

Canopy™ Access Point Module (AP)

User Manual

AP-UM-en
Issue 5
January 2004

NOTICES

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.

U.S. Federal Communication Commission (FCC) and Industry Canada (IC) Notification

This device complies with part 15 of the U. S. FCC Rules and Regulations and 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. In Canada, users should be cautioned to take note that 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 Part 15 of the U.S. FCC Rules and with 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.

FCC IDs and Industry Canada Certification Numbers are listed in the following table:

Module Types	Frequency Band Range	Maximum Transmitter Power	Reflector	FCC ID	Industry Canada Cert Number
SM AP BH	ISM 2400-2483.5 MHz	340 mW	Allowed on SM and BH	ABZ89FC5808	109W-2400
SM AP BH	U-NII 5250-5350 MHz	200 mW	Not Allowed	ABZ89FC3789	109W-5200
SM BH	U-NII 5250-5350 MHz	3.2 mW	Recommended	ABZ89FC5807	109W-5210
SM AP BH	U-NII 5725-5825 MHz	200 mW	Allowed on SM and BH	ABZ89FC4816	109W-5700
SM AP BH	ISM 5725-5850 MHz	200 mW	Allowed on SM and BH	ABZ89FC5804	109W-5700

The term “IC:” before the radio certification number only signifies that Industry Canada technical specifications were met.

European Community Notification

Notification of Intended Purpose of Product Uses

This product is a two-way radio transceiver suitable for use in Broadband RLAN systems. It uses operating frequencies which are not harmonized through the EC. All licenses must be obtained before using the product in any EC country.

Declaration of conformity:

Motorola declares the GHz radio types listed below comply with the essential requirements and other relevant provisions of Directive 1999/5/EC.

- Relevant Specification
- EN 301 893 or similar - radio spectrum
- EN301489-17 - EMC
- EN60950 – safety



Product Details for Products Tested for Compliance with Relevant EC Directives

Module Type	Frequency Band Range	Maximum Transmitter Power	Effective Isotropic Radiated Power (EIRP)	Modulation Type	Operating Channels	Non-overlapping Channel Spacing
Access Point	5.725 to 5.825 GHz	200 mW RMS	1 Watt EIRP	High Index 2-level FSK	5745 to 5805 MHz in 5-MHz increments	20 MHz
Subscriber Module	5.725 to 5.825 GHz	200 mW RMS	1 Watt EIRP	High Index 2-level FSK	5745 to 5805 MHz in 5-MHz increments	20 MHz
Subscriber Module with Reflector	5.725 to 5.825 GHz	200 mW RMS	63 Watts EIRP	High Index 2-level FSK	5745 to 5805 MHz in 5-MHz increments	20 MHz
Backhaul	5.725 to 5.825 GHz	200 mW RMS	1 Watt EIRP	High Index 2-level or 4-level FSK	5745 to 5805 MHz in 5-MHz increments	20 MHz
Backhaul with Reflector	5.725 to 5.825 GHz	200 mW RMS	63 Watts EIRP	High Index 2-level or 4-level FSK	5745 to 5805 MHz in 5-MHz increments	20 MHz

Canopy can be configured to operate at a range of frequencies, but at this time, only channels from 5745 MHz through 5805 MHz of the 5.7 GHz product have been tested for compliance with relevant EC directives. Before configuring equipment to operate outside this range, please check with your regulator.

Exposure Note

A Canopy module must be installed to provide a separation distance of at least 20 cm (7.9 in) from all persons. When adding the Canopy reflector dish, the reflector dish must be installed to provide a separation distance of at least 1.5m (59.1 in) from all persons. When so installed, the module’s RF field is within Health Canada limits for the general population; consult Safety Code 6, obtainable from Health Canada’s website <http://www.hc-sc.gc.ca/rpb>.

In both configurations the maximum RMS power does not exceed 340mW.

The applicable power density exposure limit is 10 Watt/m², according to the FCC OET Bulletin 65, the ICNIRP guidelines, and the Health Canada Safety Code 6. The corresponding compliance distances referenced above have been determined by assuming worst-case scenarios. The peak power density (*S*) in the far-field of a radio-frequency source with rms transmit power *P* and antenna gain *G* at a distance *d* is

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

In the case of the Canopy SM *without* reflector, the gain is 8 dBi (a factor of 6.3), so the peak power density equals the exposure limit at a distance of 13 cm for 2.4 GHz product and 10 cm for 5.2 and 5.7 GHz product. A power compliance margin of over 2 is artificially introduced by setting the distance to a consistent 20 cm across all modules, giving a power compliance margin of x2.4 for 2.4 GHz modules and x4 for 5.2 and 5.7 GHz modules.

