for a 5.7GHz Access Point. Below this, a table lists MAC addresses, DestLUIDs, Ages, Hashes, and Ent values for various devices. At the bottom, it shows "Used: 111 BridgeFree: 3985 BridgeFullErr: 0".

MAC Address	DestLUID	Age	Hash	Ent
Mac:0A003EF00045	DestLUID:035	Age:03	Hash:0693	Ent:01
Mac:0A003EF009A7	DestLUID:02A	Age:01	Hash:0855	Ent:02
Mac:1A003EF025DD	DestLUID:01D	Age:02*	Hash:0813	Ent:02
Mac:0A003EF2515D	DestLUID:002	Age:01	Hash:0943	Ent:02
Mac:1A003EF006D2	DestLUID:021	Age:02*	Hash:0034	Ent:02
Mac:0A003EF006D2	DestLUID:021	Age:01	Hash:0034	Ent:02
Mac:1A003EF009C1	DestLUID:032	Age:02*	Hash:0817	Ent:02
Mac:0A003EF009C1	DestLUID:032	Age:01	Hash:0817	Ent:02
Mac:0A003EF0F1E5	DestLUID:02D	Age:02	Hash:0789	Ent:02
Mac:1A003EF00162	DestLUID:038	Age:02*	Hash:0914	Ent:02
Mac:0A003EF00162	DestLUID:038	Age:01	Hash:0914	Ent:02
Mac:1A003EF25545	DestLUID:00B	Age:02*	Hash:0951	Ent:02
Mac:0A003EF25545	DestLUID:00B	Age:01	Hash:0951	Ent:02
Mac:1A003EF00C9A	DestLUID:02F	Age:02*	Hash:0618	Ent:02
Mac:0A003EF2553E	DestLUID:00A	Age:01	Hash:0972	Ent:02
Mac:1A003EF2554D	DestLUID:00E	Age:02*	Hash:0959	Ent:02
Mac:0A003EF2554D	DestLUID:00E	Age:01	Hash:0959	Ent:02
Mac:1A003EF018C5	DestLUID:03B	Age:02*	Hash:0565	Ent:02
Mac:0A003EF25462	DestLUID:006	Age:01	Hash:0656	Ent:02
Mac:0A003EF018C5	DestLUID:03B	Age:01	Hash:0565	Ent:02
Mac:3A003EF009C7	DestLUID:023	Age:01	Hash:0823	Ent:02
Mac:1A003EF01779	DestLUID:022	Age:02*	Hash:0393	Ent:02
Mac:0A003EF01779	DestLUID:022	Age:01	Hash:0393	Ent:02
Mac:1A003EF00D52	DestLUID:037	Age:02*	Hash:0930	Ent:02
Mac:0A003EF00D52	DestLUID:037	Age:01	Hash:0930	Ent:02
Mac:0A003EF009C3	DestLUID:034	Age:01	Hash:0819	Ent:02
Mac:1A003EF0F1EB	DestLUID:103	Age:-1	Hash:0795	Ent:02
Mac:0A003EF0F1EB	DestLUID:102	Age:-1	Hash:0795	Ent:02

Used: 111 BridgeFree: 3985 BridgeFullErr: 0

Figure 160: Bridging Table tab of AP, example

If NAT (network address translation) is not active on the SM, then the Bridging Table tab provides the MAC address of all devices that are attached to registered SMs (identified by LUIDs). The bridging table allows data to be sent to the correct module as follows:

- For the AP, the uplink is from RF to Ethernet. Thus, when a packet arrives in the *RF* interface to the AP, the AP reads the MAC address from the inbound packet and creates a bridging table entry of the source MAC address on the other end of the *RF* interface.
- For the SM, BHM, and BHS, the uplink is from Ethernet to RF. Thus, when a packet arrives in the *Ethernet* interface to one of these modules, the module reads the MAC address from the inbound packet and creates a bridging table entry of the source MAC address on the other end of the *Ethernet* interface.

26.10 TRANSLATION TABLE (SM)

When Translation Bridging is enabled in the AP, each SM keeps a table mapping MAC addresses of devices attached to the AP to IP addresses, as otherwise the mapping of end-user MAC addresses to IP addresses is lost. (When Translation Bridging is enabled, an AP modifies all uplink traffic originating from registered SMs such that the source MAC address of every packet will be changed to that of the SM which bridged the packet in the uplink direction.)

An example of the Translation Table is displayed in [Figure 161](#).

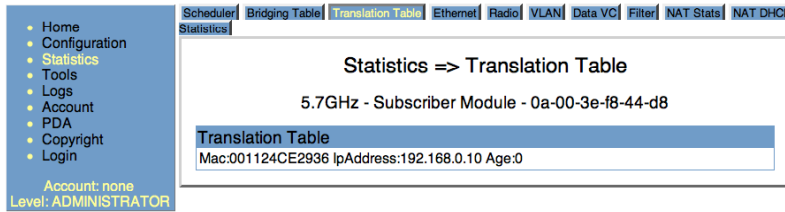


Figure 161: Translation Table tab of SM, example

26.11 INTERPRETING DATA IN THE ETHERNET TAB (ALL)

The Ethernet tab of the Statistics web page reports TCP throughput and error information for the Ethernet connection of the module.

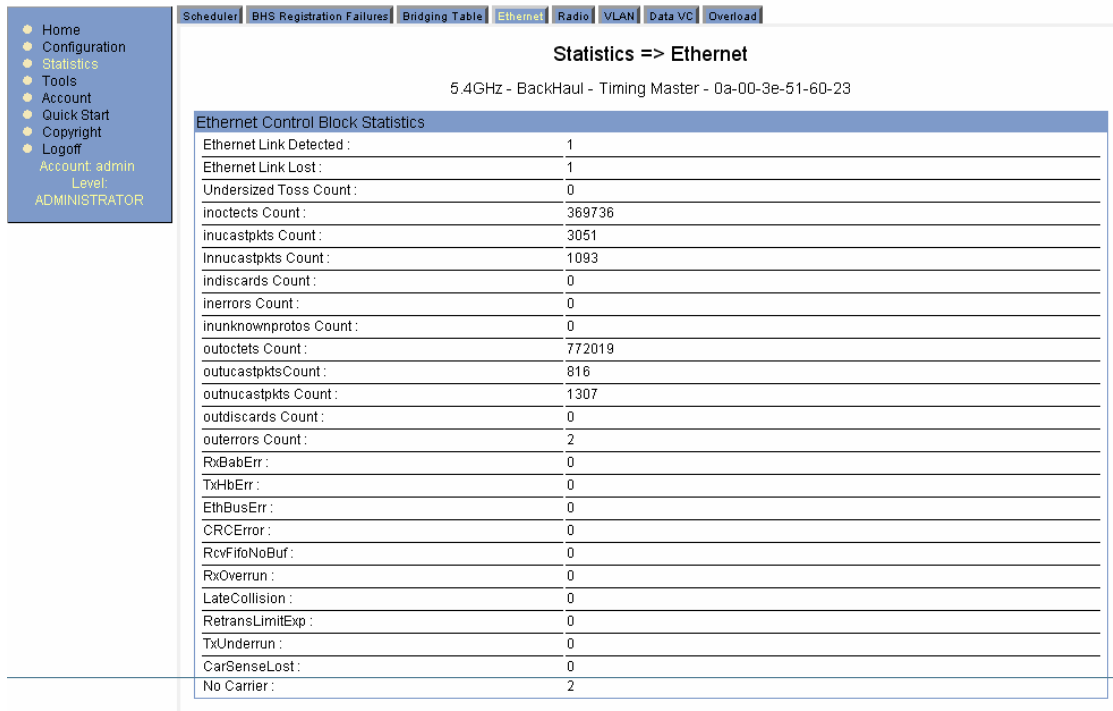


Figure 162: Ethernet tab of BHM, example

The Ethernet tab displays the following fields.

inoctets Count

This field displays how many octets were received on the interface, including those that deliver framing information.

inucastpkts Count

This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.

Innucastpkts Count

This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.

indiscards Count

This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)

inerrors Count

This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.

inunknownprotos Count

This field displays how many inbound packets were discarded because of an unknown or unsupported protocol.

outoctets Count

This field displays how many octets were transmitted out of the interface, including those that deliver framing information.

outucastpkts Count

This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.

outnucastpkts Count

This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.

outdiscards Count

This field displays how many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)

outerrors Count

This field displays how many outbound packets contained errors that prevented their transmission.

RxBabErr

This field displays how many receiver babble errors occurred.

EthBusErr

This field displays how many Ethernet bus errors occurred on the Ethernet controller.

CRCErr


This field displays how many CRC errors occurred on the Ethernet controller.

RxOverrun

This field displays how many receiver overrun errors occurred on the Ethernet controller.

Late Collision

This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision.



IMPORTANT!
 A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.

RetransLimitExp

This field displays how many times the retransmit limit has expired.

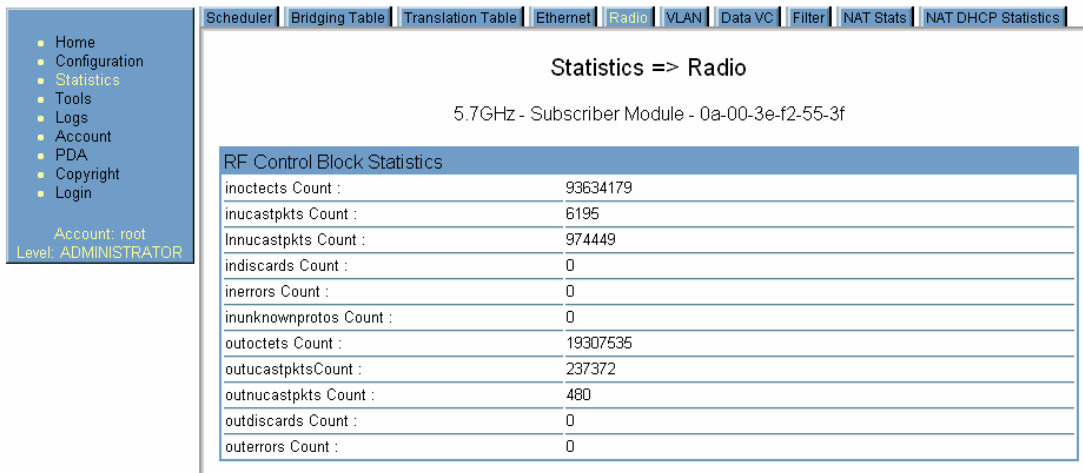
TxUnderrun

This field displays how many transmission-underrun errors occurred on the Ethernet controller.

CarSenseLost

This field displays how many carrier sense lost errors occurred on the Ethernet controller.

26.12 INTERPRETING RF CONTROL BLOCK STATISTICS IN THE RADIO TAB (ALL)



RF Control Block Statistics	
inocets Count :	93634179
inucastpkts Count :	6195
Innucastpkts Count :	974449
indiscards Count :	0
inerrors Count :	0
inunknownprotos Count :	0
outoctets Count :	19307535
outucastpktsCount :	237372
outnucastpkts Count :	480
outdiscards Count :	0
outerrors Count :	0

Figure 163: Radio tab of Statistics page in SM, example

The Radio tab of the Statistics page displays the following fields.

inocets Count

This field displays how many octets were received on the interface, including those that deliver framing information.

inucastpkts Count

This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.

Innucastpkts Count

This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.

indiscards Count

This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)

inerrors Count

This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.

inunknownprotos Count

This field displays how many inbound packets were discarded because of an unknown or unsupported protocol.

outoctets Count

This field displays how many octets were transmitted out of the interface, including those that deliver framing information.

outucastpkts Count

This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.

outnucastpkts Count

This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.

outdiscards Count

This field displays how many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)

outerrors Count

This field displays how many outbound packets contained errors that prevented their transmission.

26.13 INTERPRETING DATA IN THE VLAN TAB (ALL)

The VLAN tab in the Statistics web page provides a list of the most recent packets that were filtered because of VLAN membership violations. An example of the VLAN tab is shown in [Figure 164](#).

Figure 164: VLAN tab of AP, example

Interpret entries under **Most Recent Filtered Frames** as follows:

- **Unknown**—This should not occur. Contact Technical Support.
- **Only Tagged**—The packet was filtered because the configuration is set to accept only packets that have an 802.1Q header, and this packet did not.
- **Ingress**—When the packet entered through the wired Ethernet interface, the packet was filtered because it indicated an incorrect VLAN membership.
- **Local Ingress**—When the packet was received from the local TCP/IP stack, the packet was filtered because it indicated an incorrect VLAN membership. This should not occur. Contact Technical Support.
- **Egress**—When the packet attempted to leave through the wired Ethernet interface, the packet was filtered because it indicated an incorrect VLAN membership.
- **Local Egress**—When the packet attempted to reach the local TCP/IP stack, the packet was filtered because it indicated an incorrect VLAN membership.

26.14 DATA VC (ALL)

An example of a Data VC tab is displayed in [Figure 165](#).

Subscriber	VC	CoS	Inbound Statistics					Outbound Statistics					Queue Overflow
			in octets	in unicastpkts	in nncastpkts	in discards	in errors	out octets	out unicastpkts	out nncastpkts	out discards	out errors	
No Site Name - LUID: 002	018	00	87526	330	18	0	0	113969	436	49	0	0	0
	255	01	0	0	0	0	0	0	0	0	0	0	0

Figure 165: Data VC tab of BHM, example

The Data VC tab page displays the following fields.

VC

This field displays the virtual channel number. Low priority channels start at VC18 and count up. High priority channels start at VC255 and count down. If one VC is displayed, the high-priority channel is disabled. If two are displayed, the high-priority channel is enabled.

CoS

This field displays the Class of Service for the virtual channel. The low priority channel is a CoS of 00, and the high priority channel is a CoS of 01. CoS of 02 through 07 are not currently used.

in octets

This field displays how many octets were received on the interface, including those that deliver framing information.

in unicastpkts

This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.

in nncastpkts

This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.

in discards

This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)

in errors

This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.

outoctets

This field displays how many octets were transmitted out of the interface, including those that deliver framing information.

outucastpkts

This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.

outnucastpkts

This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.

outdiscards

This field displays how many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)

outerrors

This field displays how many outbound packets contained errors that prevented their transmission.

Queue Overflow

This is a count of packets that were discarded because the queue for the VC was already full.

26.15 VIEWING SUMMARY INFORMATION IN THE OVERLOAD TAB (ALL)

The Overload tab displays statistics on packet overload and resultant packet discards. An example of the Overload tab is shown in [Figure 166](#).

Packet Overload Statistics	
Total Packets Overload Count:	0
Ethernet In Discards:	0
Ethernet Out Discards (Statistics=>Ethernet=>outdiscards count):	0
RF In Discards (Sum of all VCs of: Statistics=>Data VC=>indiscards count):	0
RF Out Discards (Statistics=>Radio=>outdiscards count):	0

Figure 166: Overload tab of BHM, example

Unlike the other fields, the **Total Packets Overload Count** is expressed in only this tab. It is not a count of how many packets have been lost, but rather of how many discard events (packet loss bursts) have been detected.

26.16 FILTER (SM, BHS)

The Filter tab displays statistics on packets that have been filtered (dropped) due to the filters set on the Protocol Filtering tab. An example of the Filter tab is shown in [Figure 167](#).

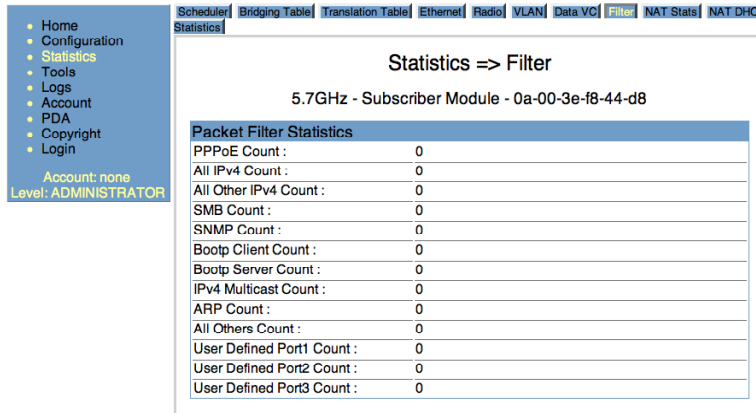


Figure 167: Filter tab of SM, example

26.17 ARP (SM, BHS)

The ARP tab in a slave module correlated the IP address of the Ethernet-connected device to its MAC address and provides data about the connection. An example of an ARP tab is shown in [Figure 168](#).

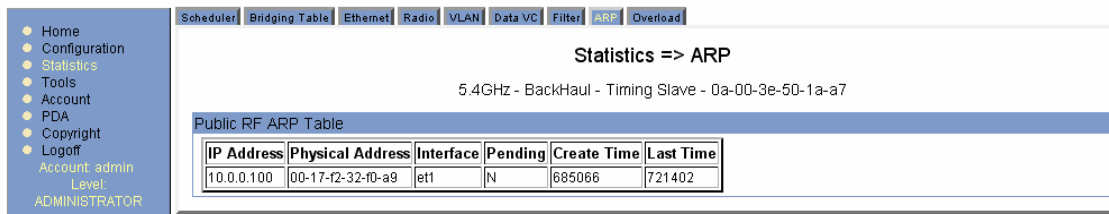


Figure 168: ARP tab of BHS, example

26.18 NAT STATS (SM)

When NAT is enabled on an SM, statistics are kept on the Public and Private (WAN and LAN) sides of the NAT, and displayed on the NAT Stats tab. An example of the NAT Stats tab is shown in [Figure 169](#).

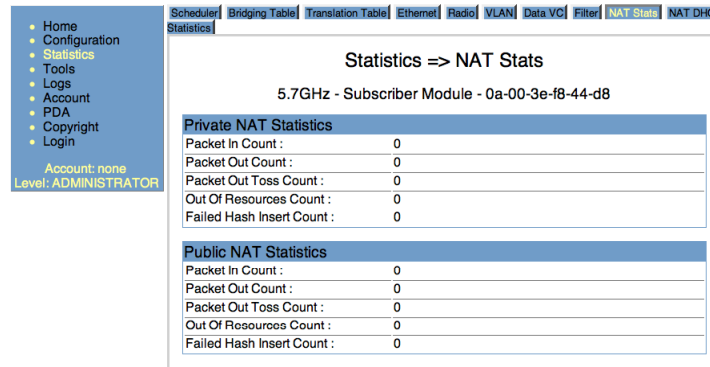


Figure 169: Nat Stats tab of SM, example

26.18.1 NAT DHCP Statistics (SM)

When NAT is enabled on an SM with DHCP client (**DHCP** selected as the **Connection Type** of the WAN interface) and/or DHCP Server, statistics are kept for packets transmitted, received, and tossed, as well as a table of lease information for the DHCP server (Assigned IP Address, Hardware Address, and Lease Remained/State). An example of the NAT DHCP Statistics tab is shown in Figure 170.

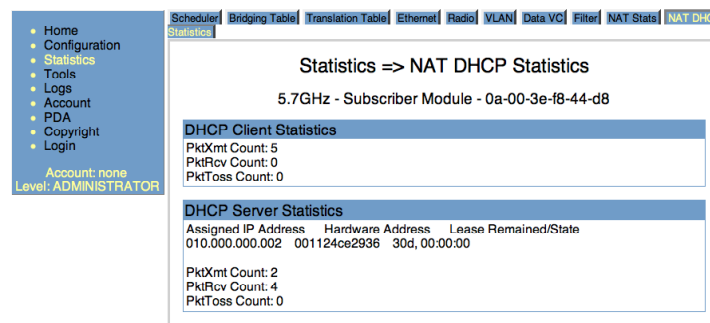



Figure 170: NAT DHCP Statistics tab of SM, example

26.18.2 Interpreting Data in the GPS Status Page (AP, BHM)

The GPS Status tab is only displayed when the Sync Input is set to Sync to Received Signal (Timing Port), which is the configuration desired when connecting an AP or BHM to a CMM2. See [Sync Input](#) on Page 228.

The page displays information similar to that available on the web pages of a CMM, including Pulse Status, GPS Time and Date, Satellites Tracked, Available Satellites, Height, Latitude, and Longitude. This page also displays the state of the antenna in the **Antenna Connection** field as

- **Unknown**—Shown for early CMM2s.
- **OK**—Shown for later CMM2s where no problem is detected in the signal.
- **Overcurrent**—Indicates a coax cable or connector problem.
- **Undercurrent**—Indicates a coax cable or connector problem.



IMPORTANT!
 If **Unknown** is displayed where a later CMM2 is deployed, then the connection is not working but the reason is unknown.

This information may be helpful in a decision of whether to climb a tower to diagnose a perceived antenna problem.

26.19 ACCESSING PPPOE STATISTICS ABOUT CUSTOMER ACTIVITIES (SM)

When the PPPoE feature has been enabled in the SM (see [PPPoE Tab of the SM](#) on Page 289), the PPPoE statistics provide data about the activities of the customer. An example of the PPPoE tab in the SM is displayed in [Figure 171](#).

- Home
- Configuration
- Statistics
- Tools
- Logs
- Account
- PDA
- Copyright
- Logoff
- Account: admin
- Level: ADMINISTRATOR

Scheduler
Bridging Table
Translation Table
Ethernet
Radio
VLAN
Data VC
Filter
NAT Stats
NAT DHCP
ARP
Overload
PPPoE Statistics

Statistics => PPPoE Statistics

5.4GHz - Subscriber Module - 0a-00-3e-52-14-8b

PPPoE Statistics	
IP address :	0.0.0.0
PPPoE Session Status :	Out Of Session
PPPoE AC Name :	
PPPoE Service Name :	
PPPoE Session ID :	0
PPPoE Session Uptime :	00:00:00
PPPoE Session Idle Time :	00:00:00
PPPoE Session MTU :	1492
Primary DNS Address :	0.0.0.0
Secondary DNS Address :	0.0.0.0
PPPoE Control Bytes Sent :	0
PPPoE Control Bytes Received :	0
PPPoE Data Session Bytes Sent :	0
PPPoE Data Session Bytes Received :	0

Figure 171: PPPoE tab of SM, example

27 USING TOOLS IN THE GUI

27.1 USING THE SPECTRUM ANALYZER TOOL (SM, BHS)

See [Monitoring the RF Environment](#) on Page 373.

27.2 USING THE ALIGNMENT TOOL (SM, BHS)

An example of the Alignment Tool tab in an SM or BHS is displayed in [Figure 172](#).

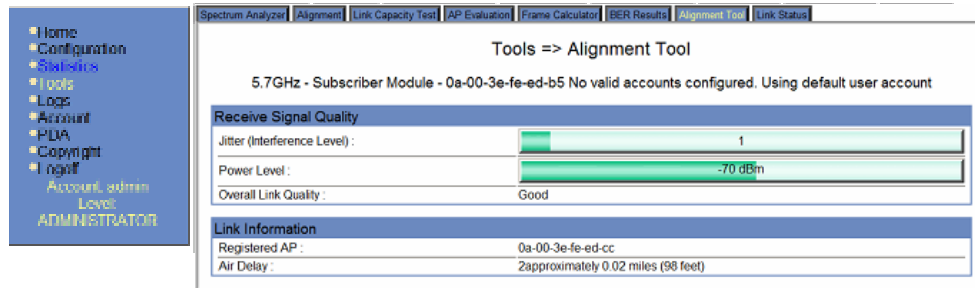


Figure 172: Alignment Tool tab of SM, example for a good link

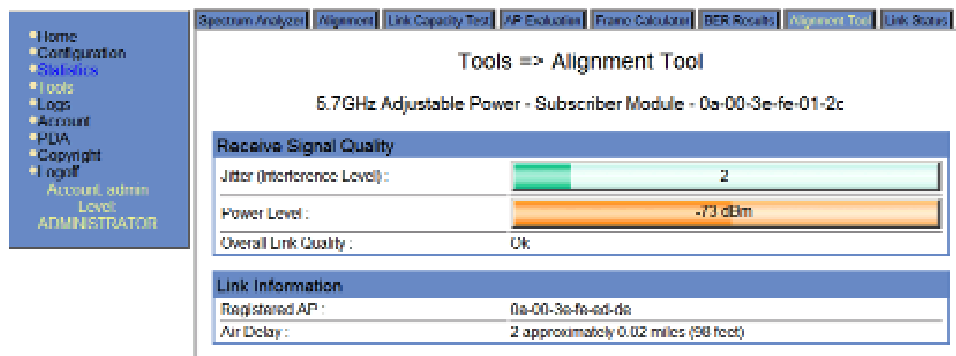


Figure 173: Alignment Tool tab of SM, example for an acceptable link

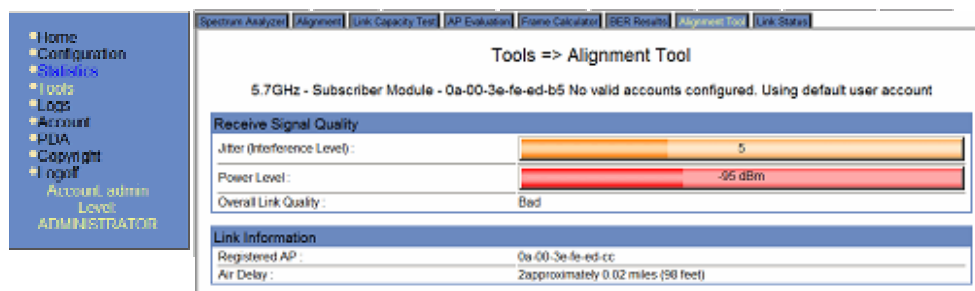



Figure 174: Alignment Tool tab of SM, example for an unacceptable link

Proper alignment must achieve all of the following indications for an acceptable link between the modules:

- power level of not less than -75dBm
- jitter value between 0 and 4
- uplink and downlink efficiency greater than 90%, except as described under [Comparing Efficiency in 1X Operation to Efficiency in 2X Operation](#) on Page 136.



IMPORTANT!

If any of these values is not achieved, a link can be established but will manifest occasional problems.

The relationship between Air Delay and link quality is described under [AP-SM Links](#) on Page 101.

27.3 USING THE LINK CAPACITY TEST TOOL (ALL)

Examples of Link Capacity Test tabs are displayed in [Figure 175](#) and [Figure 176](#).

- Home
- Configuration
- Statistics
- Tools
- Account
- Quick Start
- Copyright
- Logoff
- Account: admin
- Level: ADMINISTRATOR

Link Capacity Test
Frame Calculator
DFS

Tools => Link Capacity Test

5.4GHZ - BackHaul - Timing Master - 0a-00-3e-51-60-23

Link Test Settings

Duration :	<input type="text" value="2"/> Seconds (2 - 10)
Number of Packets :	<input type="text" value="0"/> (0 - 64) Zero will flood the link for duration of test
Packet Length :	<input type="text" value="1522"/> Bytes (64 - 1522)

Current Results Status

Stats for LUID: 2 Test Duration: 2 Pkt Length: 1522

Downlink RATE: 7344640 bps
 Uplink RATE: 8947840 bps
 Aggregate RATE: 14292480 bps
 Pkt Xmt (Act/Exp): 2396/0
 Pkt Rcv (Act/Exp): 2260/0

Downlink Efficiency: 100 Percent
 Downlink Index (Act/Max): 100/100
 Frag Count (Act/Exp): 28690/28690

Uplink Efficiency: 100 Percent
 Uplink Index (Act/Max): 100/100
 Frag Count (Act/Exp): 27140/27140

Figure 175: Link Capacity Test tab of BHM, example

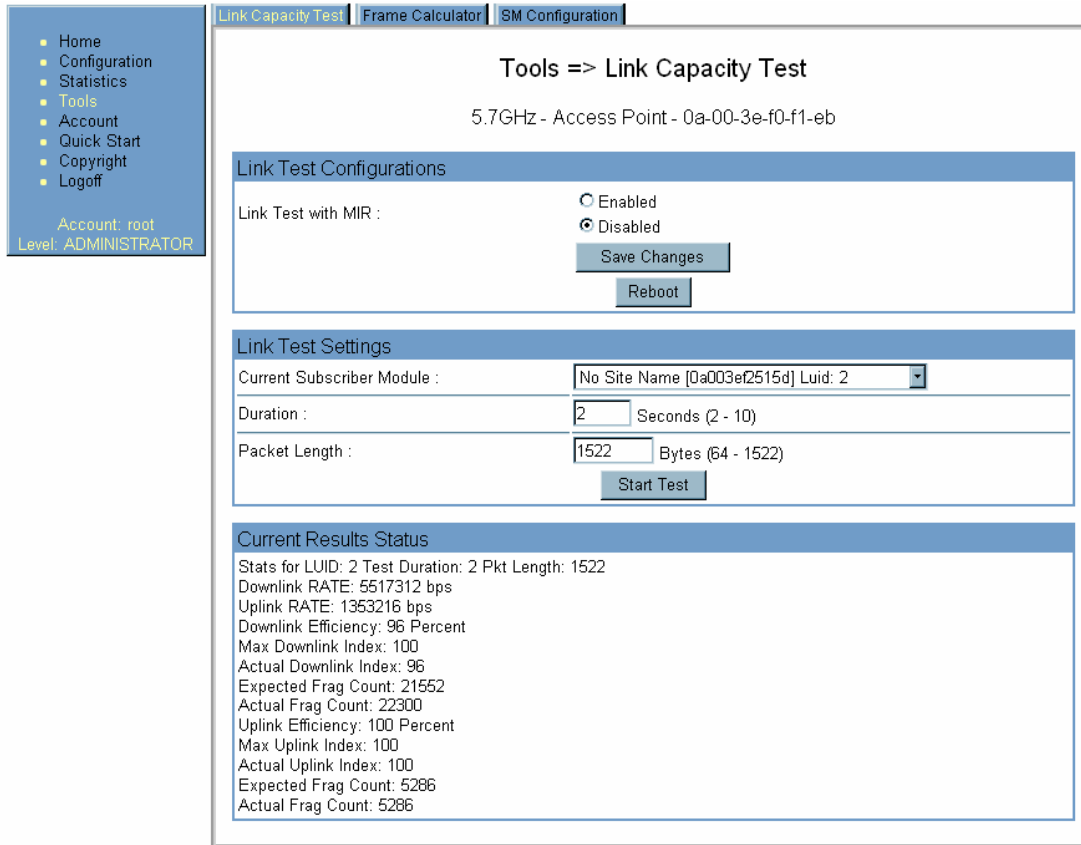


Figure 176: Link Capacity Test tab with 1522-byte packet length, example

The Link Capacity Test page allows you to measure the throughput and efficiency of the RF link between two modules. Many factors, including packet length, affect throughput. The Link Capacity Test tab contains the settable parameter **Packet Length** with a range of 64 to 1522 bytes. This allows you to compare throughput levels that result from various packet sizes.

For example, the same link was measured in the same time frame at a packet length of 64 bytes. The results are shown in [Figure 177](#).

Link Capacity Test | Frame Calculator | SM Configuration

Tools => Link Capacity Test

5.7GHz - Access Point - 0a-00-3e-f0-f1-eb

Link Test Configurations

Link Test with MIR : Enabled
 Disabled

Save Changes

Reboot

Link Test Settings

Current Subscriber Module : No Site Name [0a003ef2515d] Luid: 2

Duration : 2 Seconds (2 - 10)

Packet Length : 64 Bytes (64 - 1522)

Start Test

Current Results Status

Stats for LUID: 2 Test Duration: 2 Pkt Length: 64

Downlink RATE: 1292268 bps
 Uplink RATE: 618752 bps
 Downlink Efficiency: 78 Percent
 Max Downlink Index: 100
 Actual Downlink Index: 78
 Expected Frag Count: 5048
 Actual Frag Count: 6400
 Uplink Efficiency: 84 Percent
 Max Uplink Index: 100
 Actual Uplink Index: 84
 Expected Frag Count: 2417
 Actual Frag Count: 2845

Account: root
Level: ADMINISTRATOR

Figure 177: Link Capacity Test tab with 64-byte packet length, example

To test a link, perform the following steps.

Procedure 36: Performing a Link Capacity Test

1. Access the Link Capacity Test tab in the Tools web page of the module.
2. If you are running this test from an AP
 - a. and you want to see Maximum Information Rate (MIR) data for the SM whose link you will be testing, then perform the following steps:
 - (1) For **Link Test with MIR**, select **Enabled**.
 - (2) Click the **Save Changes** button.
 - (3) Click the **Reboot** button.
 - (4) Similarly, set the **Link Test with MIR** parameter in the SM to **Enabled**.
NOTE: If this parameter is enabled on one end of the link and disabled on the other, the results are misleading.
 - b. use the drop-down list to select the SM whose link you want to test.
3. Type into the **Duration** field how long (in seconds) the RF link should be tested.
4. Type into the **Packet Length** field the packet length at which you want the test conducted.

5. Type into the **Number of Packets** field either
 - the number of packets (1 to 64) for the test.
 - **0** to flood the link for as long as the test is in progress.
6. Click the **Start Test** button.
7. In the Current Results Status block of this tab, view the results of the test.
8. Optionally
 - a. change the packet length.
 - b. repeat Steps 5 and 6.
 - c. compare the results to those of other tests.
9. If you are finished with the link tests, and if you had **Link Test with MIR** enabled on both ends, disable it on both ends.
NOTE: This safeguards against leaving it enabled on one and not the other.

===== **end of procedure** =====

The key fields in the test results are

- **Downlink RATE** and **Uplink RATE**, expressed in bits per second
- **Downlink Efficiency** and **Uplink Efficiency**, expressed as a percentage

A link is acceptable only if the efficiencies of the link test are greater than 90% in both the uplink and downlink direction, except during 2X or 3X operation. See [Using Link Efficiency to Check FSK Received Signal Quality](#) on Page 136. Whenever you install a new link, execute a link test to ensure that the efficiencies are within recommended guidelines.

The AP downlink data percentage, slot settings, other traffic in the sector, and the quality of the RF environment all affect throughput. However, a Maximum Information Rate (MIR) throttle or cap on the SM does not affect throughput.

27.4 USING THE AP EVALUATION OR BHM EVALUATION TOOL (SM, BHS)

The AP Evaluation tab in the Tools web page of the SM provides information about the AP that the SM sees. Similarly, the BHM Evaluation tab of the BHS provides information about the BHM. An example of the AP Evaluation tab is shown in [Figure 178](#).



NOTE:

The data for this page can be suppressed by the **SM Display of AP Evaluation Data** selection in the Security tab of the Configuration page in the AP.

Figure 178: AP Evaluation tab of SM, example

The AP Evaluation tab provides the following fields that can be useful to manage and troubleshoot a system:

Index

This field displays the index value that the system assigns (for only this page) to the AP where this SM is registered (or to the BHM to which this BHS is registered).

Frequency

This field displays the frequency that the AP or BHM transmits.

ESN

This field displays the MAC address (electronic serial number) of the AP or BHM. For operator convenience during SM or BHS aiming, this tab retains each detected ESN for up to 15 minutes. If the broadcast frequency of a detected AP or BHM changes during a 15-minute interval in the aiming operation, then a multiple instance of the same ESN is possible in the list. Eventually, the earlier instance expires and disappears, and the later instance remains to the end of its interval, but you can ignore the early instance(s) whenever two or more are present.

Region

Where the DFS feature is enabled, the following information follows the ESN:

- Region Code name
- Region Code numeric value
- corresponding Country Code numeric value

These are shown in the following line:

```
Index: 0 Frequency: 5560.00 MHz ESN: 0a-00-3e-51-60-23 Europe (RC: 3 CC: 1)
```

Jitter, RSSI, and Power Level

The AP Evaluation tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm. For example, if coarse alignment gives an SM a power level of -75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to -78 dBm and the jitter to 2 or 3, use the refined alignment, with the following caveats:

- When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
- When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

OFDM modules do not have this parameter. For historical relevance, the AP Evaluation tab also shows the **RSSI**, the unitless measure of power. Use **Power Level** and ignore **RSSI**. **RSSI** implies more accuracy and precision than is inherent in its measurement.



NOTE:

Unless the page is set to auto-refresh, the values displayed are from the instant the General Status tab was selected. To keep a current view of the values, refresh the browser screen or set to auto-refresh.

Beacon Count

A count of the beacons seen in a given time period.

FEC

This field contains the SNMP value from the AP that indicates whether the Forward Error Correction feature is enabled. PMP 400 Series OFDM APs do not have this field.

Type

Multipoint indicates an AP, not a BHM.

Age

This is a counter for the number of minutes that the AP has been inactive. At 15 minutes of inactivity for the AP, this field is removed from the AP Eval tab in the SM.

Lockout

This field displays how many times the SM or BHS has been temporarily locked out of making registration attempts.

RegFail

This field displays how many registration attempts by this SM or BHS failed.

Range

This field displays the distance in feet for this link. To derive the distance in meters, multiply the value of this parameter by 0.3048.

TxBER

A 1 in this field indicates the AP or BHM is sending Radio BER.

EBcast

A 1 in this field indicates the AP or BHM is encrypting broadcast packets. A 0 indicates it is not.

Session Count

This field displays how many sessions the SM (or BHS) has had with the AP (or BHM). Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum.

In the case of a multipoint link, if the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem or an interference problem.

NoLUIDs

This field indicates how many times the AP has needed to reject a registration request from an SM because its capacity to make LUID assignments is full. This then locks the SM out of making any valid attempt for the next 15 minutes. It is extremely unlikely that a non-zero number would be displayed here.

OutOfRange

This field indicates how many times the AP has rejected a registration request from an SM because the SM is a further distance away than the range that is currently configured in the AP. This then locks the SM out of making any valid attempt for the next 15 minutes.

AuthFail

This field displays how many times authentication attempts from this SM have failed in the AP.

EncryptFail

This field displays how many times an encryption mismatch has occurred between the SM and the AP.

Rescan Req

This field displays how many times a re-range request has occurred for the BHM that is being evaluated in the AP Eval page of a BHS.

FrameNumber

This field displays the number from the tag applied by the FPGA to the last previous beacon frame. After the SM registers and is put into session with the AP, the value of this field is no longer kept up to date.

Sector ID

This field displays the value of the **Sector ID** field that is provisioned for the AP or BHM.

Color Code

This field displays the value of the **Color Code** field that is provisioned for the AP or BHM.

BeaconVersion

This field indicates whether the beacon is OFDM (value of 0) or FSK (value of 1).

Sector User Count

This field displays how many SMs are registered on the AP.

Frequency

This field displays the frequency of the received signal, expressed in MHz.

NumULHalfSlots

This is the number of uplink half slots in the frame for this AP or BHM. To find the number of slots, divide by 2.

NumDLHalfSlots

This is the number of downlink half slots in the frame for this AP or BHM. To find the number of slots, divide by 2.

NumULContSlots

This field displays how many control slots are being used in the uplink portion of the frame.

The AP Evaluation tab also provides the following buttons.

WhiteSched

This field numerically indicates whether the **Schedule Whitening** feature is enabled. See [Schedule Whitening](#) on Page 236. OFDM modules do not have this field.

PtoP VLAN

This field indicates whether VLAN is supported in the backhaul module.

Rescan APs or BHM

You can click this button to force the SM or BHS to rescan the frequencies that are selected in the Radio tab of the Configuration page. (See [Custom Radio Frequency Scan Selection List](#) on Page 271.) This module will then register to the AP or BHM that provides the best results for power level, jitter, and—in an SM—the number of registered SMs.

Update Display

You can click this button to gather updated data without causing the SM or BHS to rescan and re-register.

27.5 USING THE FRAME CALCULATOR TOOL (ALL) FOR COLLOCATION

The first step to avoid interference is to set all APs to receive timing from CMMs. This ensuring they are in sync and start transmitting at the same time each frame.

The second step to avoid interference is to configure parameters on all APs of the same frequency band in proximity such that they have compatible transmit/receive ratios (all stop transmitting each frame before any start receiving). This avoids the problem of one AP attempting to receive the signal from a distant SM while a nearby AP transmits, which could overpower that signal.

The following parameters on the AP determine the transmit/receive ratio:

- **Max Range**
- **Downlink Data** percentage
- (reserved) **Control Slots**

If all the APs of a given frequency band are FSK APs or all are OFDM APs, the simplest way to avoid interference is to set these three parameters with identical values on all APs in proximity. If OFDM and FSK APs of the same frequency band are in proximity, or if you want APs set to different parameters (differing in their Max Range values, for example), then you should use the Frame Calculator to identify compatible settings.

The frame calculator is available on the Frame Calculator tab of the Tools web page. To use the Frame Calculator, type into the calculator various configurable parameter values for each proximal AP, and then record the resulting **Uplink Rcv SQ Start** value. Next vary the **Downlink Data** percentage in each calculation and iterate until the calculated **Uplink Rcv SQ Start** for all collocated APs are within 300 bit times; if possible, within 150 bit times.

OFDM modules provide an OFDM Frame Calculator and FSK modules provide an FSK Frame Calculator. To perform frame calculations for collocated OFDM and FSK modules, you must use an OFDM module for the OFDM calculations and an FSK module for the FSK calculations.

The calculator *does not* use values in the module or populate its parameters. It is merely a convenience application that runs on a module. For this reason, you can use any FSK module (AP, SM, BHM, BHS) to perform FSK frame calculations for setting the parameters on an FSK AP and any OFDM module (AP, SM, BHM, BHS) to perform OFDM frame calculations for setting the parameters on an OFDM AP.



IMPORTANT!

APs that have slightly mismatched transmit-to-receive ratios and low levels of data traffic may see little effect on throughput. A system that was not tuned for collocation may work fine at low traffic levels, but encounter problems at higher traffic levels. The conservative practice is to tune for collocation before traffic ultimately increases. This prevents problems that occur as sectors are built.

An example of the Frame Calculator tab is shown in [Figure 179](#).

Tools => Frame Calculator

5.4GHz - BackHaul - Timing Master - 0a-00-3e-51-60-23

Frame Calculator Parameters

Software Version Transmitter :	CANDPY7.2-Current
Software Version Receiver :	CANDPY7.2-Current
Transmit Sync Input :	Generate Sync Signal
Link Mode :	<input type="radio"/> Point-To-Point Link <input checked="" type="radio"/> Multipoint Link
AES, 2X Rate, Encryption Enabled :	<input checked="" type="radio"/> True <input type="radio"/> False
Max Range :	2 Miles (Range: 1- 30 miles)
Air Delay :	0 bits
Scheduling :	<input checked="" type="radio"/> Hardware <input type="radio"/> Software
Mobility :	<input type="radio"/> On <input checked="" type="radio"/> Off
Wireless/Wired :	<input checked="" type="radio"/> Wireless Link <input type="radio"/> Wired Link
Platform Type Transmitter :	P10
Platform Type Receiver :	P10
Frequency Band :	5.4GHz
External Bus Frequency Transmitter :	40
External Bus Frequency Receiver :	40
Downlink Data :	75 %
Control Half Slots :	3 (Range: 0--10)

Apply Settings

Calculate

Calculated Frame Results

Invalid Configuration

Figure 179: Frame Calculator tab, example

In the Frame Calculator tab, you may set the following parameters.

Software Version Transmitter

From the drop-down menu, select the software release that runs on the AP(s).

Software Version Receiver

From the drop-down menu, select the software release that runs on the SM(s).

Transmit Sync Input

If the APs in the cluster

- receive sync from a CMMmicro or CMM4, select **Sync to Received Signal (Power Port)**.
- receive sync from a CMM2, select **Sync to Received Signal (Timing Port)**.
- are self timed, select **Generate Sync Signal**.

Link Mode

For AP to SM frame calculations, select **Multipoint Link**.

AES, 2X Rate, Encryption Enabled

This value is not settable by the operator.