In the case of the Canopy SM *with* reflector, the gain depends on frequency and ranges from 19 dBi (a factor of 80) for 2.4 GHz modules to 26 dBi (a factor of 400) for 5.2 GHz Extended Range and 5.7 GHz modules, so the peak power density equals the exposure limit at a distance of 10 to 80 cm. A power compliance margin is artificially introduced by defining a consistent compliance distance of 1.5 m across all modules with reflectors, giving a power compliance margin of x10 for 2.4 GHz modules, x220 for 5.2 GHz Extended Range modules, and x3.5 for 5.7 GHz modules. The compliance distance is greatly overestimated in this case because the far-field equation neglects the physical dimension of the antenna, which is modeled as a point-source.

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 OF IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. 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 duly 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 U.S. 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.

U.S. Government Users. If you are a U.S. 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.

Hardware Warranty in U.S.A.

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.

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.

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 trademark of Motorola, Inc. All other product or service names are the property of their respective owners.

Motorola, Inc
Broadband Wireless Technology Center
50 East Commerce Drive
Schaumburg, IL 60173
USA

<http://www.motorola.com/canopy>

TABLE OF CONTENTS

1	WELCOME	11
1.1	Feedback.....	11
1.2	Technical Support	11
2	ABOUT THIS DOCUMENT	12
2.1	Intended Use	12
2.2	New in This Issue	12
2.3	Additional Feature Information.....	13
3	SYSTEM OVERVIEW	14
3.1	Module-to-Module Communications	14
3.2	Types of AP Applications	14
3.3	Synchronization.....	16
3.3.1	Unsynchronized Modules	16
3.3.2	Passing Sync.....	16
3.4	Wiring	18
4	ADVANCED FEATURES	19
4.1	Security Features	19
4.1.1	BRAID.....	19
4.1.2	DES Encryption	19
4.1.3	AES Encryption.....	19
4.1.4	AES-DES Operability Comparisons	19
4.2	Bandwidth Management	20
4.2.1	Bandwidth and Authentication Manager (BAM)	20
4.2.2	Recharging Buckets	21
4.2.3	Subscriber Module Perspective.....	21
4.2.4	Interaction of Burst Data and Sustained Data Settings.....	21
4.3	High-Priority Bandwidth.....	22
4.3.1	High Priority Uplink Percentage.....	23
4.3.2	UAcks Reserved High	23
4.3.3	DAcks Reserved High	23
4.3.4	NumCtlSlots Reserved High.....	23
4.3.5	Allocations to Downlink and Uplink.....	23
4.4	Branding	24
4.5	Denying All Remote Access.....	26
4.6	Reinstating Remote Access Capability	26
4.7	SNMP	26
4.7.1	Agent	27
4.7.2	Managed Device.....	27
4.7.3	NMS.....	27
4.7.4	Dual Roles	27
4.7.5	SNMP Commands.....	27
4.7.6	Traps.....	27
4.7.7	MIBS	28
4.7.8	MIB-II	29
4.7.9	Canopy Enterprise MIB	29