Max Range

Set to the same value as the **Max Range** parameter is set in the AP(s).

Air Delay

Leave this parameter set to the default value of 0 bits.

Scheduling

Select **Hardware**.

Mobility

Leave the default value of **Off** selected.

Wireless/Wired

Leave the default value of **Wireless Link** selected.

Platform Type Transmitter

Use the drop-down list to select the hardware series (board type) of the AP.

Platform Type Receiver

Use the drop-down list to select the hardware series (board type) of the SM.

Frequency Band

Use the drop-down list to select the radio frequency band of the AP and SM.

External Bus Frequency Transmitter

Leave this parameter set to the default value of 40.

External Bus Frequency Receiver

Leave this parameter set to the default value of 40.

Downlink Data

Initially set this parameter to the same value that the AP has for its **Downlink Data** parameter (percentage). Then, as you use the Frame Calculator tool in [Procedure 37](#), you will vary the value in this parameter to find the proper value to write into the **Downlink Data** parameter of all APs in the cluster.

PMP 100 Series APs offer a range of 1% to 99%, and default to 75%. PMP 400 Series APs offer a range of 1% to 90%, and default to 75%. The value that you set in this parameter has the following interaction with the value of the **Max Range** parameter (above):

- The default **Max Range** value is 5 miles and, at that distance, the maximum **Downlink Data** value (90% in OFDM) is functional.
- Where **Max Range** is set to 6 to 10 miles, **Downlink Data** should be set to not greater than 85%. This lesser maximum avoids registration problems for nearby SMs. The user interface of the OFDM AP automatically imposes the lesser maximum.

Control Half Slots

Set this parameter to the value of the **Control Slot** parameter is set in the APs. Since control slots are half the size of data slots, they are sometimes called half slots.

Control Slots in the Configuration > Radio tab or Home > General Status tab of the AP are the same as **Control Half Slots** in the Tools > Frame Calculator tab.

The Calculated Frame Results display several items of interest.

Data Slots (Down/UpLow/UpHigh)

A result within the typical range is 57/19/0, meaning 59 half slots down and 19 half slots up (the 0 is an artifact from software scheduling). The same configuration would be shown on the Home > General Status tab **Frame Configuration Information** field as 28+ data slots down and 9+ data slots up. (The + indicates there are additional bit times that can be used for control (half) slots, but not enough bit times for a full data slot.)

Air Delay

This is the roundtrip air delay in bit times for the **Max Range** value set in the calculator.

Uplink Rcv SQ Start

In bit times, this is the frame position at which the AP is ready to receive transmissions from the SM.

To use the Frame Calculator, perform the following steps.

Procedure 37: Using the Frame Calculator

1. Use a module of the technology type (FSK or OFDM) of the first AP.
2. Populate the FSK or OFDM Frame Calculator parameters with appropriate values as described above.
3. Click the **Apply Settings** button.
4. Click the **Calculate** button.
5. Scroll down the tab to the Calculated Frame Results section.

NOTE: An example of the Calculated Frame Results section is displayed in [Figure 180](#).

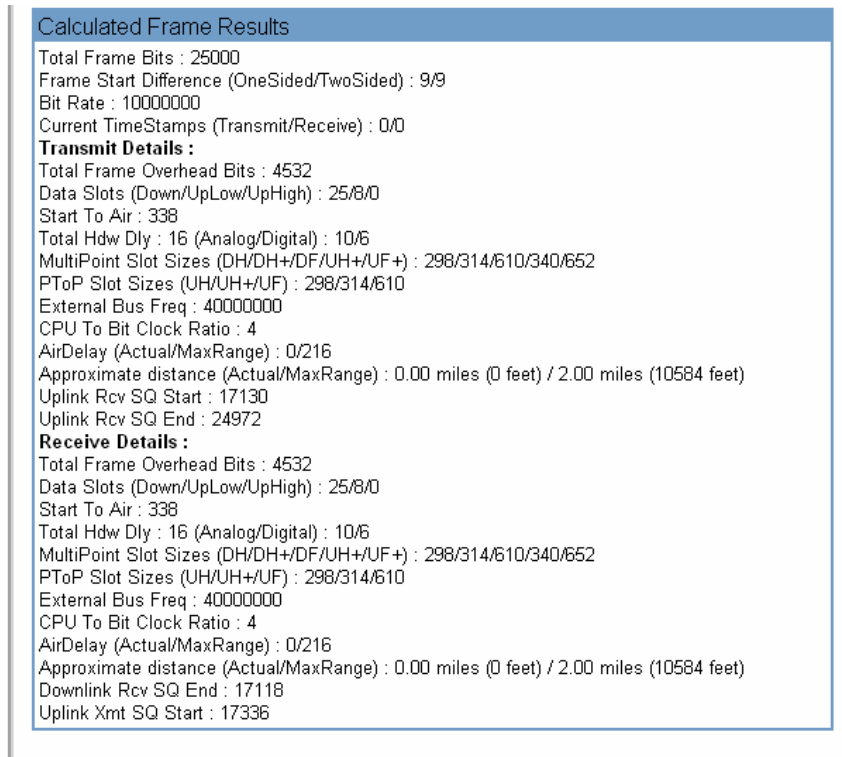


Figure 180: Calculated Frame Results section of Frame Calculator tab, example

6. Record the value of the **Uplink Rcv SQ Start** field.
7. Enter a parameter set from another AP or use a different module (OFDM or FSK) to calculate results for that technology type.
8. Click the **Apply Settings** button.
9. Click the **Calculate** button.
10. Scroll down the tab to the Calculated Frame Results section. If “Invalid Configuration” is displayed, check and change values and settings, with special attention to the **Platform Type** parameters (P7, P8, and so on).
11. Record the value of the **Uplink Rcv SQ Start** field.
12. If the recorded values of the **Uplink Rcv SQ Start** field are within 150 time bits of each other, skip the next step.
13. Repeat this procedure, changing the value of the **Downlink Data** parameter until the values that this tool calculates for the **Uplink Rcv SQ Start** field are within 300 time bits of each other; if possible, within 150 time bits.
14. Access the Radio tab in the Configuration web page of each AP in the cluster and change its **Downlink Data** parameter (percentage) to the last value that you used in the Frame Calculator.
See [Figure 75: Radio tab of AP \(900 MHz\), example](#) on Page 233.

===== **end of procedure**=====

27.6 VIEWING THE DFS STATUS TAB (ALL)

Examples of the DFS Status tab in the Tools page are shown in [Figure 181](#) and [Figure 182](#).

Figure 181: DFS Status tab of AP, example

Figure 182: DFS Status tab of SM, example

This tab provides an instant view of the current frequency in use and thus whether the Dynamic Frequency Selection (DFS) feature has shut down operation on the primary frequency to avoid competition with radar that is protected by regulation.

DFS Event History

This log is useful for seeing when DFS events happened, including the response of any **Alternate RF Carriers** that were assigned.

In the example shown in [Figure 181](#), the AP

1. performed a 60-second Channel Availability Check (CAC).
2. started transmitting at 1:03 (mm:ss) on 5580 MHz, the Primary RF Carrier Frequency.
3. experienced a DFS hit at 6:58:58 (hh:mm:ss).
4. switched to the Alternate RF Carrier Frequency 1 (5590 MHz).
5. performed a 60-second Channel Availability Check (CAC).
6. started transmitting on 5590 MHz.

27.7 USING THE SM CONFIGURATION TOOL (AP, BHM)

The SM Configuration tab in the Tools page of the AP or BHM displays

- the current values whose control may be subject to the setting in the **Configuration Source** parameter.
- an indicator of the source for each value.

An example of the SM Configuration tab is displayed in [Figure 183](#).

The screenshot shows the SM Configuration interface. On the left is a navigation menu with options like Configuration, Statistics, Tools, Account, Quick Start, Copyright, and Logoff. The main content area is titled 'Tools => SM Configuration' and shows the device '2.4GHZ - Access Point - 0a-00-3e-20-70-7c'. Below this is a 'Select Subscriber' section with a dropdown menu showing 'Idle [0a003e203ad4] Luid: 2'. The 'SM Configuration Info' section contains the following text:

LUID: 002 ; MAC: 0a-00-3e-20-3a-d4 State: IDLE

Site Name : Jok Wong's House (.98)

Sustained Uplink Data Rate(AP): 10000 Uplink Burst Allocation(AP): 10000 Sustained

Downlink Data Rate (AP): 10000 Downlink Burst Allocation (AP): 10000 (kbit)

HiPriChan(D): 0 VCChannel: 1

Low Priority Uplink CIR (D): 0 Low Priority Downlink CIR (D): 0 High Priority Uplink CIR (D): 0

High Priority Downlink CIR (D): 0 (kbps)

Low Priority Uplink (D): 3 Low Downlink Priority (D): 3 High Uplink Priority (D): 5 High

Downlink Priority (D): 5

APBerLevel(D): 4 Level HiPriTCPAck(D): 1

AllowVLANLearning(D): 0 AllowVLANFrameType(D): 0 VLANAgeTmout(D): 25

SMManageVID(D): 1

IngressVID(D): 1 ManageVID(D): 1

MemberSet(D):

VID Number Type Age

Empty Set

At the bottom of the configuration area are two buttons: 'Save Changes' and 'Reboot'.

Figure 183: SM Configuration tab of AP, example

Indicators for configuration source are explained under [Session Status Tab of the AP](#) on [Page 196](#).

27.8 REVIEWING THE LINK STATUS TOOL RESULTS (AP)

An example of the Link Status tool results is shown in [Figure 184](#).

Link Capacity Test | Frame Calculator | Subscriber Configuration | DFS Status | **Link Status** | Remote Spectrum Analyzer

Tools => Link Status

5.4GHz - Access Point - 0a-00-3e-52-14-7d

Subscriber	Uplink Statistics			Downlink Statistics			BER Results	Reg Requests	ReReg Requests
	Power Level	Jitter	Last Link Test Efficiency Percentage	Power Level	Jitter	Last Link Test Efficiency Percentage			
Garcia [0a003e521463] Luid: 2	-74 dBm	9	98 %	-73 dBm	2	97 %	1.826951e-04	4	0
Smith [0a003e521486] Luid: 3	-42 dBm	10	100 %	-40 dBm	2	100 %	2.530763e-07	1	0
Lee [0a003e521465] Luid: 4	-76 dBm	5	84 %	-77 dBm	6	88 %	1.126781e-02	1	1

Figure 184: Link Status tab of AP, example

The Link Status tool results include values for the following fields.

Power Level

Jitter

These are reported near-instantaneously, if web refresh rate is set to 1 or 2 seconds. These values are the same as those that are displayed on the Session Status tab of the Home page in the AP and the General Status tab of the Home page in the SM.

Last Link Test Efficiency Percentage

This field displays the results of the last link test initiated from the SM. Link tests initiated from the AP *are not* shown. A link test exercises both uplink and downlink, and efficiencies for both are reported.

BER Results

This field displays the over-the-air Bit Error Rates for each downlink. (The ARQ [Automatic Resend reQuest] ensures that the transport BER [the BER seen end-to-end through a network] is essentially zero.) The level of acceptable over-the-air BER varies, based on operating requirements, but a reasonable value for a good link is a BER of $1e-4$ (1×10^{-4}) or better, approximately a packet resend rate of 5%.

BER is generated using unused bits in the downlink. During periods of peak load, BER data is not updated as often, because the system puts priority on transport rather than on BER calculation.

Registration Requests
Re-registration Requests

These request counts are shown for each SM since the time of the last AP reboot. A **Registration Requests** count is the number of times the SM registered after the AP determined that the link had been down. A **Re-registration Requests** count is the number of times the AP received an SM registration request while the AP considered the link to be still up (and therefore did not expect registration requests).

27.9 USING THE REMOTE SPECTRUM ANALYZER TOOL (AP)

The Remote Spectrum Analyzer tool in the AP provides additional flexibility in the use of the spectrum analyzer in the SM. You can set a duration of 10 to 1000 seconds and select an SM from the drop-down list, then click the **Start Remote Spectrum Analysis** button to launch the analysis from that SM. An example of this tool in the AP is shown in [Figure 185](#).

Link Capacity Test
Frame Calculator
Subscriber Configuration
Link Status
Remote Spectrum Analyzer

- Home
- Configuration
- Statistics
- Tools
- Account
- Quick Start
- Copyright
- Logoff

Account: admin
Level: ADMINISTRATOR

Tools => Remote Spectrum Analyzer

5.7GHz - Access Point - 0a-00-3e-fe-ed-de

Access Point Stats

Registered SM Count :	2
Max Registered SM Count :	2

Configuration

Current Subscriber Module :

Duration : Seconds (10-1000)

Results from Subscriber

Results retrieved successfully.

Timed Spectrum Analysis complete for 10 seconds
System time at start of analysis: 00:26:17 01/01/2001
Site Name: No Site Name Location: No Site Location Contact: No Site Contact

Freq	-100	-95	-90	-85	-80	-75	-70	-65	-60	-55	-50	-45	I-40 (dBm)	Avg I	Max I
5715	[Bar]												-82	-82	
5720	[Bar]												-82	-82	
5725	[Bar]												-82	-82	
5730	[Bar]												-82	-82	
5735	[Bar]												-82	-82	
5740	[Bar]												-82	-82	
5745	[Bar]												-82	-82	
5750	[Bar]												-79	-79	
5755	[Bar]												-74	-73	
5760	[Bar]												-49	-48	
5765	[Bar]												-48	-47	
5770	[Bar]												-48	-47	
5775	[Bar]												-48	-48	
5780	[Bar]												-49	-49	
5785	[Bar]												-49	-49	
5790	[Bar]												55	53	
5795	[Bar]												-77	-77	
5800	[Bar]												-82	-82	
5805	[Bar]												-82	-82	
5810	[Bar]												-82	-82	
5815	[Bar]												-82	-82	
5820	[Bar]												-82	-82	
5825	[Bar]												-82	-82	
5830	[Bar]												-82	-82	
5835	[Bar]												-82	-82	
5840	[Bar]												-82	-82	
5845	[Bar]												-82	-82	
5850	[Bar]												-82	-82	
5855	[Bar]												-82	-82	
5860	[Bar]												-82	-82	

Data : [SpectrumAnalysis.xml](#)

Figure 185: Remote Spectrum Analyzer tab of AP, example

This feature proceeds in the following sequence:

1. The AP de-registers the target SM.
2. The SM scans (for the duration set in the AP tool) to collect data for the bar graph.
3. The SM re-registers to the AP.
4. The AP displays the bar graph.

The bar graph is an HTML file, but can be changed to an XML file, which is then easy to analyze through the use of scripts that you may write for parsing the data. To transform the file to XML, click the [SpectrumAnalysis.xml](#) link. Although the resulting display appears mostly unchanged, the bar graph is now coded in XML. You can now right-click on the bar graph for a **Save Target As** option to save the `Spectrum Analysis.xml` file.

27.10 USING THE BER RESULTS TOOL (SM, BHS)

Radio BER data represents bit errors at the RF link level. Due to CRC checks on fragments and packets and ARQ (Automatic Repeat reQuest), the BER of customer data is essentially zero. Radio BER gives one indication of link quality. Other important indications to consider include the received power level, jitter, and link tests. Radio BER is supported on FSK and OFDM radios.

BER is only instrumented on the downlink and is displayed on the BER Results tab of the Tools page in any SM. Each time the tab is clicked, the current results are read, and counters are reset to zero. An example of the BER Results tab is displayed in [Figure 186](#).

The screenshot shows the 'BER Results' tab of the Tools page. The main content area displays the following information:

Tools => BER Results
2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48

Receive BER Results

BER 4-Level
 Number of bits received : 292510720
 Number of Primary bit errors : 238
 Number of Secondary bit errors : 271
 Measured Primary Bit Error Rate : 8.136454e-07
 Measured Secondary Bit Error Rate : 9.264618e-07
 Measured Total Bit Error Rate : 1.740107e-06

A 'Clear BER Results' button is located at the bottom right of the results area, highlighted with a red box.

Figure 186: BER Results tab of FSK SM, example

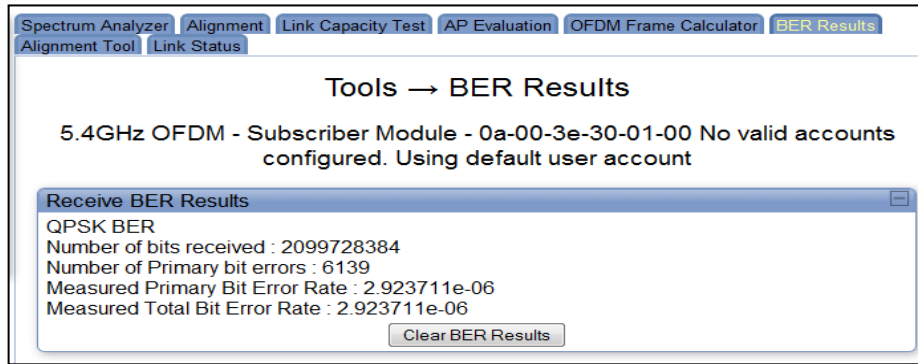


Figure 187: BER Results tab of OFDM SM, example

The BER Results tab can be helpful in troubleshooting poor link performance. The value in the **Measured Total Bit Error Rate** field represents the bit error rate (BER) in the RF link since the last time the BER Results tab was clicked. If the AP is enabled for 2X operation, then this tab displays both **Primary (1X)** and **Secondary (2X) Bit Error Rate** fields. If the link sometimes operates in 2X, then the **Measured Secondary Bit Error Rate** field is populated by a measurement.

The link is acceptable if the value of this field is less than 10^{-4} . If the BER is greater than 10^{-4} , re-evaluate the installation of both modules in the link.

The BER test signal is broadcast by the AP (and compared to the expected test signal by the SM) only when capacity in the sector allows it. This signal is the lowest priority for AP transmissions.

28 MAINTAINING YOUR SOFTWARE

Motorola provides release compatibility information and caveats about each release. For the latest information and caveats about each software release, see the release notes available for download from <http://motorola.wirelessbroadbandsupport.com/software/>.

28.1 HISTORY OF SYSTEM SOFTWARE UPGRADES

28.1.1 Release 8 Features

Release 8 introduced the following features:

- Scheduling Limited to Hardware Scheduler
- Tiered Permissions and User Accounts
- GUI Customizable via CSS
- Links to SM GUI via Session Status and Remote Subscribers Tabs of AP
- Dynamic Frequency Selection (DFS) v1.2.3 in All 5.4- and 5.7-GHz Modules
- Bit Error Rate (BER) Display with Hardware Scheduler
- AP SNMP Proxy to SMs
- Translation Bridging (MAC Address Mapping)
- SM Isolation
- Management Access Filtering for SM
- Source IP Management Access for AP and SM
- Optional DHCP Configuration of Management Interface
- High-priority Channel on P7 and P8 SMs on Hardware Scheduling
- Power Save Mode on P10 Radios
- Dynamic Frequency Selection (DFS) ETSI v1.3.1 Update (5.4- and 5.7-GHz in Europe, 5.4-GHz in Brazil, and other ETSI-regulated regions)
- Automatic Configuration for DFS through Settable Region Code
- Two Settable Alternate Frequencies for Radar Competition Avoidance
- Whitening for Self-interference Avoidance
- One-fourth Increase in Maximum Packet Processing Rate
- New MIR Settings to Limit Broadcast Packets from SMs
- VLAN ID Added to PTP Modules for Management Traffic
- Overload Indicators for Ethernet and RF Interfaces
- Link Layer Discovery Protocol (LLDP) Support
- Ten Accessing Subnets for Management via SNMP
- Weather Notch-out for 5.4-GHz Radios in Europe
- 5.9-GHz Radios Supporting Center-channel Frequencies of 5960 to 6050
- DFS Feature Removed from 5.4-GHz SM/BHS When Set to Brazil

28.1.2 Release 8 Fixes

Release 8 included the following fixes:

- Management Web (http) Access Lockup Fix
- Enforcement of Ethernet Link Speed Setting
- MIBs Support Only Applicable Objects
- Configured CIR Applied in 2X Operation

28.1.3 Release 9 Features

Release 9 introduces the following features:

- Support for PMP 400 Series APs and SMs in the 4.9- and 5.4-GHz Frequency Band Range
- Support for 2- and 4-Mbps PTP 100 Series Wireless Ethernet Bridges in the 5.7-GHz Frequency Band Range
- Support for PTP 200 Series Wireless Ethernet Bridges in the 4.9- and 5.4-GHz Frequency Band Range
- Support for P11 Firmware
- Support for Dynamic Frequency Selection (DFS) ETSI v1.4.1
- Per-SM Query Instead of Link Status Table

28.1.4 Release 9 Fixes

Release 9 includes the following fixes:

- Ethernet Speed Selection No Longer Trouble-prone
- Capability to Reset the BER to Zero
- Capability to Obtain a NAT Public IP Address via DHCP when Two DHCP Servers Exist in the Subnet
- Telnet Session Continues Through Upgrade from Release 8.2.7 to Release 9
- All SM Upgrades from Release 8.2.7 to Release 9 Succeed
- Erroneous Frequency Indication of Factory Not Displayed Following Upgrade from Release 8.2.7 to Release 9
- Scan Selection List Includes All Available Frequencies Following Upgrade from Release 8.2.7 to Release 9
- Accurate BER Count
- Accurate Count of Layer 2 Neighbors Reported via SNMP
- Null Community String Disallowed
- PC Connected to NAT-enabled SM Limited to DHCP Server Pool for IP Address
- Transmit Power Setting Displayed Correctly in P7 and P8 Firmware Platform
- SNMP OID Added for RXOverRun Count
- SM Management VLAN ID Pass-through Filtering in Both Uplink and Downlink
- Connecting Mode Replaces Persistent LCP Negotiating Mode for PPPoE Session Setup Problems in SM
- TFTP Server Option Functional for Upgrades
- Config Source and VLAN Allow Frame Types Configurable in PMP 100 Series APs and SMs

- Correct [Received] Power Level Display in P9 Firmware Platform for CAP 09130 and CSM 09130
- Default Read/Write and Read Only Community String Values in CAP 54400, CSM 54400, and PTP 54200 Radios Consistent with Defaults in Other Frequency Band Ranges

28.2 HISTORY OF CMMmicro SOFTWARE UPGRADES

Canopy currently supports CMMmicro Releases up through Release 3.0.