4.7.10	Module Parameters for SNMP Implementation.....	30
4.7.11	Objects Defined in the Canopy Enterprise MIB.....	31
4.7.12	Traps Provided in the Canopy Enterprise MIB.....	38
4.7.13	MIB Viewers.....	38
5	SITE PLANNING.....	40
5.1	Specific Mounting Considerations.....	40
5.1.1	Lightning Protection.....	40
5.1.2	Electrical Requirements.....	40
5.2	General RF Considerations.....	41
5.2.1	Vertical Beam Width.....	41
5.2.2	Radio Horizon.....	42
5.2.3	Antenna Downward Tilt.....	43
5.2.4	Fresnel Loss.....	43
5.2.5	Free Space Path Loss.....	45
5.2.6	Loss Due to Foliage.....	47
5.2.7	Carrier-to-Interference Ratio.....	47
5.3	Canopy Component Proliferation.....	48
5.3.1	Subscriber Modules.....	48
5.3.2	Access Point Modules.....	48
5.3.3	Access Point Clusters.....	48
5.4	AP Update of SM Software Release.....	48
5.5	Channel Plans.....	50
5.5.1	Physical Proximity.....	50
5.5.2	Spectrum Analysis.....	50
5.5.3	Power Reduction to Mitigate Interference.....	51
5.5.4	2.4-GHz AP Channels.....	52
5.5.5	5.2-GHz AP Channels.....	53
5.5.6	5.7-GHz AP Channels.....	54
5.5.7	Example Channel Plans for AP Clusters.....	55
5.5.8	Multiple Access Points Clusters.....	57
6	IP NETWORK PLANNING.....	58
6.1	General IP Addressing Concepts.....	58
6.1.1	IP Address.....	58
6.1.2	Subnet Mask.....	58
6.1.3	Example IP Address and Subnet Mask.....	58
6.1.4	Subnet Classes.....	58
6.2	Dynamic or Static Addressing.....	59
6.2.1	When a DHCP Server is Not Found.....	59
6.3	AP Module Address Assignment.....	59
6.3.1	Operator Assignment of IP Addresses.....	60
7	AP MODULE INSTALLATION.....	61
7.1	Unpacking the Canopy Products.....	61
7.1.1	Component Layout.....	61
7.1.2	Diagnostic LEDs.....	62
7.2	Cabling the AP.....	62
7.2.1	Standards for Wiring.....	62
7.2.2	Recommended Tools.....	63
7.2.3	Connector Wiring.....	63
7.2.4	Overriding IP Address and Password Setting.....	66

7.2.5	Wiring to Extend Network Sync	67
7.3	Configuring the AP	68
7.3.1	Configuration from the Factory	68
7.3.2	GUI Access Difficulty	68
7.3.3	Configuration Procedure	69
7.4	Installing the AP	70
7.5	Verifying System Performance	72
8	USER INTERFACE PAGES	74
8.1	Quick Start Page	74
8.1.1	Quick Start Available Pages	75
8.1.2	Quick Start Operator Options	75
8.2	Status Page	76
8.2.1	Status Parameters	76
8.3	Configuration Page	78
8.3.1	Configuration Parameters	79
8.3.2	Configuration Buttons	86
8.4	IP Configuration Page	86
8.4.1	IP Configuration Parameters	87
8.4.2	IP Configuration Buttons	87
8.5	Event Log Page	88
8.5.1	Event Log Operator Option	88
8.6	LUID Select Page	89
8.7	Link Test Page	90
8.7.1	Key Link Capacity Test Fields	90
8.7.2	Capacity Criteria for the Link	91
8.7.3	High-priority Bandwidth Planning	91
8.8	Time & Date Page	91
8.9	Sessions Page	92
8.9.1	Sessions Parameters	93
8.10	GPS Status Page	94
8.11	Ethernet Stats Page	95
8.11.1	Ethernet Stats Parameters	95
8.12	Expanded Stats Page	96
8.13	Reg Failed SMs Page	97
8.14	Bridge Table Page	98
9	CANOPY SYSTEM ACCESSORIES	99
10	AP MODULE SPECIFICATIONS	100
11	HISTORY OF CHANGES IN THIS DOCUMENT	102

LIST OF FIGURES

Figure 1: Additional link to extend network sync, Design 3	17
Figure 2: Additional link to extend network sync, Design 4	17
Figure 3: Additional link to extend network sync, Design 5	18
Figure 4: Canopy system wiring	18
Figure 5: Burst Allocation vs. Sustained Rate, Example 1	21
Figure 6: Burst Allocation vs. Sustained Rate, Example 2	22
Figure 7: Burst Allocation vs. Sustained Rate, Example 3	22
Figure 8: Burst Allocation vs. Sustained Rate, Example 4	22
Figure 9: High-priority channel layout	23
Figure 10: Example FTP session.....	24
Figure 11: Example telnet session to change screen logo	25
Figure 12: Canopy System Calculator page for beam width	41
Figure 13: Canopy System Calculator page for antenna elevation	42
Figure 14: Canopy System Calculator page for antenna downward tilt	43
Figure 15: Fresnel zone	44
Figure 16: Canopy System Calculator page for Fresnel zone dimensions	45
Figure 17: Determinants in Rx signal level	46
Figure 18: Canopy System Calculator page for path loss	47
Figure 19: FTP to AP for SM auto-update	49
Figure 20: Telnet to AP for SM auto-update	49
Figure 21: Telnet to AP to turn off SM auto-update	50
Figure 22: Example layout of 7 Access Point clusters.....	57
Figure 23: Example of IP address in Class B subnet	58
Figure 24: Canopy AP base cover, attached and detached	61
Figure 25: Location of 115-/230-volt switch	72
Figure 26: Quick Start screen	74
Figure 27: Status screen.....	76
Figure 28: Configuration screen	78
Figure 29: Configuration screen, continued.....	83
Figure 30: IP Configuration screen	86
Figure 31: Event Log screen.....	88
Figure 32: LUID Select screen.....	89
Figure 33: Link Test screen	90
Figure 34: Time & Data screen	91
Figure 35: Example Sessions page data	92
Figure 36: GPS Status screen	94
Figure 37: Reg Failed SMS screen	97
Figure 38: Bridge Table screen	98

LIST OF TABLES

Table 1: Definitions of Canopy components	14
Table 2: Ranges of links with and without Passive Reflector	15
Table 3: Categories of MIB-II objects	29
Table 4: Canopy Enterprise MIB objects for APs, SMs, and BHs	31
Table 5: Canopy Enterprise MIB objects for APs and BH timing masters.....	32
Table 6: Canopy Enterprise MIB objects for SMs and BH timing slaves.....	36
Table 7: Example 2.4-GHz channel assignment by sector.....	55
Table 8: Example 5.2-GHz channel assignment by sector.....	56
Table 9: Example 5.7-GHz channel assignment by sector.....	56
Table 10: Subnet masks for Network Classes A, B, and C	58
Table 11: Status information that LEDs provide	62
Table 12: Module auto-sensing per MAC address	63
Table 13: Specifications.....	100

LIST OF PROCEDURES

Procedure 1: Replacing the Canopy logo	24
Procedure 2: Denying all remote access	26
Procedure 3: Reinstating remote access capability.....	26
Procedure 4: Installing the Canopy Enterprise MIB files	30
Procedure 5: Auto-updating SMs.....	48
Procedure 6: Enabling spectrum analysis	51
Procedure 7: Invoking the low power mode.....	51
Procedure 8: Fabricating an override plug.....	67
Procedure 9: Regaining access to the module	67
Procedure 10: Extending network sync	67
Procedure 11: Bypassing proxy settings to gain access module web pages.....	68
Procedure 12: Setting mandatory Configuration page parameters	69
Procedure 13: Setting optional Configuration page parameters.....	70
Procedure 14: Installing the AP	70
Procedure 15: Verifying system performance.....	72
Procedure 16: Viewing web pages for a selected SM	89
Procedure 17: Testing a link	90

1 WELCOME

Thank you for purchasing Motorola Canopy™ Access Point Modules.¹ This technology is the latest innovation in high speed wireless networking. Canopy system features include

- network speeds of 10/100 BaseT
- small compact design
- no special requirements for PC setup.

1.1 FEEDBACK

We welcome your feedback on Canopy system documentation. This includes feedback on the structure, content, accuracy, or completeness of our documents, and any other comments you have. Please send your comments to technical-documentation@canopywireless.com.

1.2 TECHNICAL SUPPORT

To get information or assistance as soon as possible for problems that you encounter, use the following sequence of action:

1. Search this document, the user manuals that support other modules, and the software release notes of supported releases
 - a. in the Table of Contents for the topic.
 - b. in the Adobe Reader® search capability for keywords that apply.²
2. Visit the Canopy systems website at <http://www.motorola.com/canopy>.
3. Ask your Canopy products supplier to help.
4. Gather information such as
 - the IP addresses and MAC addresses of any affected Canopy modules.
 - the software releases that operate on these modules.
 - data from the Event Log page of the modules.
 - the configuration of software features on these modules.
5. Escalate the problem to Canopy systems Technical Support (or another Tier 3 technical support that has been designated for you) as follows. You may either
 - send e-mail to technical-support@canopywireless.com.
 - call 1 888 605 2552 during the following hours of operation:
Monday through Sunday
7:00 a.m. to 11:00 p.m. EST

For warranty assistance, contact your reseller or distributor for the process.

¹ Canopy is a trademark of Motorola, Inc.

² Reader is a registered trademark of Adobe Systems, Incorporated.

2 ABOUT THIS DOCUMENT

The following information describes the purpose of this document and the reasons for reissue.

2.1 INTENDED USE

This manual includes Canopy features through Software Release 4.1. The audience for this manual comprises system operators, network administrators, and equipment installers. The user of this manual should have

- basic knowledge of RF theory. (See [General RF Considerations](#) on Page 41.)
- network experience. (See [General IP Addressing Concepts](#) on Page 58.)