28.3 TYPICAL CONTENTS OF RELEASE NOTES

Motorola supports each release with software release notes, which include

- description of features that are introduced in the new release.
- issues that the new release resolves.
- known issues and special notes for the new release.
- installation procedures for the new release.

28.4 TYPICAL UPGRADE PROCESS

In a typical upgrade process, proceed as follows:

1. Visit <http://motorola.wirelessbroadbandsupport.com/support/>.
2. Click the **Software Updates** link.
3. Read the compatibility information and any caveats that Motorola associates with the release.
4. Read the software release notes from the web site.
5. On the basis of these, decide whether the release is appropriate for your network.
6. Download the software release and associated files.
7. Use CNUT to manage the upgrade across your network.



NOTE:

After the initial 12-month standard warranty, an annual Software Maintenance Contract must be obtained to continue receiving software updates and technical support. The contract includes minor software enhancements as they become available and 24/7 telephone support. Contracts are available through Motorola's authorized reseller partners or directly from the Technical Support Center with a credit card.

Major software feature enhancements may require the purchase of a license key and/or new hardware.

28.4.1 Downloading Software and Release Notes

All supported software releases, the associated software release notes document, and updated MIB files are available for download at any time from <http://motorola.wirelessbroadbandsupport.com/support/software>. This web site also typically provides a summary of the backward compatibility and any advantages or disadvantages of implementing the release.

When you click on the release that you wish to download, you are prompted for information that identifies yourself and your organization (such as name, address, and e-mail address). When you complete and submit the form that prompts for this information, the download is made available to you.

29 REBRANDING MODULE INTERFACE SCREENS

Distinctive fonts indicate

```
literal user input.  
variable user input.  
literal system responses.  
variable system responses.
```

The interface screens on each module display the Canopy or Canopy Advantage logo. These logos can be replaced with other logos using [Procedure 38](#).

The logo is a hyperlink, and clicking on it takes the user to the Canopy web site. A different site (perhaps the operator's support site) can be made the destination using [Procedure 39](#).

To return a module to regular logos and hyperlinks, use [Procedure 40](#).

The logo at the top of each page is a key indicator to the user whether a module is Canopy or Canopy Advantage. If you choose to replace the logos, use two noticeably different logos so that users can continue to easily distinguish between a Canopy module and a Canopy Advantage module.

To replace logos and hyperlinks efficiently throughout your network, read the following two procedures, write a script, and execute your script through the Canopy Network Updater Tool (CNUT).⁹ To replace them individually, use one of the following two procedures.

Procedure 38: Replacing the Canopy logo on the GUI with another logo

1. If the current logo is the Canopy logo, name your custom logo file on your computer `canopy.jpg` and put it in your home directory.
If the current logo is the Canopy Advantage logo, name your custom logo file on your computer `advantaged.jpg` and put it in your home directory.
2. Use an FTP (File Transfer Protocol) session to transfer this file to the module, as in the example session shown in [Figure 188](#).

⁹ See [Using the Canopy Network Updater Tool \(CNUT\)](#) on Page 413.

```
> ftp ModuleIPAddress
Connected to ModuleIPAddress
220 FTP server ready
Name (ModuleIPAddress:none): root
331 Guest login ok
Password: <password-if-configured>
230 Guest login ok, access restrictions apply.

ftp> binary
200 Type set to I
ftp> put canopy.jpg
      OR
      put advantaged.jpg
      OR
      put top.html
ftp> quit
221 Goodbye
```

Figure 188: Example ftp session to transfer custom logo file

3. Use a telnet session and the `addwebfile` command to add the new file to the file system, as in the example session shown in [Figure 189](#).



NOTE:

Supported telnet commands execute the following results:

- `addwebfile` adds a custom logo file to the file system.
- `clearwebfile` clears the logo file from the file system.
- `lsweb` lists the custom logo file and display the storage space available on the file system.


```

>telnet ModuleIPAddress
/-----\
C A N O P Y

Motorola Broadband Wireless Technology Center
(Copyright 2001, 2002 Motorola Inc.)

Login: root
Password: <password-if-configured>

Telnet +> addwebfile canopy.jpg
          OR
          addwebfile advantaged.jpg
          OR
          addwebfile top.html

Telnet +> lsweb

Flash Web files
/canopy.jpg      7867
free directory entries: 31
free file space: 55331

Telnet +> exit

```

Figure 189: Example telnet session to activate custom logo file

===== end of procedure =====

Procedure 39: Changing the URL of the logo hyperlink

1. In the editor of your choice, create a file named `top.html`, consisting of one line:

```
<a href="myurl">
```

where *myurl* is the desired URL, for example, `http://www.canopywireless.com`.
2. Save and close the file as `top.html`.
3. Use an FTP (File Transfer Protocol) session to transfer this file to the module, as in the example session shown in [Figure 188](#) on Page 464.
4. Use a telnet session and the `addwebfile` command to add the new file (`top.html`) to the file system, as in the example session shown in [Figure 189](#).

===== end of procedure =====

If you ever want to restore the original logo and hyperlink in a module, perform the following steps.

Procedure 40: Returning a module to its original logo and hyperlink

1. Use a telnet session and the clearwebfile command to clear all custom files from the file system of the module, as in the example session shown in [Figure 190](#) below.

```
>telnet ModuleIPAddress
/-----\
C A N O P Y

Motorola Broadband Wireless Technology
Center
(Copyright 2001, 2002 Motorola Inc.)

Login: root
Password: <password-if-configured>

Telnet +> lsweb
Flash Web files
canopy.jpg      7867
free directory entries: 31
free file space: 56468

Telnet +> clearwebfile
Telnet +> lsweb

Flash Web files
free directory entries: 32
free file space      64336 bytes

Telnet +> exit
```

Figure 190: Example telnet session to clear custom files

===== end of procedure =====

30 TOGGLING REMOTE ACCESS CAPABILITY

Based on your priorities for additional security and ease of network administration, you can deny or permit remote access individually to any AP, SM, or BH.

30.1 DENYING ALL REMOTE ACCESS

Wherever the No Remote Access feature is enabled by the following procedure, physical access to the module is required for

- any change in the configuration of the module.
- any software upgrade in the module.

Where additional security is more important than ease of network administration, you can disable all remote access to a module as follows.

Procedure 41: Denying all remote access

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power up or power cycle the module.
3. Access the web page <http://169.254.1.1/lockconfig.html>.
4. Click the check box.
5. Save the changes.
6. Reboot the module.
7. Remove the override plug.

RESULT: No access to this module is possible through HTTP, SNMP, FTP, telnet, or over an RF link.

===== end of procedure =====

30.2 REINSTATING REMOTE ACCESS CAPABILITY

Where ease of network administration is more important than the additional security that the No Remote Access feature provides, this feature can be disabled as follows:

Procedure 42: Reinstating remote access capability

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power up or power cycle the module.
3. Access the web page <http://169.254.1.1/lockconfig.html>.
4. Click the check box to uncheck the field.
5. Save the changes.
6. Reboot the module.
7. Remove the override plug.

RESULT: Access to this module is possible through HTTP, SNMP, FTP, telnet, or over an RF link.

===== end of procedure =====

31 SETTING UP A PROTOCOL ANALYZER ON YOUR NETWORK

Selection of protocol analyzer software and location for a protocol analyzer depend on both the network topology and the type of traffic to capture. However, the examples in this section are based on free-of-charge Ethernet software, which is available at <http://ethereal.com/>.

The equipment required to set up a protocol analyzer includes:

- 1 hub
- 1 laptop computer with protocol analyzer software installed
- 2 straight-through Ethernet cables
- 1 power converter

31.1 ANALYZING TRAFFIC AT AN SM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the SM. If the SM has DHCP enabled, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the SM.

The configuration for analyzing traffic at an SM is shown in [Figure 191](#).

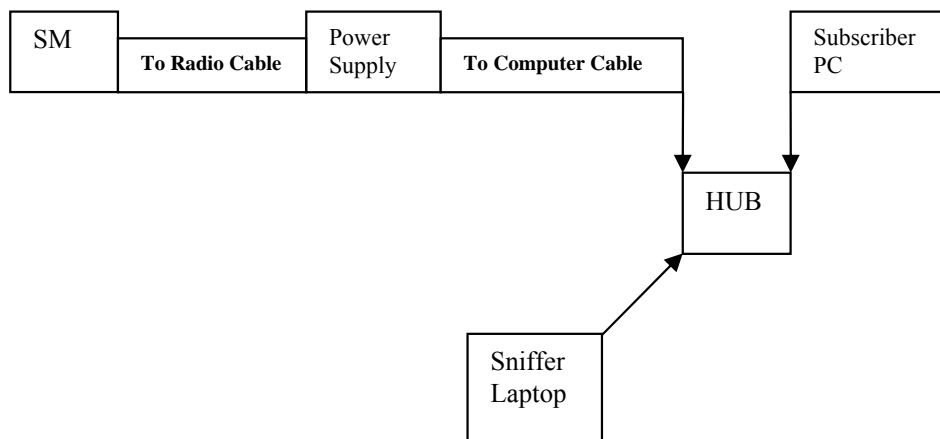


Figure 191: Protocol analysis at SM

31.2 ANALYZING TRAFFIC AT AN AP OR BH WITH NO CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP/BH. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the AP/BH.

The configuration for analyzing traffic at an AP or BH that *is not* connected to a CMM is shown in [Figure 192](#).

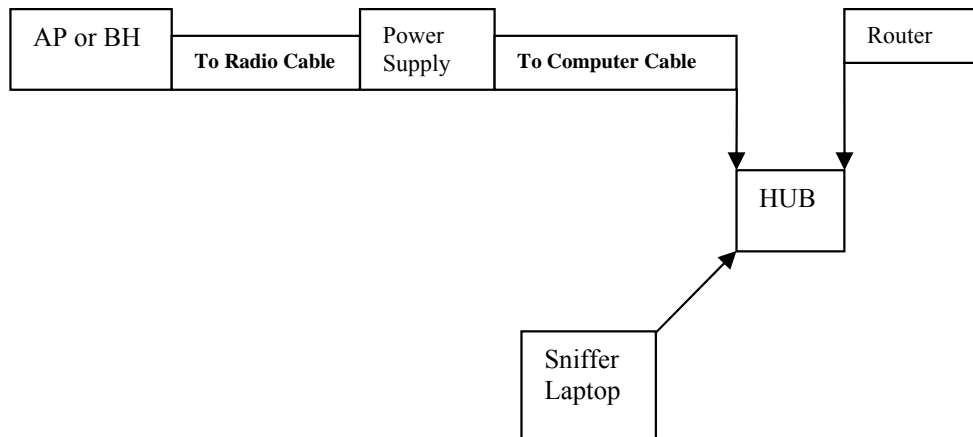


Figure 192: Protocol analysis at AP or BH not connected to a CMM

31.3 ANALYZING TRAFFIC AT AN AP OR BH WITH A CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP/BH. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, ensure that the laptop computer is configured with a static IP address in the same subnet as the AP/BH.

Connect the hub to the J2 Ethernet to Switch of the port that is associated with the AP/BH. This example is of capturing traffic from AP/BH 111, which is connected to Port 1. The configuration for analyzing traffic at an AP or BH that is connected to a CMM is shown in [Figure 193](#).

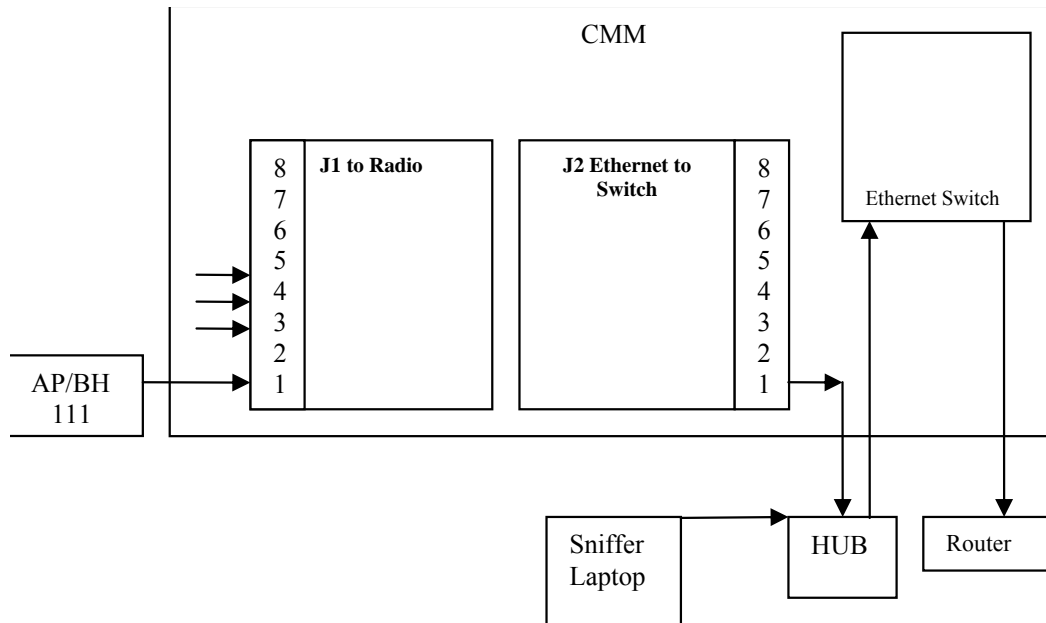


Figure 193: Protocol analysis at AP or BH connected to a CMM

31.4 EXAMPLE OF A PROTOCOL ANALYZER SETUP FOR AN SM

The following is an example of a network protocol analyzer setup using *Ethereal*[®] software to capture traffic at the SM level. The *Ethereal* network protocol analyzer has changed its name to *Wireshark*[™], but functionality and use remains much the same. This example is based on the following assumptions:

- All required physical cabling has been completed.
- The hub, protocol analyzer laptop computer, and subscriber PC are successfully connected.
- The SM is connected
 - as shown in [Figure 192](#) on Page 470.
 - to the subscriber PC and the AP.
- *Ethereal* software is operational on the laptop computer.

Although these procedures involve the SM, the only difference in the procedure for analyzing traffic on an AP or BH is the hub insertion point.

The IP Configuration screen of the example SM is shown in [Figure 194](#).

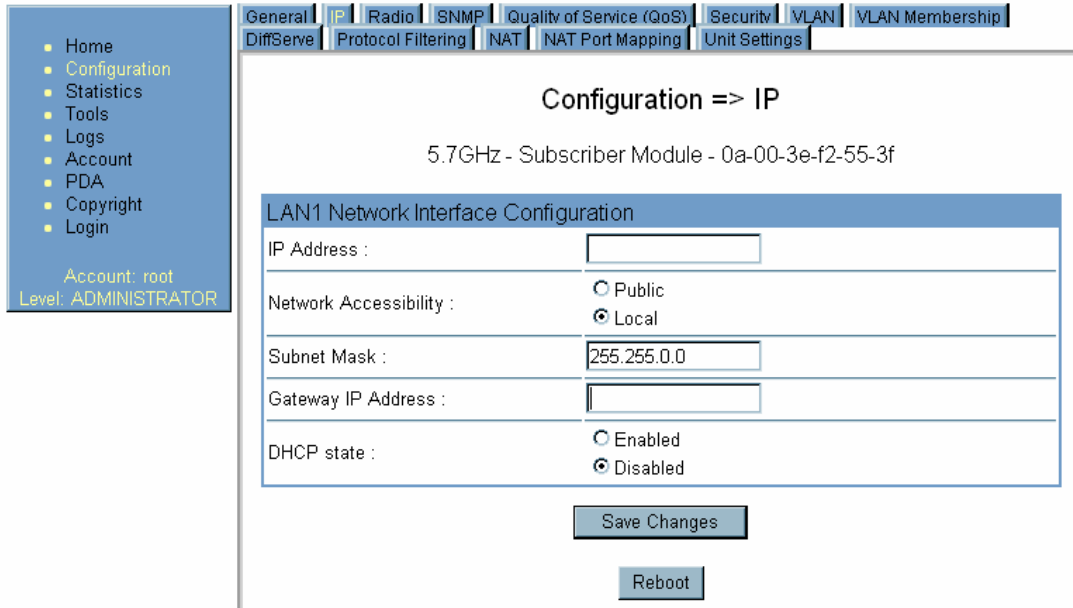


Figure 194: IP tab of SM with NAT disabled and local accessibility

Procedure 43: Setting up a protocol analyzer

1. Note the IP configuration of the SM.
2. Browse to **Start→My Network Places→Network and Dialup Connections**.
3. For **Local Area Connection**, select **Properties**.

RESULT: The Local Area Connections Properties window opens, as shown in [Figure 195](#).

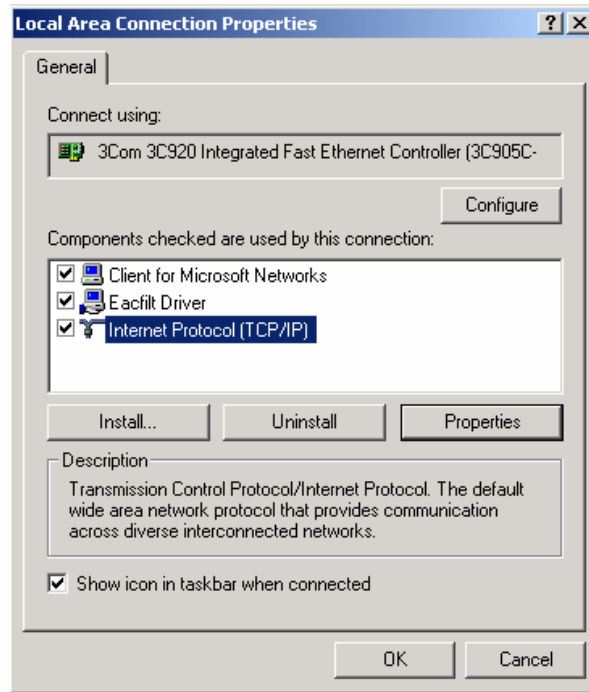


Figure 195: Local Area Connection Properties window

4. Select **Internet Protocol (TCP/IP)**.
5. Click the **Properties** button.
RESULT: The Internet Protocol (TCP/IP) Properties window opens, as shown in [Figure 196](#).

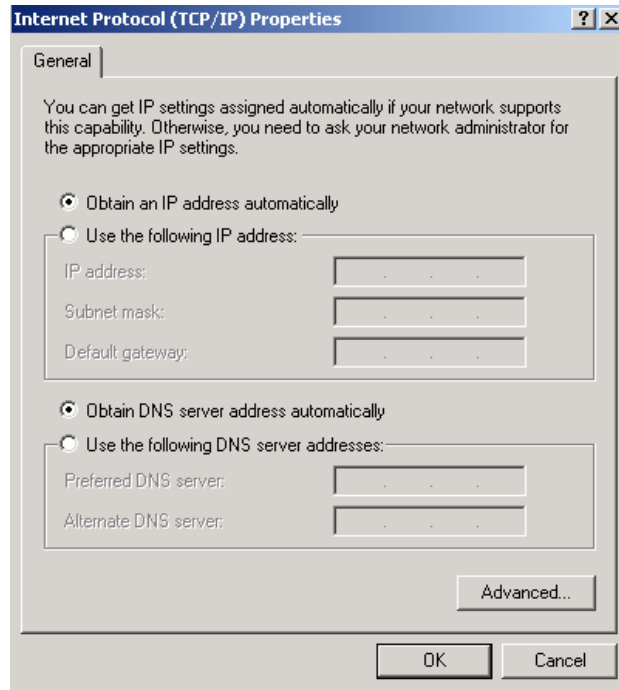


Figure 196: Internet Protocol (TCP/IP) Properties window

6. Unless you have a static IP address configured on the SM, select **Obtain an IP address automatically** for the protocol analyzer laptop computer, as shown in [Figure 196](#).
7. If you have configured a static IP address on the SM, then
 - a. select **Use the following IP address**.
 - b. enter an IP address that is in the same subnet as the SM.
8. Click **OK**.
9. Open your web browser.
10. Enter the IP address of the SM.
RESULT: The General Status tab of the SM opens, as shown in [Figure 65](#) on [Page 202](#).
11. If the General Status tab did not open, reconfigure how the laptop computer obtains an IP address.
12. Verify that you have connectivity from the laptop computer to the SM with the hub inserted.
13. Launch the protocol analyzer software on the laptop computer.
14. In the **Capture** menu, select **Start**.
RESULT: The Ethereal Capture Options window opens, as shown in [Figure 197](#).

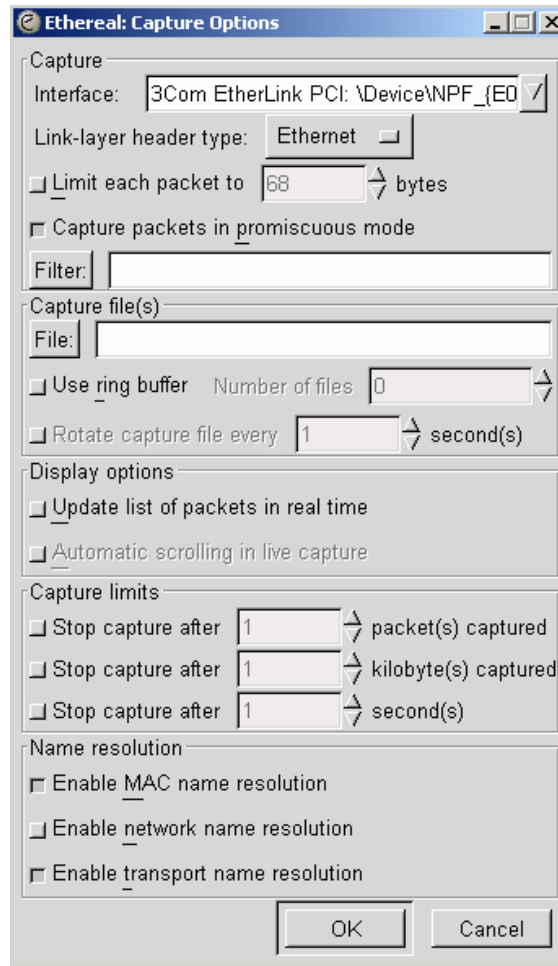


Figure 197: Ethereal Capture Options window

15. Ensure that the **Interface** field reflects the network interface card (NIC) that is used on the protocol analyzer laptop computer.
NOTE: Although you can select filters based on specific types of traffic, all values are defaults in this example.
16. If you wish to select filters, select them now.
17. Click **OK**.
RESULT: The Ethereal Capture window opens, as shown in [Figure 198](#).