2.2 NEW IN THIS ISSUE

This document has been revised to include changes in technical content. Issue 5 introduces the following changes:

- Coverage limited to the Access Point Module (Cluster Management Module information is now provided in a separate document.)
- Rearrangement of topics to make the document easier to return to as a reference source.
- Editorial changes to reduce redundancy and clarify technical concepts.
- Revision of the warranty stated in the legal section above (effective for products purchased on or after October 1, 2003).
- Information that supports 2.4-GHz Canopy modules. See
 - [Types of AP Applications](#) on Page 11.
 - [Channel Plans](#) on Page 50.
 - [Table 12](#) on Page 63.
 - [AP MODULE SPECIFICATIONS](#) on Page 100.
- Reminders to observe local and national regulations.
- Examples of interactions between burst data rate and sustained data rate settings. See [Interaction of Burst Data and Sustained Data Settings](#) on Page 21.
- More logical telnet session for branding the interface screens. See [Figure 11](#) on Page 25.
- Procedures to deny or permit remote access to an AP. See [Denying All Remote Access](#) on Page 26 and [Reinstating Remote Access Capability](#) on Page 26.
- Information on the MIB (Management Information Base) that a network management station can access through SNMP (Simple Network Management Protocol) to monitor and control variables in the Canopy system. See [SNMP](#) on Page 26.
- Links to Canopy System Calculator pages for
 - beam width dimensions (see [Vertical Beam Width](#) on Page 41).
 - minimum antenna elevation (see [Radio Horizon](#) on Page 42).
 - antenna downward tilt angle (see [Antenna Downward Tilt](#) on Page 43).
 - Fresnel zone dimensions (see [Fresnel Loss](#) on Page 43).

- free space path loss (see [Free Space Path Loss](#) on Page 45).
- A procedure to use the AP to update the software release of all registered SMs that are entered onto an action list. See [AP Update of SM Software Release](#) on Page 48.
- A procedure to reduce the power of module transmission to mitigate or avoid interference. See [Power Reduction to Mitigate Interference](#) on Page 51.
- Expansion and clarification of available channel frequencies. See [5.2-GHz AP Channels](#) on Page 53 and [5.7-GHz AP Channels](#) on Page 54.
- Corrections for the roles of Pins 4 and 5 (to +V return) and Pins 7 and 8 (to +V) and inclusion of a Protective Earth label for ground. See [Connector Wiring](#) on Page 63.
- Clarifications about the use of an override plug to regain control of a module. See [Overriding IP Address and Password Setting](#) on Page 66.
- A procedure that allows sync to be passed to an AP by a collocated SM or a BH timing slave that receives sync over the air from another AP. See [Wiring to Extend Network Sync](#) on Page 67.
- A new field in the Status page to specify the active encryption technology with reboot and software version information. See [Software Version](#) on Page 76.
- New fields in the Configuration page to
 - specify how synchronization is sent to or from the AP. See [Sync Input](#) on Page 79.
 - clarify the interactions of password settings. See [Display-Only Access](#) on Page 82.
 - specify the type of air link security to be used on this AP. See [Airlink Security](#) on Page 83.
 - allow the operator to suppress the display of AP data on the AP Eval Data page of all SMs that register. See [SM Scan Privacy](#) on Page 83.
 - indicate whether SMs can authenticate on the AP (whether the BAM server is used). See [Authentication Mode](#) on Page 84.
 - enable SNMP traps. See [Trap Enable](#) on Page 85.
 - allow multiple APs to send beacons to multiple SMs in the same range without interference. See [Transmit Frame Spreading](#) on Page 85.
- A new web page for TCP/IP addressing. See [IP Configuration Page](#) on Page 86.
- A new field that displays antenna status. See [GPS Status Page](#) on Page 94.
- A new web page that provides information about any SM that attempted to register with the AP but failed since the last power cycle or reboot. See [Expanded Stats Page](#) on Page 96.
- Clarifications in the module specifications table. See [AP MODULE SPECIFICATIONS](#) on Page 100.

See also [HISTORY OF CHANGES IN THIS DOCUMENT](#) on Page 102.

2.3 ADDITIONAL FEATURE INFORMATION

Additional information about features that are introduced in new releases is available in Canopy Software Release Notes. These release notes are available at <http://www.motorola.com/canopy>.

3 SYSTEM OVERVIEW

The Canopy network uses the Canopy components that are defined in [Table 1](#).