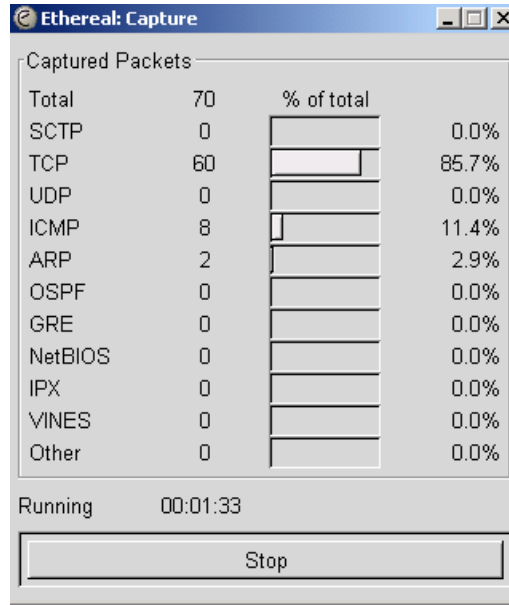


Figure 198: Ethereal Capture window

NOTE: This window graphically displays the types of packets (by percentage) that are being captured.

18. If all packet types are displayed with 0%, either
 - launch your Web browser on the subscriber PC for the IP address of the SM
 - ping the SM from the home PC.
19. If still all packet types are displayed with 0% (meaning that no traffic is being captured), reconfigure IP addressing until you can successfully see traffic captured on the laptop computer.
20. Whenever the desired number of packets have been captured, click **Stop**.
RESULT: When you stop the packet capture, the <capture> - Ethereal window opens, as shown in [Figure 199](#).

===== end of procedure =====

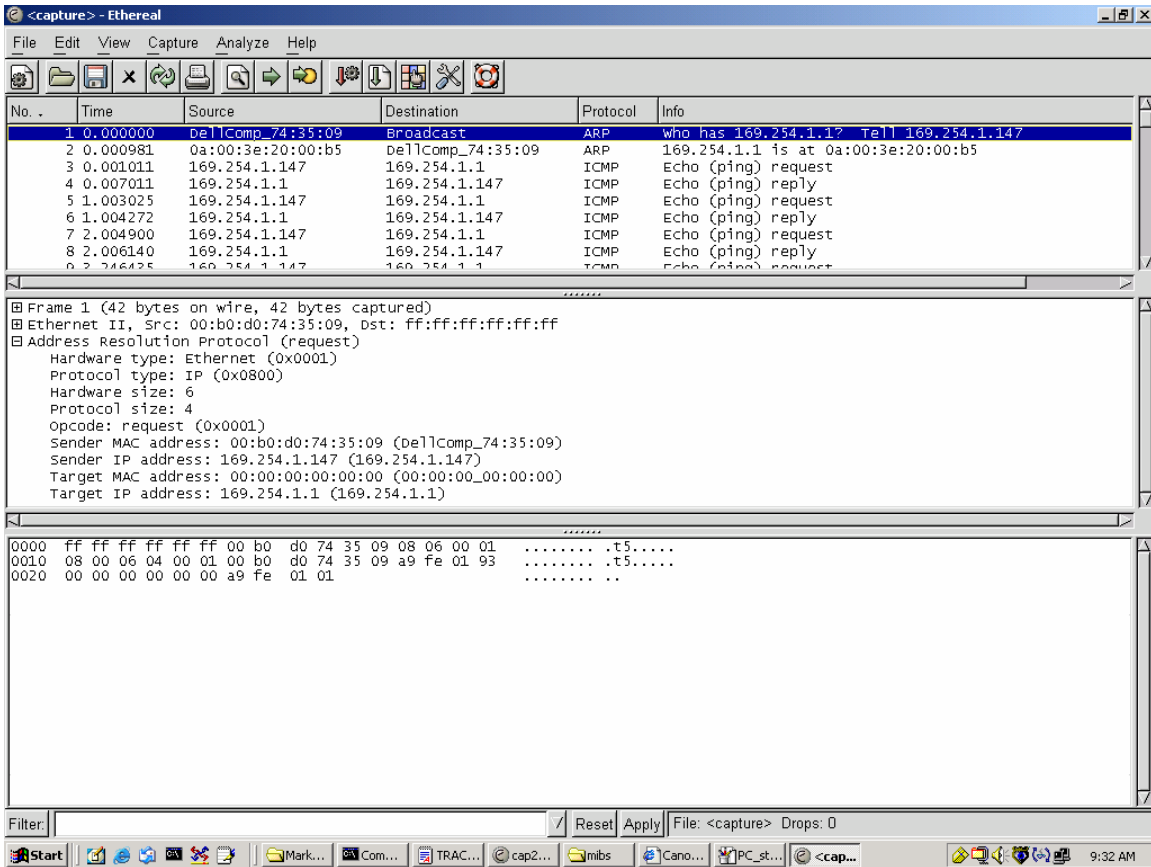


Figure 199: <capture> - Ethereal window, Packet 1 selected

This window has three panes:

- The top pane provides a sequenced summary of the packets captured and includes SRC/DEST address and type of protocol. What you select in this pane determines the additional information that is displayed in the lower two panes.
- The lower two panes facilitate drill-down into the packet that you selected in the top pane.

In this example, Packet 1 (a broadcast ARP request) was selected in the top pane. The lower two panes provide further details about Packet 1.

Another example is shown in [Figure 200](#).

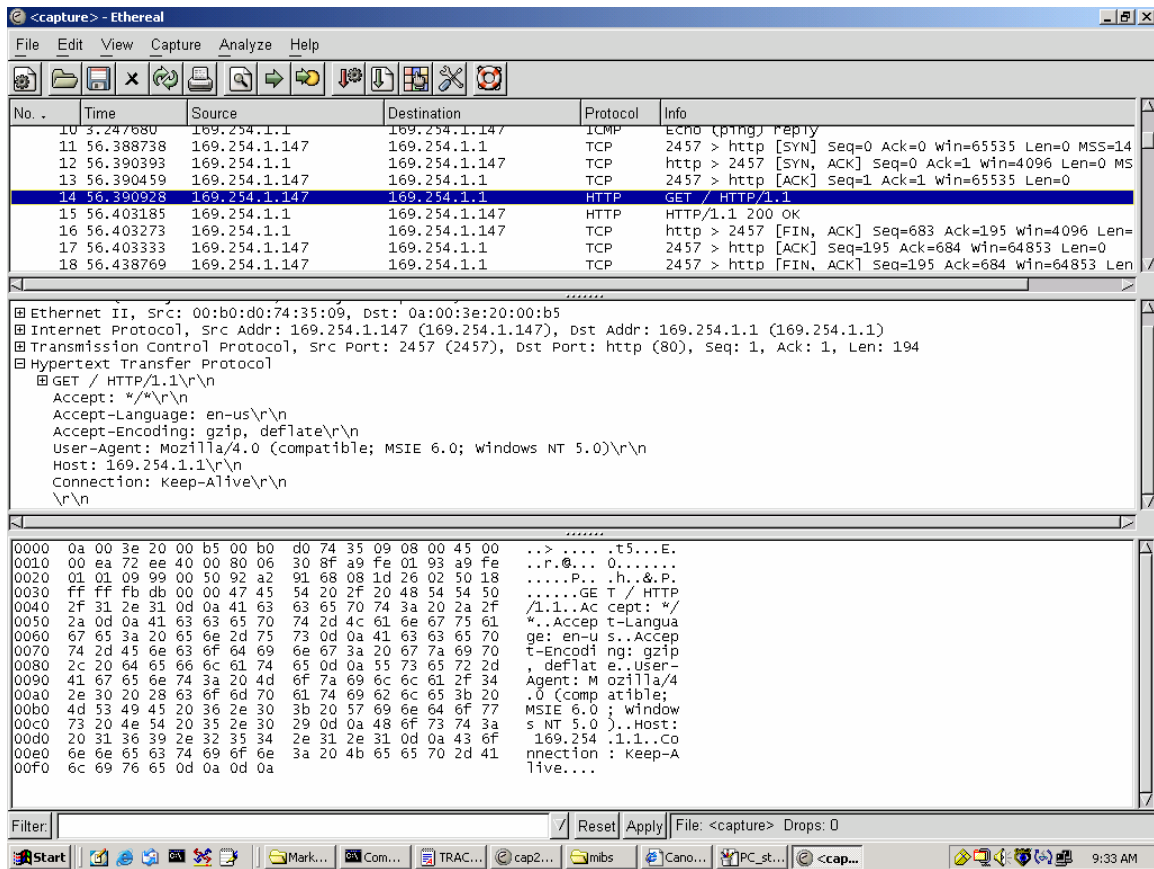


Figure 200: <capture> - Ethereal window, Packet 14 selected

In this second example, Packet 14 (protocol type HTTP) is selected in the top pane. The two lower panes provide further details about Packet 14.

32 TROUBLESHOOTING

32.1 GENERAL PLANNING FOR TROUBLESHOOTING

Effective troubleshooting depends in part on measures that you take before you experience trouble in your network. Motorola recommends the following measures for each site:

1. Identify troubleshooting tools that are available at your site (such as a protocol analyzer).
2. Identify commands and other sources that can capture baseline data for the site. These may include
 - **ping**
 - **tracert** or **tracertoute**
 - Link Capacity Test results
 - throughput data
 - Configuration tab captures
 - Status tab captures
 - session logs
3. Start a log for the site.
4. Include the following information in the log:
 - operating procedures
 - site-specific configuration records
 - network topology
 - software releases, boot versions, and FPGA firmware versions
 - types of hardware deployed
 - site-specific troubleshooting processes
 - escalation procedures
5. Capture baseline data into the log from the sources listed in Step 2.

32.2 GENERAL FAULT ISOLATION PROCESS

Effective troubleshooting also requires an effective fault isolation methodology that includes

- attempting to isolate the problem to the level of a system, subsystem, or link, such as
 - AP to SM
 - AP to CMM
 - AP to GPS
 - CMM to GPS
 - BHM to BHS
 - BHM to CMM
 - power

- researching Event Logs of the involved equipment. (See [Interpreting Messages in the Event Log](#) on Page 418.)
- answering the questions listed in the following section.
- reversing the last previous corrective attempt before proceeding to the next.
- performing only one corrective attempt at a time.

32.3 QUESTIONS TO HELP ISOLATE THE PROBLEM

When a problem occurs, attempt to answer the following questions:

1. What is the history of the problem?
 - Have we changed something recently?
 - Have we seen other symptoms before this?
2. How wide-spread is the symptom?
 - Is the problem on only a single SM? (If so, focus on that SM.)
 - Is the problem on multiple SMs? If so
 - is the problem on one AP in the cluster? (If so, focus on that AP)
 - is the problem on multiple, but not all, APs in the cluster? (If so, focus on those APs)
 - is the problem on all APs in the cluster? (If so, focus on the CMM and the GPS signal.)
3. Based on data in the Event Log (described in [Interpreting Messages in the Event Log](#) on Page 418)
 - does the problem correlate to External Hard Resets with no WatchDog timers? (If so, this indicates a loss of power. Correct your power problem.)
 - is intermittent connectivity indicated? (If so, verify your configuration, power level, jitter, cables and connections, and the speed duplex of both ends of the link).
 - does the problem correlate to loss-of-sync events?
4. Are connections made via *shielded* cables?
5. Does the GPS antenna have an *unobstructed* view of the entire horizon?

32.4 SECONDARY STEPS

After preliminary fault isolation through the above steps

1. check the Canopy knowledge base (<http://motorola.wirelessbroadbandsupport.com/support/knowledge/>) to find whether other network operators have encountered a similar problem.
2. proceed to any appropriate set of diagnostic steps. These are organized as follows:
 - [Module Has Lost or Does Not Establish Connectivity](#)
 - [NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity](#) on Page 482
 - [SM Does Not Register to an AP](#) on Page 484
 - [BHS Does Not Register to the BHM](#) on Page 485
 - [Module Has Lost or Does Not Gain Sync](#) on Page 486

- [Module Does Not Establish Ethernet Connectivity](#) on Page 487
- [Module Does Not Power Up](#) on Page 487
- [Power Supply Does Not Produce Power](#) on Page 488
- [CMM Does Not Pass Proper GPS Sync to Connected Modules](#) on Page 489

32.5 PROCEDURES FOR TROUBLESHOOTING

32.5.1 Module Has Lost or Does Not Establish Connectivity

To troubleshoot a loss of connectivity, perform the following steps.

Procedure 44: Troubleshooting loss of connectivity

1. Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.
2. Set up the minimal amount of equipment.
3. On each end of the link
 - a. check the cables and connections.
 - b. verify that the cable/connection scheme—straight-through or crossover—is correct.
 - c. verify that the LED labeled LNK is green.
 - d. access the General Status tab in the Home page of the module.
 - e. verify that the SM is registered.
 - f. verify that RSSI is 700 or higher.
 - g. verify that jitter is reported as 9 or lower.
 - h. access the IP tab in the Configuration page of the module.
 - i. verify that IP addresses match and are in the same subnet.
4. On the SM end of the link
 - a. verify that the PC that is connected to the SM is correctly configured to obtain an IP address through DHCP.
 - b. execute `ipconfig`.
 - c. verify that the PC has an assigned IP address.
5. On each end of the link
 - a. access the General tab in the Configuration page of each module.
 - b. verify that the setting for **Link Speeds** (or negotiation) matches that of the other module.
 - c. access the Radio tab in the Configuration page of each module.
 - d. verify that the **Radio Frequency Carrier** setting is checked in the Custom Radio Frequency Scan Selection List.
 - e. verify that the **Color Code** setting matches that of the other module.
 - f. access the browser LAN settings (for example, at **Tools→Internet Options→Connections→LAN Settings** in Internet Explorer).
 - g. verify that none of the settings are selected.
 - h. access the Link Capacity Test tab in the Tools page of the module.

- i. perform a link test. (See [Procedure 36: Performing a Link Capacity Test](#) on Page 440.)
 - j. verify that the link test results show efficiency greater than 90% in both the uplink and downlink (except as described under [Comparing Efficiency in 1X Operation to Efficiency in 2X Operation](#) on Page 136).
 - k. execute `ping`.
NOTE: A ping size larger than 1494 Bytes to a module times out and fails. However, a ping of this size or larger to a system that is behind a Canopy module typically succeeds. It is generally advisable to ping such a system, since Canopy handles that ping with the same priority as is given all other transport traffic. The results are unaffected by ping size and by the load on the Canopy module that brokers this traffic.
 - l. verify that no packet loss was experienced.
 - m. verify that response times are not significantly greater than
 - 2.5 ms from BH to BH
 - 4 ms from AP to SM
 - 15 ms from SM to AP
 - n. replace any cables that you suspect may be causing the problem.
6. After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

===== end of procedure =====

32.5.2 NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity

Before troubleshooting this problem, identify the NAT/DHCP configuration from the following list:

- NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface) and DHCP Server
- NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface)
- NAT with DHCP Server
- NAT without DHCP

To troubleshoot a loss of connectivity for an SM configured for NAT/DHCP, perform the following steps.

Procedure 45: Troubleshooting loss of connectivity for NAT/DHCP-configured SM

1. Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.
2. Set up the minimal amount of equipment.
3. On each end of the link
 - a. check the cables and connections.
 - b. verify that the cable/connection scheme—straight-through or crossover—is correct.
 - c. verify that the LED labeled LNK is green.

4. At the SM
 - a. access the NAT Table tab in the Logs web page.
NOTE: An example of this tab is shown in [Figure 201](#).

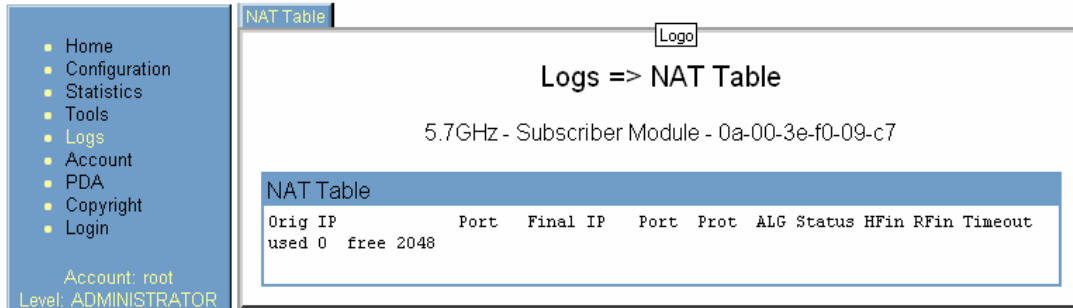


Figure 201: NAT Table tab of SM, example

- b. verify that the correct NAT translations are listed.
RESULT: NAT is eliminated as a possible cause if these translations are correct.
5. If this SM is configured for NAT with DHCP, then at the SM
 - a. execute `ipconfig`.
 - b. verify that the PC has an assigned IP address.
 - c. if the PC *does not* have an assigned IP address, then
 - enter `ipconfig /release "Adapter Name"`.
 - enter `ipconfig /renew "Adapter Name"`.
 - reboot the PC.
 - retreat to Step 5a.

if the PC has an assigned IP address, then

 - access the NAT DHCP Statistics tab in the Statistics web page of the SM.
NOTE: An example of this tab is shown in [Figure 202](#).

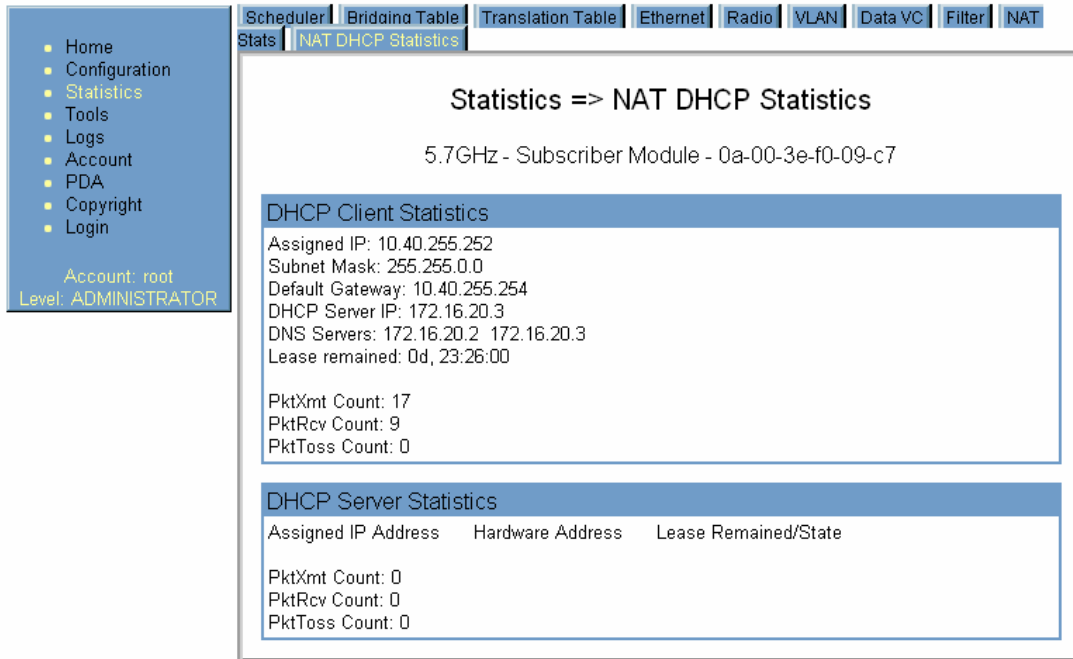


Figure 202: NAT DHCP Statistics tab of SM, example

- verify that DHCP is operating as configured.
6. After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

===== end of procedure =====

32.5.3 SM Does Not Register to an AP

To troubleshoot an SM failing to register to an AP, perform the following steps.

Procedure 46: Troubleshooting SM failing to register to an AP

1. Access the Radio tab in the Configuration page of the SM.
2. Note the **Color Code** of the SM.
3. Access the Radio tab in the Configuration page of the AP.
4. Verify that the **Color Code** of the AP matches that of the SM.
5. Note the **Radio Frequency Carrier** of the AP.
6. Verify that the value of the **RF Frequency Carrier** of the AP is selected in the **Custom Radio Frequency Scan Selection List** parameter in the SM.
7. In the AP, verify that the **Max Range** parameter is set to a distance slightly greater than the distance between the AP and the furthest SM that must register to this AP.
8. Verify that a clear line of sight exists between the AP and the SM, and that no obstruction significantly penetrates the Fresnel zone of the attempted link. If these conditions are not established, then verify that the AP and SM are 900-MHz modules in close proximity to each other.
9. Access the General Status tab in the Home page of each module.

10. In the **Software Version** field, verify that both the AP and SM are of the same encryption scheme (AES or DES).
11. Remove the bottom cover of the SM to expose the LEDs.
12. Power cycle the SM.
RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the SM is in Alignment mode because the SM failed to establish the link.
13. In this latter case, and if the SM has encountered no customer-inflicted damage, then request an RMA for the SM.

===== end of procedure =====

32.5.4 BHS Does Not Register to the BHM

To troubleshoot an BHS failing to register to the BHM, perform the following steps.

Procedure 47: Troubleshooting BHS failing to register to a BHM

1. Access the Radio tab in the Configuration page of the BHS.
2. Note the **Color Code** of the BHS.
3. Access the Radio tab in the Configuration page of the BHM.
4. Verify that the **Color Code** of the BHM matches that of the BHS.
5. Note the **Radio Frequency Carrier** of the BHM.
6. Verify that the value of the **RF Frequency Carrier** of the BHM is selected in the **Custom Radio Frequency Scan Selection List** parameter on the Configuration page of the BHS.
7. Verify that a clear line of sight exists between the BHM and BHS, and that no obstruction significantly penetrates the Fresnel zone of the attempted link.
8. Access the General Status tab in the Home page of each module.
9. In the **Software Version** field, verify that both the BHM and BHS are of the same encryption scheme (AES or DES).
10. Also in the **Software Version** field, verify that both the BHM and BHS are of the same modulation rate from the factory (BH20 or BH10).
11. Remove the bottom cover of the BHS to expose the LEDs.
12. Power cycle the BHS.

RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the BHS is in Alignment mode because the BHS failed to establish the link. In this latter case, and if the BHS has encountered no customer-inflicted damage, then request an RMA for the BHS.

===== end of procedure =====

32.5.5 Module Has Lost or Does Not Gain Sync

To troubleshoot a loss of sync, perform the following steps.

Procedure 48: Troubleshooting loss of sync

1. Access the Event Log tab in the Home page of the SM.

NOTE: An example of this tab is shown in [Figure 203](#).

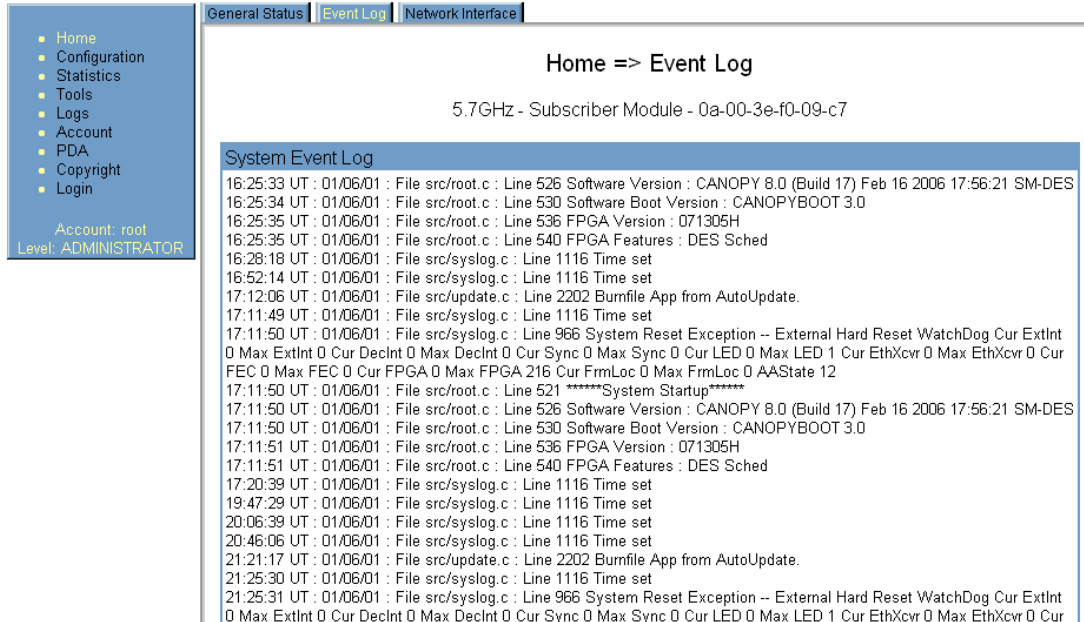


Figure 203: Event Log tab of SM, example

2. Check for messages with the following format:
RcvFrmNum =
ExpFrmNum =
(See [Table 69: Event Log messages for abnormal events](#) on Page 420.)
3. If these messages are present, check the Event Log tab of another SM that is registered to the same AP for messages of the same type.
4. If the Event Log of this second SM *does not* contain these messages, then the fault is isolated to the first SM.
If the Event Log page of this second SM contains these messages, access the GPS Status page of the AP.
5. If the **Satellites Tracked** field in the GPS Status page of the AP indicates fewer than 4 or the **Pulse Status** field does not indicate Generating Sync, check the GPS Status page of another AP in the same AP cluster for these indicators.
6. If these indicators are present in the second AP
 - a. verify that the GPS antenna still has an unobstructed view of the entire horizon.
 - b. visually inspect the cable and connections between the GPS antenna and the CMM.
 - c. if this cable is not shielded, replace the cable with shielded cable.

7. If these indicators *are not* present in the second AP
 - a. visually inspect the cable and connections between the CMM and the AP antenna.
 - b. if this cable is not shielded, replace the cable with shielded cable.

===== end of procedure =====

32.5.6 Module Does Not Establish Ethernet Connectivity

To troubleshoot a loss of Ethernet connectivity, perform the following steps.

Procedure 49: Troubleshooting loss of Ethernet connectivity

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. If the Ethernet cable connects the module to a network interface card (NIC), verify that the cable is pinned out as a straight-through cable.
4. If the Ethernet cable connects the module to a hub, switch, or router, verify that the cable is pinned out as a crossover cable.
5. Verify that the Ethernet port to which the cable connects the module is set to auto-negotiate speed.
6. Power cycle the module.
RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the module is in Alignment mode because the module failed to establish the link.
7. In this latter case, and if the module has encountered no customer-inflicted damage, then request an RMA for the module.

===== end of procedure =====

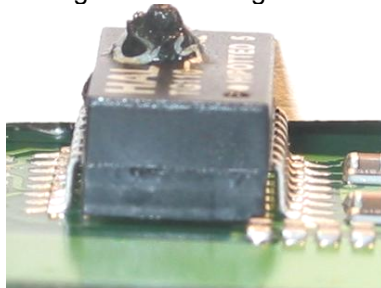
32.5.7 Module Does Not Power Up

To troubleshoot the failure of a module to power up, perform the following steps.

Procedure 50: Troubleshooting failure to power up

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. Verify that the cable is wired and pinned out according to the specifications provided under [Wiring Connectors](#) on Page 185.
4. Remove the cover of the module to expose the components on the printed wiring board.
5. Find the Ethernet transformer, which is labeled with either the name Halo or the name Pulse.

6. Verify that the Ethernet transformer does not show damage that would have been caused by improper cabling. (You can recognize damage as the top of the transformer being no longer smooth. The transformer in the following picture is damaged and is ineligible for an RMA.)



7. Connect the power supply to a known good module via a known good Ethernet cable.
8. Attempt to power up the known good module and
 - if the known good module fails to power up, request an RMA for the power supply.
 - if the known good module powers up, return to the module that does not power up.
9. Reconnect the power supply to the failing module.
10. Connect the power supply to a power source.
11. Verify that the red LED labeled PWR lights.
12. If this LED *does not* light, and the module has not been powered up since the last previous FPGA firmware upgrade was performed on the module, then request an RMA for the module.

===== end of procedure =====

32.5.8 Power Supply Does Not Produce Power

To troubleshoot the failure of a power supply to produce power, perform the following steps.

Procedure 51: Troubleshooting failure of power supply to produce power

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. Verify that the cable is wired and pinned out according to the specifications provided under [Wiring Connectors](#) on Page 185.
4. Connect the power supply to a known good module via a known good Ethernet cable.
5. Attempt to power up the known good module.
6. If the known good module fails to power up, request an RMA for the power supply.

===== end of procedure =====

32.5.9 CMM Does Not Pass Proper GPS Sync to Connected Modules

If the Event Log tabs in all connected modules contain `Loss of GPS Sync Pulse` messages, perform the following steps.

Procedure 52: Troubleshooting CMM not passing sync

1. Verify that the GPS antenna has an unobstructed view of the entire horizon.
2. Verify that the GPS coaxial cable meets specifications.
3. Verify that the GPS sync cable meets specifications for wiring and length.
4. If the web pages of connected modules indicate any of the following, then find and eliminate the source of noise that is being coupled into the GPS sync cable:
 - In the GPS Status page
 - anomalous number of **Satellites Tracked** (greater than 12, for example)
 - incorrect reported **Latitude** and/or **Longitude** of the antenna
 - In the Event Log page
 - garbled GPS messages
 - large number of `Acquired GPS Sync Pulse` messages
5. If these efforts fail to resolve the problem, then request an RMA for the CMM.

===== end of procedure =====

32.5.10 Module Software Cannot be Upgraded

If your attempt to upgrade the software of a module fails, perform the following steps.

Procedure 53: Troubleshooting an unsuccessful software upgrade

1. Download the latest issue of the target release and the associated release notes.
2. Compare the files used in the failed attempt to the newly downloaded software.
3. Compare the procedure used in the failed attempt to the procedure in the newly downloaded release notes.
4. If these comparisons reveal a difference, retry the upgrade, this time with the newer file or newer procedure.
5. If, during attempts to upgrade the FPGA firmware, the following message is repeatable, then request an RMA for the module:

Error code 6, unrecognized device

===== end of procedure =====

32.5.11 Module Functions Properly, Except Web Interface Became Inaccessible

If a module continues to pass traffic, and the telnet and SNMP interfaces to the module continue to function, but the web interface to the module does not display, perform the following steps.

Procedure 54: Restoring the web interface to a module

1. Enter `telnet DottedIPAddress`.
RESULT: A telnet session to the module is invoked.
2. At the `Login` prompt, enter `root`.

3. At the Password prompt, enter *PasswordIfConfigured*.
4. At the Telnet +> prompt, enter **reset**.
RESULT: The web interface is accessible again, and this telnet connection is closed.

===== end of procedure =====

33 OBTAINING TECHNICAL SUPPORT



NOTE:

Do not clear the Event Log after you encounter issues. The information in it may be useful to support the investigation of the problem.

Here is the escalation path for resolution of a problem:

1. Check documentation:
 - This document.
 - Recent Software Release Notes, available at <http://motorola.wirelessbroandsupport.com/software/>
2. Consider checking the Community Forum at <http://motorola.wirelessbroandsupport.com/support/community/>
3. Consider checking the Knowledge Base at <http://motorola.wirelessbroandsupport.com/support/knowledge/>
4. Escalate the problem to your Motorola supplier or reseller.
5. Escalate the problem to Technical Support or other designated Tier 3 technical support:

Country or Region		Phone	Email
NA	USA	+1 866-961-9288	EMS-EICC-RM@motorola.com
	Canada		
EMEA	Denmark	043682114	EMS-EICC-RM@motorola.com
	France	0157323434	
	Germany	06950070204	
	Italy	0291483230	
	Lithuania	880 030 828	
	Netherlands	0202061404	
	Norway	24159815	
	Portugal	0217616160	
	Spain	0912754787	
	Russia	810 800 228 41044	
	Saudi Arabia	800 844 5345	
	South Africa	0800981900	
	United Kingdom	0203 0277499	
All other EMEA	+420 533 336 946		

Country or Region		Phone	Email
LACA	Argentina	0800-666-2789	EMS-EICC-RM@motorola.com
	Brazil	0800-891-4360	
	Columbia	01-800-912-0557	
	Mexico	001-800-942-7721	
	Peru	0800-70-086	
	All other LACA	+420 533 336 946	
APAC	APAC	+6048503854 9am – 5pm Malaysia time	WiBBSupport.apac@motorola.com
		+420 533 336 946 outside hours	

When you send e-mail or call, please include, as appropriate, software release on each module, IP addresses, MAC addresses, and features enabled, like NAT, VLAN, high priority channel, or CIR. You may be asked to run the Support Tool on CNUT or Prizm to provide a complete network picture.

34 GETTING WARRANTY ASSISTANCE

For warranty assistance, contact your reseller or distributor for the process.

REFERENCE INFORMATION

35 ADMINISTERING MODULES THROUGH TELNET INTERFACE

The telnet administrative interface to a module supports the commands that are defined in [Table 71](#). (Many of these are not needed with CNUT.)

Table 71: Supported telnet commands for module administration

Command	System help Definition	Notes
addwebfile	Add a custom web file	Syntax: addwebfile filename . Copies the custom web file <i>filename</i> to non-volatile memory.
burnfile	Burn flash from file	Syntax: burnfile filename . Updates the CPU firmware with a new image. User the image contained in <i>filename</i> if <i>filename</i> is provided. If provided, <i>filename</i> must match the module type (for example, <i>SMboot.bin</i> for a Subscriber Module or <i>APboot.bin</i> for an Access Point Module).
cat	Concatenate and display.	Syntax: cat filename . Displays the contents of <i>filename</i> .
clearsyslog	Clear the system event log	Syntax: clearsyslog . Clears the system event log.
clearwebfile	Clear all custom web files	Syntax: clearwebfile . Deletes all <i>custom</i> web files.
exit	Exit from telnet session	Syntax: exit . Terminates the telnet interface session.
fpga_conf	Update FPGA program	Syntax: fpga_conf . Forces a module to perform a hard (FPGA and CPU) reset. (See reset .)
ftp	File transfer application	Syntax: ftp . Launches the ftp client application on the module.
help	Display command line function help	Syntax: help . Displays a list of available telnet commands and a brief description of each.
jbi	Update FPGA program	Syntax: jbi -aprogram file.jbc . Updates the FPGA firmware with the new image contained in <i>file.jbc</i> .
ls	List the contents of a directory	Syntax: ls . Lists the file names of all files in the directory. Syntax: ls -l . Displays additional information, such as the sizes and dates of the files.

Command	System help Definition	Notes
lsweb	List Flash Web files	Syntax: lsweb . Lists the file names of the saved custom web files.
ping ¹⁰	Send ICMP ECHO_REQUEST packets to network hosts	Syntax: ping IPaddress . Sends an ICMP ECHO_REQUEST to <i>IPaddress</i> and waits for a response. If a response is received, the system returns <i>IPaddress is alive</i> . If no response is received, the system returns no answer from <i>IPaddress</i> .
reset	Reboot the unit	Syntax: reset . Forces the module to perform a hard (FPGA and CPU) module reset. (See fpga_conf .)
rm	Remove (unlink) files	Syntax: rm filename . Remove <i>filename</i> .
syslog	Display system event log: syslog <optional filename>	Syntax: syslog . Displays the contents of the system log. Syntax: syslog filename . Saves the contents of the system log to <i>filename</i> . Caution: overwrites <i>filename</i> if it already exists.
telnet	Telnet application	Syntax: telnet hostIPaddress . Launches the telnet client application on the module.
tftp	tftp application	Syntax: tftp hostIPaddress . Launches the tftp client application on the module.
update	Enable automatic SM code updating	Syntax: update actionlist.txt . Enables the automated update procedure that <i>actionlist.txt</i> specifies. (Supported for only the Access Point Module.)
updateoff	Disable automatic SM code updating	Syntax: updateoff . Disables the automated update procedure.
version	Display the software version string	Syntax: version . Displays the module version string, which contains the software/firmware/hardware versions, the module type, and the operating frequency.

¹⁰ See [Module Has Lost or Does Not Establish Connectivity](#) on Page 481.

36 REGULATORY AND LEGAL NOTICES

36.1 IMPORTANT NOTE ON MODIFICATIONS

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

36.2 NATIONAL AND REGIONAL REGULATORY NOTICES

36.2.1 U.S. Federal Communication Commission (FCC) Notification

This device complies with Part 15 of the US FCC Rules and Regulations. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the US FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

FCC IDs and the specific configurations covered are listed in [Table 72](#).

Table 72: US FCC IDs and Industry Canada certification numbers and covered configurations

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna, Lens, or Reflector	Maximum Allowed Transmitter Output Power
ABZ89FC5809	109W-9000	8 MHz channels, centered on 906-924 MHz in 1 MHz increments (within the 902-928 MHz ISM band)	9000 SM, AP	12 dBi integrated antenna	24 dBm (250 mW)
				10 dBi Maxrad Model # Z1681 (MP9027XFPT or Motorola AN900A) flat panel	26 dBm (390 mW)
				10 dBi Mars Model # MA-IS91-T2, flat panel	26 dBm (390 mW)
				10 dBi MTI Model # MT-2630003/N (MT-263003/N) flat panel	26 dBm (390 mW)
			17 dBi Last Mile Gear Cyclone 900-17H Yagi	18 dBm (63 mW)	
			9000 Indoor SM	8 dBi integrated antenna (Indoor SM)	26 dBm (390 mW)
ABZ89FC5808	109W-2400	20 MHz channels, centered on 2415-2457.5 MHz in 2.5 MHz increments (within the 2400-2483.5 MHz ISM band)	2400 BH, SM, AP	8 dBi internal	28 dBm (630 mW)
			2400 BH, SM	8 dBi internal + 11 dB reflector	25 dBm (340 mW)
ABZ89FC3789	109W-5200	20 MHz channels, centered on 5275-5325 MHz in 5 MHz increments (within the 5250-5350 MHz U-NII band)	5200 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5200 BH SM, AP, only P10 Modules	7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm (25 mW)
ABZ89FC5807	109W-5210	20 MHz channels, centered on 5275-5325 MHz in 5 MHz increments (within the 5250-5350 MHz U-NII band)	5210 BH	7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna, Lens, or Reflector	Maximum Allowed Transmitter Output Power
ABZ89FT7623	none	20 MHz channels, centered on 5495-5705 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band)	5400 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
				7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm (25 mW)
none	109W-5400	20 MHz channels, centered on 5495-5575 and 5675-5705 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band with 5600-5650 MHz excluded)	5400 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
				7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm (25 mW)
ABZ89FC5804	109W-5700	20 MHz channels, centered on 5735-5840 MHz in 5 MHz increments (within the 5725-5850 MHz ISM band)	5700 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5700 BH, SM	7 dBi internal + 18 dB reflector	23 dBm (200 mW)
				7 dBi internal + 10 dB lens	23 dBm (200 mW)
			5700 AP	7 dBi internal + 10 dB lens	19 dBm (80 mW)
ABZ89FT7629	none	10 MHz channels, centered on 5476-5719 in 0.5 MHz increments (within the 5470-5725 MHz U-NII band)	5440 AP	17 dBi connectorized antenna (60° x 5° 3 dB beam width)	10 dBm (10 mW)
			5440 SM	17 dBi integrated antenna (18° x 18° 3 dB beam width)	10 dBm (10 mW)

36.2.2 Industry Canada (IC) Notification

This device complies with RSS-210 of Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Users should be cautioned to take note that in Canada high power radars are allocated as primary users (meaning they have priority) of 5250 – 5350 MHz and 5650 – 5850 MHz

and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to RSS-210 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

To reduce potential radio interference to other users, the antenna type and its gain should be chosen so its Equivalent Isotropic Radiated Power (EIRP) is not more than that permitted for successful communication.

Industry Canada Certification Numbers and the specific configurations covered are listed in [Table 72](#).

This device has been designed to operate with the antennas listed in [Table 72](#) and having a maximum gain as shown in [Table 72](#). Antennas not included or having a gain greater than as shown in [Table 72](#) are strictly prohibited from use with this device. Required antenna impedance is 50 ohms.

36.2.3 Regulatory Requirements for CEPT Member States (www.cept.org)

When operated in accordance with the instructions for use, Motorola Canopy Wireless equipment operating in the 2.4 and 5.4 GHz bands is compliant with CEPT Recommendation 70-03 Annex 3 for Wideband Data Transmission and HIPERLANs. For compliant operation in the 2.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 100mW (20dBm). For compliant operation in the 5.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 1 W (30 dBm).

The following countries have completely implemented CEPT Recommendation 70-03 Annex 3A (2.4 GHz band):


- EU & EFTA countries: Austria, Belgium, Denmark, Spain, Finland, Germany, Greece, Iceland, Italy, Ireland, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Switzerland, Sweden, UK
- New EU member states: Bulgaria, Czech Republic, Cyprus, Estonia, Hungary, Lithuania, Latvia, Malta, Poland, Slovenia, Slovakia
- Other non-EU & EFTA countries: Bosnia and Herzegovina, Turkey


The following countries have a limited implementation of CEPT Recommendation 70-03 Annex 3A:

- France – Outdoor operation at 100mW is only permitted in the frequency band 2400 to 2454 MHz;
 - Any outdoor operation in the band 2454 to 2483.5MHz shall not exceed 10mW (10dBm);


- Indoor operation at 100mW (20dBm) is permitted across the band 2400 to 2483.5 MHz
- o French Overseas Territories:
 - Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte – 100mW indoor & outdoor is allowed
 - Réunion and Guyana – 100mW indoor, no operation outdoor in the band 2400 to 2420MHz
- o Italy – If used outside own premises, general authorization required
- o Luxembourg - General authorization required for public service
- o Romania – Individual license required. T/R 22-06 not implemented


Motorola Canopy Radios operating in the 2400 to 2483.5MHz band are categorized as

“Class 2” devices within the EU and are marked with the class identifier symbol , denoting that national restrictions apply (for example, France). The French restriction in the 2.4 GHz band will be removed in 2011.

This 2.4 GHz equipment is “CE” marked  to show compliance with the European Radio & Telecommunications Terminal Equipment (R&TTE) directive 1999/5/EC. The relevant Declaration of Conformity can be found at <http://motorola.canopywireless.com/doc.php>.

Where necessary, the end user is responsible for obtaining any National licenses required to operate this product and these must be obtained before using the product in any particular country. However, for CEPT member states, 2.4 GHz Wideband Data Transmission equipment has been designated exempt from individual licensing under decision ERC/DEC(01)07. For EU member states, RLAN equipment in both the 2.4 & 5.4GHz bands is exempt from individual licensing under Commission Recommendation 2003/203/EC. Contact the appropriate national administrations for details on the conditions of use for the bands in question and any exceptions that might apply. Also see www.ero.dk for further information.