Table 1: Definitions of Canopy components

Component	Definition
Access Point Module (AP)	One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
Access Point cluster (AP cluster)	Two to six APs that together distribute network or Internet services to a community of 1,200 or fewer subscribers. Each AP covers a 60° sector. This cluster covers as much as 360°.
Subscriber Module (SM)	A customer premises equipment (CPE) device that extends network or Internet services by communication with an AP or an AP cluster.
Cluster Management Module (CMM)	A module that provides power, GPS timing, and networking connections for an AP cluster. If this CMM is connected to a Backhaul Module (BH), then this CMM is the central point of connectivity for the entire site.
Backhaul Module (BH)	A module that provides point-to-point connectivity as either a standalone link or a link to an AP cluster through a selected AP.

3.1 MODULE-TO-MODULE COMMUNICATIONS

Each SM communicates with an AP in an assigned time slot that the AP controls. The AP coordinates the needs of SMs for data in both the downlink and the uplink to provide seamless communication across the entire network. The BH communicates with another BH, a collocated connection to the network, and a collocated AP.

The AP uses a point-to-multipoint protocol to communicate with each registered SM. The BH timing master uses a point-to-point protocol to communicate with a BH timing slave.

For more information about the BH, see *Canopy Backhaul Module (BH) User Manual*. For more information about the SM, see *Canopy Subscriber Module (SM) User Manual*.

3.2 TYPES OF AP APPLICATIONS

APs and SMs are available in 2.4-GHz, 5.2-GHz, and 5.7-GHz frequency bands. Due to regulatory agency restrictions, a 5.2-GHz SM *cannot* be used with a reflector in the U.S.A. or Canada.

A 2.4-GHz or 5.7-GHz SM can be used with a Canopy Passive Reflector dish. This reflector extends the maximum span of a link as defined in [Table 2](#).

Table 2: Ranges of links with and without Passive Reflector

Module in Link	Reflector	Typical Range ³
2400SM (DES) with 2400AP (DES)	none	5 miles (8 km)
2401SM (AES) with 2401AP (AES)		
2400SMRF (DES) with 2400AP (DES)	on SM	15 miles (24 km)
2401SMRF (AES) with 2401AP (AES)	on SM	15 miles (24 km)
5200SM (DES) ¹ with 5200AP (DES)	None allowed in U.S.A or Canada	2 miles (3.2 km)
5201SM (AES) ² with 5201AP (AES)		
5700SM (DES) with 5700AP (DES)	none	2 miles (3.2 km)
5701SM (AES) with 5701AP (AES)		
5700SMRF (DES) with 5700AP (DES)	on SM	10 miles (16 km)
5701SMRF (AES) with 5701AP (AES)	on SM	10 miles (16 km)
NOTES:		
<ol style="list-style-type: none"> DES indicates that the module is preconfigured for Data Encryption Standard security. See DES Encryption on Page 19. AES indicates that the module is preconfigured for Advanced Encryption Standard security. See AES Encryption on Page 19. Terrain and other line of sight circumstances affect the distance that can be achieved. Additionally, local or national radio regulations may govern whether and how the Passive Reflector can be deployed. 		

3.3 SYNCHRONIZATION

The CMM is a critical element in the operation of the Canopy 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.

3.3.1 Unsynchronized Modules

Without this pulse, an AP is unsynchronized, and a BH timing master cannot synchronize a BH timing slave. An unsynchronized module may transmit during a receive cycle of other modules. This can cause one or more modules to receive an undesired signal that is strong enough to make the module insensitive to the desired signal (become desensed).

3.3.2 Passing Sync

In releases earlier than Release 4.0, network sync can be delivered in only one over the air link in any of the following network designs:

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

In Release 4.0 and later releases, network sync can be either delivered as described above or 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 in Ethernet protocol to a collocated AP.
 2. This AP sends the sync in multipoint protocol over the air to an SM.
 3. This SM delivers the sync in Ethernet protocol to a collocated AP.
 4. This AP passes the sync in multipoint protocol in the additional link over the air to SMs.

This design is illustrated in [Figure 1](#).

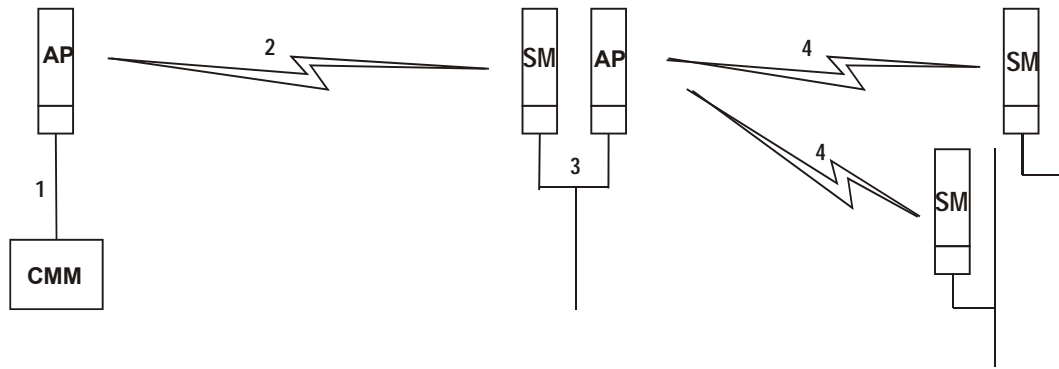


Figure 1: Additional link to extend network sync, Design 3

- Design 4
 1. A CMM provides sync in Ethernet protocol to a collocated AP.
 2. This AP sends the sync in multipoint protocol over the air to an SM.
 3. This SM delivers the sync in Ethernet protocol to a collocated BH timing master.
 4. This BH timing master passes the sync in point-to-point protocol in the additional link over the air to a BH timing slave.

This design is illustrated in [Figure 2](#).

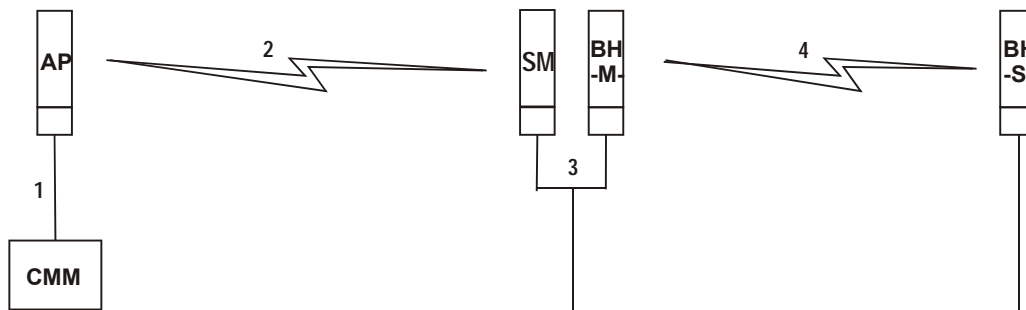


Figure 2: Additional link to extend network sync, Design 4

- Design 5
 1. A CMM provides sync in Ethernet protocol to a collocated BH timing master.
 2. This BH timing master sends the sync in point-to-point protocol over the air to a BH timing slave.
 3. This BH timing slave delivers the sync in Ethernet protocol to a collocated AP.
 4. This AP passes the sync in multipoint protocol in the additional link over the air to SMs.

This design is illustrated in [Figure 3](#).