Motorola Canopy Radio equipment operating in the 5470 to 5725 MHz band are categorized as “Class 1” devices within the EU in accordance with ECC DEC(04)08 and are “CE” marked  to show compliance with the European Radio & Telecommunications Terminal Equipment (R&TTE) directive 1999/5/EC. The relevant Declaration of Conformity can be found at <http://motorola.canopywireless.com/doc.php>.

A European Commission decision, implemented by Member States on 31 October 2005, makes the frequency band 5470-5725 MHz available in all EU Member States for wireless access systems. Under this decision, the designation of Canopy 5.4GHz products become “Class 1 devices” and these do not require notification under article 6, section 4 of the R&TTE Directive. Consequently, these 5.4GHz products are only marked with the  symbol and may be used in any member state.

For further details, see

http://europa.eu.int/information_society/policy/radio_spectrum/ref_documents/index_en.htm

36.2.4 European Union Notification for 5.7 GHz Product

The 5.7 GHz connectorized product is a two-way radio transceiver suitable for use in Broadband Wireless Access System (WAS), Radio Local Area Network (RLAN), or Fixed Wireless Access (FWA) systems. It is a Class 2 device and uses operating frequencies

that are not harmonized throughout the EU member states. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country.

This equipment is marked **CE 0977** to show compliance with the European R&TTE directive 1999/5/EC.

The relevant Declaration of Conformity can be found at <http://www.canopywireless.com/doc.php>.

36.2.5 Equipment Disposal



**Waste
(Disposal)
of Electronic
and Electric
Equipment**

Please do not dispose of Electronic and Electric Equipment or Electronic and Electric Accessories with your household waste. In some countries or regions, collection systems have been set up to handle waste of electrical and electronic equipment. In European Union countries, please contact your local equipment supplier representative or service center for information about the waste collection system in your country.

36.2.6 EU Declaration of Conformity for RoHS Compliance

Motorola hereby, declares that these Motorola products are in compliance with the essential requirements and other relevant provisions of Directive 2002/95/EC, Restriction of the use of certain Hazardous Substances (RoHS) in electrical and electronic equipment.

The relevant Declaration of Conformity can be found at <http://www.canopywireless.com/doc.php>.

36.2.7 UK Notification

The 5.7 GHz connectorized product has been notified for operation in the UK, and when operated in accordance with instructions for use it is compliant with UK Interface Requirement IR2007. For UK use, installations must conform to the requirements of IR2007 in terms of EIRP spectral density against elevation profile above the local horizon in order to protect Fixed Satellite Services. The frequency range 5795-5815 MHz is assigned to Road Transport & Traffic Telematics (RTTT) in the U.K. and shall not be used by FWA systems in order to protect RTTT devices. UK licensing specifies that radiolocation services shall be protected by a Dynamic Frequency Selection (DFS) mechanism to prevent co-channel operation in the presence of radar signals.

36.2.8 Belgium Notification

Belgium national restrictions in the 2.4 GHz band include

- EIRP must be lower than 100 mW
- For crossing the public domain over a distance > 300m the user must have the authorization of the BIPT.
- No duplex working

36.2.9 Luxembourg Notification

For the 2.4 GHz band, point-to-point or point-to-multipoint operation is only allowed on campus areas. 5.4GHz products can only be used for mobile services.

36.2.10 Czech Republic Notification

2.4 GHz products can be operated in accordance with the Czech General License No. GL-12/R/2000.

5.4 GHz products can be operated in accordance with the Czech General License No. GL-30/R/2000.

36.2.11 Norway Notification

Use of the frequency bands 5725-5795 / 5815-5850 MHz are authorized with maximum radiated power of 4 W EIRP and maximum spectral power density of 200 mW/MHz. The radio equipment shall implement Dynamic Frequency Selection (DFS) as defined in Annex 1 of ITU-R Recommendation M.1652 / EN 301 893. Directional antennae with a gain up to 23 dBi may be used for fixed point-to-point links. The power flux density at the border between Norway and neighboring states shall not exceed -122.5 dBW/m^2 measured with a reference bandwidth of 1 MHz.

Canopy 5.7 GHz connectorized products have been notified for use in Norway and are compliant when configured to meet the above National requirements. Users shall ensure that DFS functionality is enabled, maximum EIRP respected for a 20 MHz channel, and that channel spacings comply with the allocated frequency band to protect Road Transport and Traffic Telematics services (for example, 5735, 5755, 5775 or 5835 MHz are suitable carrier frequencies). Note that for directional fixed links, TPC is not required, conducted transmit power shall not exceed 30 dBm, and antenna gain is restricted to 23 dBi (maximum of 40W from the Canopy 5.7 GHz connectorized products).

36.2.12 Greece Notification

The outdoor use of 5470-5725MHz is under license of EETT but is being harmonized according to the CEPT Decision ECC/DEC/(04) 08, of 9th July. End users are advised to contact the EETT to determine the latest position and obtain any appropriate licenses.

36.2.13 Brazil Notification

Local regulations do not allow the use of 900 MHz, 2.4 GHz, or 5.2 GHz Canopy modules in Brazil.

For compliant operation of an AP in the 5.7 GHz band, the Equivalent Isotropic Radiated Power from the built-in patch antenna and any associated reflector dish or LENS shall not exceed 36 dBm (4 W). When using the passive reflector (18 dB), transmitter output power must be configured no higher than 11 dBm. When using the LENS (10 dB at 5.7 GHz), transmitter output power must be configured no higher than 19 dBm.

For compliant operation in the 5.4 GHz band, the Equivalent Isotropic Radiated Power from the built-in patch antenna and any associated reflector dish or LENS shall not exceed 30 dBm (1 W). When using the passive reflector (18 dB), transmitter output power must be configured no higher than 5 dBm. When using the LENS (9 dB at 5.4 GHz), transmitter output power must be configured no higher than 14 dBm. When not using the passive reflector or the LENS, the transmitter output power of the radio must be configured no higher than 23 dBm.

The operator is responsible for enabling the DFS feature on any Canopy 5.4 GHz radio by setting the Region Code to “Brazil”, including after the module is reset to factory defaults.

Important Note: This equipment operates as a secondary application, so it has no rights against harmful interference, even if generated by similar equipment, and cannot cause harmful interference on systems operating as primary applications.

36.2.14 Australia Notification

900 MHz modules must be set to transmit and receive only on center channels of 920, 922, or 923 MHz so as to stay within the ACMA approved band of 915 MHz to 928 MHz for the class license and not interfere with other approved users.

After taking into account antenna gain (in dBi), 900 MHz modules’ transmitter output power (in dBm) must be set to stay within the legal regulatory limit of 30 dBm (1 W) EIRP for this 900 MHz frequency band.

36.2.15 Labeling and Disclosure Table for China

The People’s Republic of China requires that Motorola’s products comply with China Management Methods (CMM) environmental regulations. (China Management Methods refers to the regulation *Management Methods for Controlling Pollution by Electronic Information Products*.) Two items are used to demonstrate compliance; the label and the disclosure table.

The label is placed in a customer visible position on the product.

- Logo 1 means that the product contains no substances in excess of the maximum concentration value for materials identified in the China Management Methods regulation.
- Logo 2 means that the product may contain substances in excess of the maximum concentration value for materials identified in the China Management Methods regulation, and has an Environmental Friendly Use Period (EFUP) in years, fifty years in the example shown.



The Environmental Friendly Use Period (EFUP) is the period (in years) during which the Toxic and Hazardous Substances (T&HS) contained in the Electronic Information Product (EIP) will not leak or mutate causing environmental pollution or bodily injury from the use of the EIP. The EFUP indicated by the Logo 2 label applies to a product and all its parts. Certain field-replaceable parts, such as battery modules, can have a different EFUP and are marked separately.

The Disclosure Table is intended only to communicate compliance with China requirements; it is not intended to communicate compliance with EU RoHS or any other environmental requirements.

Table 73: Disclosure Table for China

部件名称	有毒有害物 或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr ⁶⁺)	多溴苯 (PBB)	多溴二苯 (PBDE)
金属部件	×	○	×	×	○	○
路模	×	○	×	×	○	○
及件	×	○	×	×	○	○
塑料和聚合物部件	○	○	○	○	○	×

表示有毒有害物在部件所有均材料中的含量均在SJ/T11363-2006 准 定的限量要求以下。

表示有毒有害物至少在部件的某一均材料中的含量超出SJ/T11363-2006 准 定的限量要求。

36.3 RF EXPOSURE

For important information on RF exposure and separation distances see Section [15.1, Exposure Separation Distances](#), on Page [173](#).

36.4 LEGAL NOTICES

36.4.1 Software License Terms and Conditions

ONLY OPEN THE PACKAGE, OR USE THE SOFTWARE AND RELATED PRODUCT IF YOU ACCEPT THE TERMS OF THIS LICENSE. BY BREAKING THE SEAL ON THIS DISK KIT / CDROM, OR IF YOU USE THE SOFTWARE OR RELATED PRODUCT, YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SOFTWARE OR RELATED PRODUCT; INSTEAD, RETURN THE SOFTWARE TO PLACE OF PURCHASE FOR A FULL REFUND. THE FOLLOWING AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR ENTITY), AND MOTOROLA, INC. (FOR ITSELF AND ITS LICENSORS). THE RIGHT TO USE THIS PRODUCT IS LICENSED ONLY ON THE CONDITION THAT YOU AGREE TO THE FOLLOWING TERMS.

Now, therefore, in consideration of the promises and mutual obligations contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby mutually acknowledged, you and Motorola agree as follows:

Grant of License. Subject to the following terms and conditions, Motorola, Inc., grants to you a personal, revocable, non-assignable, non-transferable, non-exclusive and limited license to use on a single piece of equipment only one copy of the software contained on this disk (which may have been pre-loaded on the equipment)(Software). You may make two copies of the Software, but only for backup, archival, or disaster recovery purposes. On any copy you make of the Software, you must reproduce and include the copyright and other proprietary rights notice contained on the copy we have furnished you of the Software.

Ownership. Motorola (or its supplier) retains all title, ownership and intellectual property rights to the Software and any copies,

including translations, compilations, derivative works (including images) partial copies and portions of updated works. The Software is Motorola's (or its supplier's) confidential proprietary information. This Software License Agreement does not convey to you any interest in or to the Software, but only a limited right of use. You agree not to disclose it or make it available to anyone without Motorola's written authorization. You will exercise no less than reasonable care to protect the Software from unauthorized disclosure. You agree not to disassemble, decompile or reverse engineer, or create derivative works of the Software, except and only to the extent that such activity is expressly permitted by applicable law.

Termination. This License is effective until terminated. This License will terminate immediately without notice from Motorola or judicial resolution if you fail to comply with any provision of this License. Upon such termination you must destroy the Software, all accompanying written materials and all copies thereof, and the sections entitled Limited Warranty, Limitation of Remedies and Damages, and General will survive any termination.

Limited Warranty. Motorola warrants for a period of ninety (90) days from Motorola's or its customer's shipment of the Software to you that (i) the disk(s) on which the Software is recorded will be free from defects in materials and workmanship under normal use and (ii) the Software, under normal use, will perform substantially in accordance with Motorola's published specifications for that release level of the Software. The written materials are provided "AS IS" and without warranty of any kind. Motorola's entire liability and your sole and exclusive remedy for any breach of the foregoing limited warranty will be, at Motorola's option, replacement of the disk(s), provision of downloadable patch or replacement code, or refund of the unused portion of your bargained for contractual benefit up to the amount paid for this Software License.

THIS LIMITED WARRANTY IS THE ONLY WARRANTY PROVIDED BY MOTOROLA, AND MOTOROLA AND ITS LICENSORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. MOTOROLA DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN REPRESENTATIONS MADE BY MOTOROLA OR AN AGENT THEREOF SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. MOTOROLA DOES NOT WARRANT ANY SOFTWARE THAT HAS BEEN OPERATED IN EXCESS OF SPECIFICATIONS, DAMAGED, MISUSED, NEGLECTED, OR IMPROPERLY INSTALLED. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Limitation of Remedies and Damages. Regardless of whether any remedy set forth herein fails of its essential purpose, IN NO EVENT SHALL MOTOROLA OR ANY OF THE LICENSORS, DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES OF THE FOREGOING BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL OR SIMILAR DAMAGES WHATSOEVER (including, without limitation, damages for loss of business profits, business interruption, loss of business information and the like), whether foreseeable or unforeseeable, arising out of the use or inability to use the Software or accompanying written materials, regardless of the basis of the claim and even if Motorola or a Motorola representative has been advised of the possibility of such damage. Motorola's liability to you for direct damages for any cause whatsoever, regardless of the basis of the form of the action, will be limited to the price paid for the Software that caused the damages. THIS LIMITATION WILL NOT APPLY IN CASE OF PERSONAL INJURY ONLY WHERE AND TO THE EXTENT THAT APPLICABLE LAW REQUIRES SUCH LIABILITY. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Maintenance and Support. Motorola shall not be responsible for maintenance or support of the software. By accepting the license granted under this agreement, you agree that Motorola will be under no obligation to provide any support, maintenance or service in connection with the Software

or any application developed by you. Any maintenance and support of the Related Product will be provided under the terms of the agreement for the Related Product.

Transfer. In the case of software designed to operate on Motorola equipment, you may not transfer the Software to another party except: (1) if you are an end-user, when you are transferring the Software together with the Motorola equipment on which it operates; or 2) if you are a Motorola licensed distributor, when you are transferring the Software either together with such Motorola equipment or are transferring the Software as a licensed duty paid for upgrade, update, patch, new release, enhancement or replacement of a prior version of the Software. If you are a Motorola licensed distributor, when you are transferring the Software as permitted herein, you agree to transfer the Software with a license agreement having terms and conditions no less restrictive than those contained herein. You may transfer all other Software, not otherwise having an agreed restriction on transfer, to another party. However, all such transfers of Software are strictly subject to the conditions precedent that the other party agrees to accept the terms and conditions of this License, and you destroy any copy of the Software you do not transfer to that party. You may not sublicense or otherwise transfer, rent or lease the Software without our written consent. You may not transfer the Software in violation of any laws, regulations, export controls or economic sanctions imposed by the US Government.

Right to Audit. Motorola shall have the right to audit annually, upon reasonable advance notice and during normal business hours, your records and accounts to determine compliance with the terms of this Agreement.

Export Controls. You specifically acknowledge that the software may be subject to United States and other country export control laws. You shall comply strictly with all requirements of all applicable export control laws and regulations with respect to all such software and materials.

US Government Users. If you are a US Government user, then the Software is provided with "RESTRICTED RIGHTS" as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at FAR 52 227-19 or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, as applicable.

Disputes. You and Motorola hereby agree that any dispute, controversy or claim, except for any dispute, controversy or claim involving intellectual property, prior to initiation of any formal legal process, will be submitted for non-binding mediation, prior to initiation of any formal legal process. Cost of mediation will be shared equally. Nothing in this Section will prevent either party from resorting to judicial proceedings, if (i) good faith efforts to resolve the dispute under these procedures have been unsuccessful, (ii) the dispute, claim or controversy involves intellectual property, or (iii) interim relief from a court is necessary to prevent serious and irreparable injury to that party or to others.

General. Illinois law governs this license. The terms of this license are supplemental to any written agreement executed by both parties regarding this subject and the Software Motorola is to license you under it, and supersedes all previous oral or written communications between us regarding the subject except for such executed agreement. It may not be modified or waived except in writing and signed by an officer or other authorized representative of each party. If any provision is held invalid, all other provisions shall remain valid, unless such invalidity would frustrate the purpose of our agreement. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent action in the event of future breaches.

36.4.2 Hardware Warranty in U.S.

Motorola U.S. offers a warranty covering a period of one year from the date of purchase by the customer. If a product is found defective during the warranty period, Motorola will repair or replace the product with the same or a similar model, which may be a reconditioned unit, without charge for parts or labor.

36.4.3 Limit of Liability

IN NO EVENT SHALL MOTOROLA BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT

(INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.) IN NO CASE SHALL MOTOROLA'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

37 ADDITIONAL RESOURCES

Motorola provides two additional resources where you can raise questions and find answers:

- Community Forums at <http://motorola.wirelessbroadbandsupport.com/support/community/>.
This resource facilitates communication with other users and with authorized Canopy experts. Available forums include General Discussion, Network Monitoring Tools, and Suggestions.
- Canopy Knowledge Base at <http://motorola.wirelessbroadbandsupport.com/support/knowledge/>.
This resource facilitates exploration and searches, provides recommendations, and describes tools. Available categories include
 - General (Answers to general questions provide an overview of the Canopy system.)
 - Product Alerts
 - Helpful Hints
 - FAQs (frequently asked questions)
 - Hardware Support
 - Software Support
 - Tools

38 HISTORY OF DOCUMENTATION

This section is a placeholder where changes for this document will be listed.

GLOSSARY

~.	The command that terminates an SSH Secure Shell session to another server. Used on the Bandwidth and Authentication Manager (BAM) master server in the database replication setup.
10Base-T	Technology in Ethernet communications that can deliver 10 Mb of data across 328 feet (100 meters) of CAT 5 cable.
100Base-TX	Technology in Ethernet communications that can deliver 100 Mb of data across 328 feet (100 meters) of CAT 5 cable.
169.254.0.0	Gateway IP address default in Motorola fixed wireless broadband IP network modules.
169.254.1.1	IP address default in Motorola fixed wireless broadband IP network modules.
169.254.x.x	IP address default in Microsoft and Apple operating systems without a DHCP (Dynamic Host Configuration Protocol) server.
255.255.0.0	Subnet mask default in Motorola fixed wireless broadband IP network modules and in Microsoft and Apple operating systems.
802.3	An IEEE standard that defines the contents of frames that are transferred through Ethernet connections. Each of these frames contains a preamble, the address to which the frame is sent, the address that sends the frame, the length of the data to expect, the data, and a checksum to validate that no contents were lost.
802.11	The IEEE standard for wireless local area networks.
802.15	The IEEE standard for wireless personal area networks.
Access Point Cluster	Two to six Access Point Modules that together distribute network or Internet services to a community of 1,200 or fewer subscribers. Each Access Point Module covers a 60° sector. This cluster covers as much as 360°. Also known as AP cluster.
Access Point Module	Also known as AP. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
ACT/4	Second-from-left LED in the module. In the operating mode, this LED is lit when data activity is present on the Ethernet link. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Activate	To provide feature capability to a module, but not to <i>enable</i> (turn on) the feature in the module. See also Enable.
Address Resolution Protocol	Protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html .

Advanced Encryption Standard (AES)	Over-the-air link option that provides extremely secure wireless connections. Advanced Encryption Standard (AES) uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.
AES	See Advanced Encryption Standard.
Aggregate Throughput	The sum of the throughputs in the uplink and the downlink.
AP	Access Point Module. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
APA	Access Point module address.
Apache	A trademark of Apache Software Foundation, used with permission.
APAS	Access Point Authentication Server. Licensed to authenticate SMs that attempt to register to it. The AP licensed as APAS may or may not have authentication <i>enabled</i> (turned on). See also Activate and Enable.
API	Application programming interface for web services that supports Prizm integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system.
APs MIB	Management Information Base file that defines objects that are specific to the Access Point Module or Backhaul timing master. See also Management Information Base.
ARP	Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html .
ASN.1	Abstract Syntax Notation One language. The format of the text files that compose the Management Information Base.
Attenuation	Reduction of signal strength caused by the travel from the transmitter to the receiver, and caused by any object between. In the absence of objects between, a signal that has a short wavelength experiences a high degree of attenuation nevertheless.
Authentication Key	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f, padded with leading zeroes in Release 4.2.3 and later. This key must be unique to the individual SM.

Backhaul Module	Also known as BH. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module. See also Backhaul Timing Master and Backhaul Timing Slave.
Backhaul Timing Master	Backhaul Module that sends network timing (synchronization) to another Backhaul Module, which serves as the Backhaul timing slave.
Backhaul Timing Slave	Backhaul Module that receives network timing (synchronization) from another Backhaul Module, which serves as the Backhaul timing master.
BAM	Bandwidth and Authentication Manager. The subsystem of Prizm that manages sets of bandwidth, high-priority channel, and VLAN settings individually for registered Subscriber Modules. This software also provides secure Subscriber Module authentication and user-specified encryption keys.
BER	Bit Error Rate. The ratio of incorrect data received to correct data received.
BH	Backhaul Module. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module.
Bit Error Rate	Ratio of incorrect data received to correct data received.
Box MIB	Management Information Base file that defines module-level objects. See also Management Information Base.
BRAID	Stream cipher that the TIA (Telecommunications Industry Association) has standardized. The secret keys in both modules communicate with each other to establish the Data Encryption Standard key. See Data Encryption Standard.
Bridge	Network element that uses the physical address (not the logical address) of another to pass data. The bridge passes the data to either the destination address, if found in the simple routing table, or to all network segments other than the one that transmitted the data. Modules are Layer 2 bridges except that, where NAT is enabled for an SM, the SM is a Layer 3 switch. Compare to Switch and Router, and see also NAT.
Bridge Entry Timeout Field	Value that the operator sets as the maximum interval for no activity with another module, whose MAC address is the Bridge Entry. This interval should be longer than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.
Buckets	Theoretical data repositories that can be filled at preset rates or emptied when preset conditions are experienced, such as when data is transferred.
Burst	Preset amount limit of data that may be continuously transferred.

C/I Ratio	Ratio of intended signal (carrier) to unintended signal (interference) received.
Canopy	A trademark of Motorola, Inc.
Carrier-to-interference Ratio	Ratio of intended reception to unintended reception.
CarSenseLost Field	This field displays how many carrier sense lost errors occurred on the Ethernet controller.
CAT 5 Cable	Cable that delivers Ethernet communications from module to module. Later modules auto-sense whether this cable is wired in a straight-through or crossover scheme.
chkconfig	A command that the Linux [®] operating system accepts to enable MySQL [®] and Apache [™] Server software for various run levels of the mysqld and httpd utilities.
CIR	See Committed Information Rate.
Cluster Management Module	Module that provides power, GPS timing, and networking connections for an AP cluster. Also known as CMM. If this CMM is connected to a Backhaul Module, then this CMM is the central point of connectivity for the entire site.
CMM	Cluster Management Module. A module that provides power, GPS timing, and networking connections for an Access Point cluster. If this CMM is connected to a Backhaul Module (BH), then this CMM is the central point of connectivity for the entire site.
CodePoint	See DiffServ.
Color Code Field	Module parameter that identifies the other modules with which communication is allowed. The range of values is 0 to 255. When set at 0, the Color Code does not restrict communications with any other module.
Committed Information Rate (CIR)	For an SM or specified group of SMs, a level of bandwidth that can be guaranteed to never fall below a specified minimum. In the Motorola implementation, this is controlled by the Low Priority Uplink CIR, Low Priority Downlink CIR, High Priority Uplink CIR, and High Priority Downlink CIR parameters.
Community String Field	Control string that allows a network management station to access MIB information about the module.
CPE	Customer premises equipment.
CRCErrors Field	This field displays how many CRC errors occurred on the Ethernet controller.
CRM	Customer relationship management system.

Data Encryption Standard	Over-the-air link option that uses secret 56-bit keys and 8 parity bits. Data Encryption Standard (DES) performs a series of bit permutations, substitutions, and recombination operations on blocks of data.
Date of Last Transaction	A field in the data that the <code>cmd show esn</code> command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM. Expressed in the database output as DLT.
Dell	A trademark of Dell, Inc.
Demilitarized Zone	Internet Protocol area outside of a firewall. Defined in RFC 2647. See http://www.faqs.org/rfcs/rfc2647.html .
DES	Data Encryption Standard. An over-the-air link option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data.
Desensed	Received an undesired signal that was strong enough to make the module insensitive to the desired signal.
DFS	See Dynamic Frequency Selection.
DHCP	Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the system. See http://www.faqs.org/rfcs/rfc2131.html . See also Static IP Address Assignment.
Diffraction	Partial obstruction of a signal. Typically diffraction attenuates a signal so much that the link is unacceptable. However, in some instances where the obstruction is very close to the receiver, the link may be acceptable.
DiffServ	Differentiated Services, consistent with RFC 2474. A byte in the type of service (TOS) field of packets whose values correlates to the channel on which the packet should be sent. The value is a numeric code point. Motorola modules map each of 64 code points to values of 0 through 7. Three of these code points have fixed values, and the remaining 61 are settable. Values of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities. (However, configuring DiffServ does not automatically enable the VLAN feature.) Among the settable parameters, the values are set in the AP for all downlinks within the sector and in the SM for each uplink.
Disable	To turn off a feature in the module after both the feature activation file has <i>activated</i> the module to use the feature and the operator has <i>enabled</i> the feature in the module. See also Activate and Enable.

DLT	Date of last transaction. A field in the data that the <code>cmd show esn</code> command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM.
DMZ	Demilitarized Zone as defined in RFC 2647. An Internet Protocol area outside of a firewall. See http://www.faqs.org/rfcs/rfc2647.html .
Dynamic Frequency Selection (DFS)	A requirement in certain countries and regions for systems to detect interference from other systems, notably radar systems, and to avoid co-channel operation with these systems. See also Region Code.
Dynamic Host Configuration Protocol	See DHCP.
Electronic Serial Number	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
Element Pack	A license for Prizm management of a multi-point sector and covers the AP and up to 200 SMs or a backhaul link.
Enable	To turn on a feature in the module after the feature activation file has <i>activated</i> the module to use the feature. See also Activate.
Engine	Bandwidth and Authentication Manager (BAM) interface to the AP and SMs. Unique sets of commands are available on this interface to manage parameters and user access. Distinguished from SSE. See also SSE.
ESN	Electronic Serial Number. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
ESN Data Table	Table in which each row identifies data about a single SM. In tab-separated fields, each row stores the ESN, authentication key, and QoS information that apply to the SM. The operator can create and modify this table. This table is both an input to and an output from the Bandwidth and Authentication Manager (BAM) SQL database, and should be identically input to redundant BAM servers.
/etc/services	File that stores telnet ports on the Bandwidth and Authentication Manager (BAM) server.
EthBusErr Field	This field displays how many Ethernet bus errors occurred on the Ethernet controller.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.

Fade Margin	The difference between strength of the received signal and the strength that the receiver requires for maintaining a reliable link. A higher fade margin is characteristic of a more reliable link. Standard operating margin.
FCC	Federal Communications Commission of the U.S.A.
Feature Activation Key	Software key file whose file name includes the ESN of the target module. When installed on the module, this file <i>activates</i> the module to have the feature <i>enabled</i> or disabled in a separate operator action.
Field-programmable Gate Array	Array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.
File Transfer Protocol	Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. Defined in RFC 959. See http://www.faqs.org/rfcs/rfc959.html .
FPGA	Field-programmable Gate Array. An array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.
Frame Spreading	Transmission of a beacon in only frames where the receiver expects a beacon (rather than in every frame). This avoids interference from transmissions that are not intended for the receiver.
Frame Timing Pulse Gated Field	Toggle parameter that prevents or allows the module to continue to propagate GPS sync timing when the module no longer receives the timing.
Free Space Path Loss	Signal attenuation that is naturally caused by atmospheric conditions and by the distance between the antenna and the receiver.
Fresnel Zone	Space in which no object should exist that can attenuate, diffract, or reflect a transmitted signal before the signal reaches the target receiver.
FSK	Frequency Shift Keying, a variation of frequency modulation to transmit data, in which two or more frequencies are used.
FTP	File Transfer Protocol, defined in RFC 959. Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. See http://www.faqs.org/rfcs/rfc959.html .
Global Positioning System	Network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.

GPS/3	Third-from-left LED in the module. In the operating mode for an Access Point Module or Backhaul timing master, this LED is continuously lit as the module receives sync pulse. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
GUI	Graphical user interface.
High-priority Channel	Channel that supports low-latency traffic (such as Voice over IP) over low-latency traffic (such as standard web traffic and file downloads). To recognize the latency tolerance of traffic, this channel reads the IPv4 Type of Service DiffServ Control Point (DSCP) bits. Enabling the high-priority channel reduces the maximum number of SMs that can be served in the sector.
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web. Defined in RFC 2068. See http://www.faqs.org/rfcs/rfc2068.html .
ICMP	Internet Control Message Protocols defined in RFC 792, used to identify Internet Protocol (IP)-level problems and to allow IP links to be tested. See http://www.faqs.org/rfcs/rfc792.html .
indiscards count Field	How many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)
inerrors count Field	How many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
innucastpkts count Field	How many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
inoctets count Field	How many octets were received on the interface, including those that deliver framing information.
Intel	A registered trademark of Intel Corporation.
inucastpkts count Field	How many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
inunknownprotos count Field	How many inbound packets were discarded because of an unknown or unsupported protocol.
IP	Internet Protocol defined in RFC 791. The Network Layer in the TCP/IP protocol stack. This protocol is applied to addressing, routing, and delivering, and re-assembling data packets into the Data Link layer of the protocol stack. See http://www.faqs.org/rfcs/rfc791.html .
IP Address	32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.

IPv4	Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.
ISM	Industrial, Scientific, and Medical Equipment radio frequency band, in the 900-MHz, 2.4-GHz, and 5.8-GHz ranges.
Jitter	Timing-based measure of the reception quality of a link. An acceptable link displays a jitter value between 0 and 4 for a 10-Mbps Backhaul timing slave in Release 4.0 and later, between 0 and 9 for a 20-Mbps Backhaul timing slave, or between 5 and 9 for any Subscriber Module or for a Backhaul timing slave in any earlier release. OFDM modules do not have this parameter.
L2TP over IPSec	Level 2 Tunneling Protocol over IP Security. One of several virtual private network (VPN) implementation schemes. Regardless of whether Subscriber Modules have the Network Address Translation feature (NAT) enabled, they support VPNs that are based on this protocol.
Late Collision Field	This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision. A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.
Latency Tolerance	Acceptable tolerance for delay in the transfer of data to and from a module.
Line of Sight	Wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
Linux	A registered trademark of Linus Torvalds.
LNK/5	Furthest left LED in the module. In the operating mode, this LED is continuously lit when the Ethernet link is present. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Logical Unit ID	Final octet of the 4-octet IP address of the module.
LOS	Line of sight. The wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
LUID	Logical Unit ID. The final octet of the 4-octet IP address of the module.
MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.

Management Information Base	Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
Master	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul module that provides synchronization over the air to another Backhaul module (a Backhaul timing slave) and applies to a Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically copied onto a redundant BAM server (BAM slave). In each case, the master is not a product. Rather, the master is the role that results from deliberate configuration steps.
Maximum Information Rate (MIR)	The cap applied to the bandwidth of an SM or specified group of SMs. In the Motorola implementation, this is controlled by the Sustained Uplink Data Rate, Uplink Burst Allocation, Sustained Downlink Data Rate, and Downlink Burst Allocation parameters.
Media Access Control Address	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
MIB	Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
MIR	See Maximum Information Rate.
MySQL	A registered trademark of MySQL AB Company in the United States, the European Union, and other countries.
mysqladmin	A command to set the administrator and associated password on the Bandwidth and Authentication Manager (BAM) server.
mysql-server	Package group that enables the SQL Database Server application in the Red Hat® Linux® 9 operating system to provide SQL data for Bandwidth and Authentication Manager (BAM) operations.
NAT	Network Address Translation defined in RFC 1631. A scheme that isolates Subscriber Modules from the Internet. See http://www.faqs.org/rfcs/rfc1631.html .
NBI	See Northbound Interface.
NEC	National Electrical Code. The set of national wiring standards that are enforced in the U.S.A.

NetBIOS	Protocol defined in RFC 1001 and RFC 1002 to support an applications programming interface in TCP/IP. This interface allows a computer to transmit and receive data with another host computer on the network. RFC 1001 defines the concepts and methods. RFC 1002 defines the detailed specifications. See http://www.faqs.org/rfcs/rfc1001.html and http://www.faqs.org/rfcs/rfc1002.html .
Network Address Translation	Scheme that defines the Access Point Module as a proxy server to isolate registered Subscriber Modules from the Internet. Defined in RFC 1631. See http://www.faqs.org/rfcs/rfc1631.html .
Network Management Station	See NMS.
NMS	Network Management Station. A monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects). See also Simple Network Management Protocol.
Northbound Interface (NBI)	The interface within Prizm to higher-level systems. This interface consists of a Simple Network Management Protocol (SNMP) agent for integration with a network management system (NMS); a Simple Object Access Protocol (SOAP) XML-based application programming interface (API) for web services that supports integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system; and console automation that allows such higher-level systems to launch and appropriately display the PrizmEMS management console in a custom-developed GUI.
Object	Network variable that is defined in the Management Information Base.
OptiPlex	A trademark of Dell, Inc.
OSS	Operations support system, such as a customer relationship management (CRM), billing, or provisioning system. The application programming interface (API) for Prizm supports integrating Prizm with an OSS.
outdiscards count Field	How many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)
outerrors count Field	How many outbound packets contained errors that prevented their transmission.
outnucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.
outoctets count Field	How many octets were transmitted out of the interface, including those that deliver framing information.

outcastpkts count Field	How many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
Override Plug	Device that enables the operator to regain control of a module that has been locked by the No Remote Access feature, the 802.3 Link Disable feature, or a password or IP address that cannot be recalled. This device can be either fabricated on site or ordered.
Pentium	A registered trademark of Intel Corporation.
php-mysql	Package group that enables the Web Server application in the Red Hat® Linux® 9 operating system to provide data from the SQL Database Server application as PHP in the Bandwidth and Authentication Manager (BAM) GUI.
PMP	See Point-to-Multipoint Protocol.
Point-to-Multipoint Protocol	Defined in RFC 2178, which specifies that data that originates from a central network element can be received by all other network elements, but data that originates from a non-central network element can be received by only the central network element. See http://www.faqs.org/rfcs/rfc2178.html . Also referenced as PMP.
Point-to-Point Protocol	Standards that RFC 1661 defines for data transmittal on the Internet. Also known as PPP or PTP. See http://www.faqs.org/rfcs/rfc1661.html .
Power Control	Feature in Release 4.1 and later that allows the module to operate at less than 18 dB less than full power to reduce self-interference.
PPPoE	Point to Point Protocol over Ethernet. Supported on SMs for <ul style="list-style-type: none">◦ operators who use PPPoE in other parts of their network◦ operators who want to deploy PPPoE to realize per-subscriber authentication, metrics, and usage control.
PPTP	Point to Point Tunneling Protocol. One of several virtual private network implementations. Regardless of whether the Network Address Translation (NAT) feature enabled, Subscriber Modules support VPNs that are based on this protocol.
Prizm	The software product that allows users to partition their entire networks into criteria-based subsets and independently monitor and manage those subsets. Prizm Release 1.0 and later includes a Northbound Interface to higher-level systems. Prizm integrates Bandwidth and Authentication Manager (BAM) functionality.
Protective Earth	Connection to earth (which has a charge of 0 volts). Also known as ground.
Proxy Server	Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer, which has an IP address that is not unique or not registered.

PTMP	See Point-to-Multipoint Protocol.
PTP	See Point-to-Point Protocol.
QoS	Quality of Service. A frame field that Bandwidth and Authentication Manager (BAM) provides to the AP and SM about the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields.
Quality of Service	A frame bit that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields. Also known as QoS.
Quick Start	Interface page that requires minimal configuration for initial module operation.
Radio Signal Strength Indicator	Relative measure of the strength of a received signal. An acceptable link displays an Radio Signal Strength Indicator (RSSI) value of greater than 700.
Random Number	Number that the Bandwidth and Authentication Manager (BAM) generates, invisible to both the SM and the network operator, to send to the SM as a challenge against an authentication attempt.
Reader	A registered trademark of Adobe Systems, Incorporated.
Recharging	Resumed accumulation of data in available data space (buckets). See Buckets.
Red Hat	A registered trademark of Red Hat, Inc.
Reflection	Change of direction and reduction of amplitude of a signal that encounters an object larger than the wavelength. Reflection may cause an additional copy of the wavelength to arrive after the original, unobstructed wavelength arrives. This causes partial cancellation of the signal and may render the link unacceptable. However, in some instances where the direct signal cannot be received, the reflected copy may be received and render an otherwise unacceptable link acceptable.
Region Code	A parameter that offers multiple fixed selections, each of which automatically implements either the Dynamic Frequency Selection (DFS) standard that is required by law or regulatory to apply or no DFS, based on the frequency band range and the selected region.
Registrations MIB	Management Information Base file that defines registrations for global items such as product identities and product components. See also Management Information Base.

repl-m	A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) master server, uses SFTP to copy both the database and the <code>repl-s</code> script to a BAM slave server, and remotely executes the <code>repl-s</code> script on the BAM slave server. See Master, Slave, <code>repl-s</code> , Secure Shell, and SFTP.
repl-s	A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) slave server. See Master, Slave, and <code>repl-m</code> .
RES	Result. A field in the data that the <code>cmd show esn</code> command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server.
RetransLimitExp Field	This field displays how many times the retransmit limit has expired.
RF	Radio frequency. How many times each second a cycle in the antenna occurs, from positive to negative and back to positive amplitude.
RJ-11	Standard cable that is typically used for telephone line or modem connection.
RJ-45	Standard cable that is typically used for Ethernet connection. This cable may be wired as straight-through or as crossover. Later modules auto-sense whether the cable is straight-through or crossover.
Router	Network element that uses the logical (IP) address of another to pass data to only the intended recipient. Compare to Switch and Bridge.
RPM	Red Hat® Package Manager.
rpm	A command that the Linux® operating system accepts to identify the version of Linux® software that operates on the Bandwidth and Authentication Manager (BAM) server.
RSSI	Radio Signal Strength Indicator. A relative measure of the strength of a received signal. An acceptable link displays an RSSI value of greater than 700.
RxBabErr Field	This field displays how many receiver babble errors occurred.
RxOverrun Field	This field displays how many receiver overrun errors occurred on the Ethernet controller.
SDK	<i>PrizmEMS™ Software Development Kit (SDK)</i> —the document that provides server administrator tasks, GUI developer information for console automation that allows higher-level systems to launch and appropriately display the Prizm management console. The SDK also describes the how to define new element types and customize the Details views.
Secure Shell	A trademark of SSH Communications Security.
Self-interference	Interference with a module from another module in the same network.

SES/2	Third-from-right LED in the module. In the Access Point Module and Backhaul timing master, this LED is unused. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Session Key	Software key that the SM and Bandwidth and Authentication Manager (BAM) separately calculate based on that both the authentication key (or the factory-set default key) and the random number. BAM sends the session key to the AP. Neither the subscriber nor the network operator can view this key. See also Random Number.
SFTP	Secure File Transfer Protocol.
Simple Network Management Protocol	Standard that is used for communications between a program (agent) in the network and a network management station (monitor). Defined in RFC 1157. See http://www.ietf.org/rfc/rfc1157.html .
skey	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f. This key must be unique to the individual SM. Also known as authentication key.
Slave	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul slave that receives synchronization over the air from another Backhaul module (a Backhaul timing master) and applies to a redundant Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically overwritten by a copy from the primary BAM server (BAM master). In each case, the slave is not a product. Rather, the slave is the role that results from deliberate configuration steps.
SM	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.
SM MIB	Management Information Base file that defines objects that are specific to the Subscriber Module or Backhaul timing slave. See also Management Information Base.
SNMP	See Simple Network Management Protocol, defined in RFC 1157.
SNMP Trap	Capture of information that informs the network monitor through Simple Network Management Protocol of a monitored occurrence in the module.

SOAP	Simple Object Access Protocol (SOAP). The protocol that the Northbound Interface in Prizm uses to support integration of Prizm with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system
SSE	Bandwidth and Authentication Manager (BAM) interface to the SQL server. Unique sets of commands are available on this interface to manage the BAM SQL database and user access. Distinguished from Engine. See also Engine.
Standard Operating Margin	See Fade Margin.
Static IP Address Assignment	Assignment of Internet Protocol address that can be changed only manually. Thus static IP address assignment requires more configuration time and consumes more of the available IP addresses than DHCP address assignment does. RFC 2050 provides guidelines for the static allocation of IP addresses. See http://www.faqs.org/rfcs/rfc2050.html . See also DHCP.
su -	A command that opens a Linux [®] operating system session for the user root.
Subnet Mask	32-bit binary number that filters an IP address to reveal what part identifies the network and what part identifies the host. The number of subnet mask bits that are set to 1 indicates how many leading bits of the IP address identify the network. The number of subnet mask bits that are set 0 indicate how many trailing bits of the IP address identify the host.
Subscriber Module	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.
Sustained Data Rate	Preset rate limit of data transfer.
Switch	Network element that uses the port that is associated with the physical address of another to pass data to only the intended recipient. Compare to Bridge and Router.
SYN/1	Second-from-right LED in the module. In the Access Point Module or Backhaul timing master, as in a registered Subscriber Module or Backhaul timing slave, this LED is continuously lit to indicate the presence of sync. In the operating mode for a Subscriber Module or Backhaul timing slave, this LED flashes on and to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Sync	GPS (Global Positioning System) absolute time, which is passed from one module to another. Sync enables timing that prevents modules from transmitting or receiving interference. Sync also provides correlative time stamps for troubleshooting efforts.

TCP	Alternatively known as Transmission Control Protocol or Transport Control Protocol. The Transport Layer in the TCP/IP protocol stack. This protocol is applied to assure that data packets arrive at the target network element and to control the flow of data through the Internet. Defined in RFC 793. See http://www.faqs.org/rfcs/rfc793.html .
tcp	Transport Control type of port. The system uses Port 3306:tcp for MySQL [®] database communications, Port 9080:tcp for SSE <code>telnet</code> communications, and Port 9090:tcp for Engine <code>telnet</code> communications.
TDD	Time Division Duplexing. Synchronized data transmission with some time slots allocated to devices transmitting on the uplink and some to the device transmitting on the downlink.
telnet	Utility that allows a client computer to update a server. A firewall can prevent the use of the <code>telnet</code> utility to breach the security of the server. See http://www.faqs.org/rfcs/rfc818.html , http://www.faqs.org/rfcs/rfc854.html and http://www.faqs.org/rfcs/rfc855.html .
Textual Conventions MIB	Management Information Base file that defines system-specific textual conventions. See also Management Information Base.
Time of Last Transaction	A field in the data that the <code>cmd show esn</code> command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM. Expressed in the database output as TLT.
TLT	Time of last transaction. A field in the data that the <code>cmd show esn</code> command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM.
TNAF	Total number of authentication requests failed. A field in the data that the <code>cmd show esn</code> command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate but was denied by BAM.
TNAR	Total number of authentication requests. A field in the data that the <code>cmd show esn</code> command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate, regardless of whether the attempt succeeded.
Tokens	Theoretical amounts of data. See also Buckets.
TOS	8-bit field in that prioritizes data in a IP transmission. See http://www.faqs.org/rfcs/rfc1349.html .

TxUnderrun Field	This field displays how many transmission-underrun errors occurred on the Ethernet controller.
UDP	User Datagram Protocol. A set of Network, Transport, and Session Layer protocols that RFC 768 defines. These protocols include checksum and address information but does not retransmit data or process any errors. See http://www.faqs.org/rfcs/rfc768.html .
udp	User-defined type of port.
U-NII	Unlicensed National Information Infrastructure radio frequency band, in the 5.1-GHz through 5.8-GHz ranges.
VID	VLAN identifier. See also VLAN.
VLAN	Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.
VPN	Virtual private network for communication over a public network. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes is possible. SMs support L2TP over IPsec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs, regardless of whether the Network Address Translation (NAT) feature enabled.