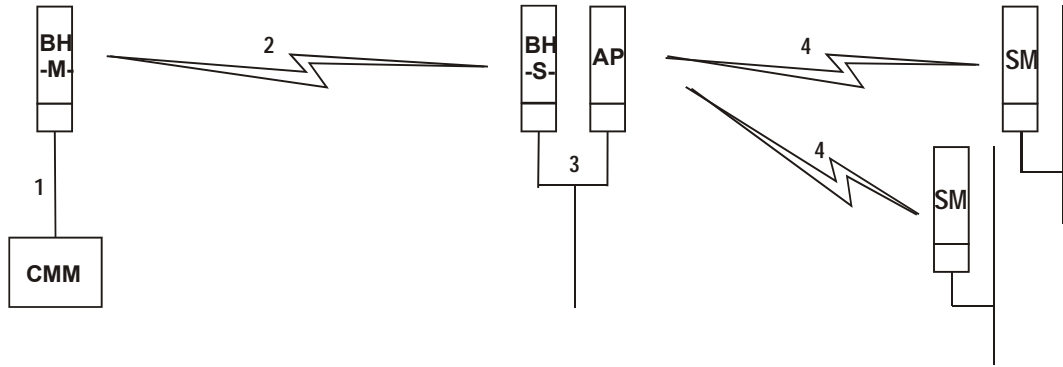
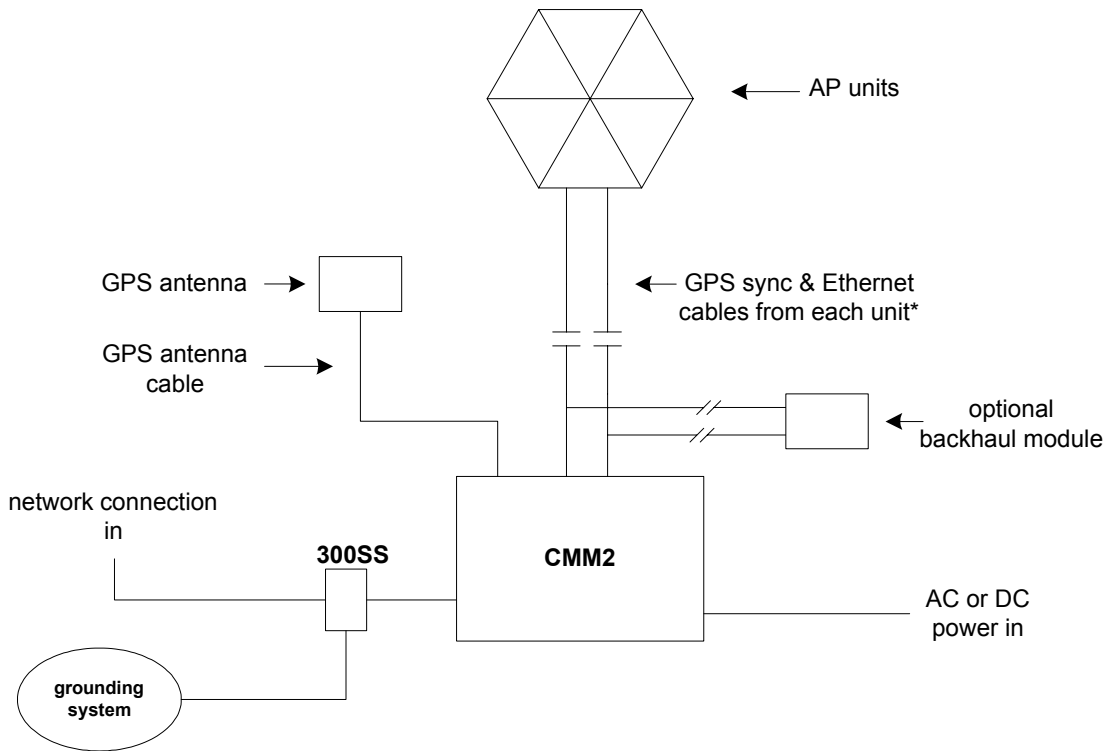


Figure 3: Additional link to extend network sync, Design 5

Wiring and configuration information for this sync extension is described under [Wiring to Extend Network Sync](#) on Page 67.

3.4 WIRING

The wiring scheme of the Canopy system is displayed in [Figure 4](#).



* Two cables, Ethernet and GPS sync, connect each sector AP to the CMM2.

Figure 4: Canopy system wiring

4 ADVANCED FEATURES

The following features are available in the Canopy system but not required for basic operation.

4.1 SECURITY FEATURES

Canopy 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.

4.1.1 BRAID

BRAID is a stream cipher that the TIA (Telecommunications Industry Association) has standardized. Standard Canopy 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.

4.1.2 DES Encryption

Standard Canopy 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.

4.1.3 AES Encryption

Motorola also offers Canopy 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 to ensure that these products are available in only certain regions. The Canopy distributor or reseller can advise service providers about current regional availability.

4.1.4 AES-DES Operability Comparisons

This section describes the similarities and differences between DES and AES products, and the extent to which they may interoperate.

Key Consistency

The DES AP and the DES Backhaul timing master module are factory-programmed to enable or disable *DES* encryption. Similarly, the AES AP and the AES Backhaul timing master module are factory-programmed to enable or disable *AES* encryption.

In either case, the authentication key entered in the Backhaul Configuration page establishes the encryption key. For this reason, the authentication key must be the same on each end of the backhaul link.

Feature Availability

Canopy 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.

Field-programmable Gate Array

Canopy AES products 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.

Signaling Rates for Backhaul Modules

DES BHs are available in both 10-Mbps and 20-Mbps signaling rates. AES BHs are available with only a 10-Mbps signaling rate.

Upgradeability

Canopy DES products cannot be upgraded to AES. To have the option of AES encryption, the service provider must purchase AES products.

Interoperability

Canopy AES products 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.

4.2 BANDWIDTH MANAGEMENT

Each AP controls SM bandwidth management. All SMs registered to an AP receive and use the same bandwidth management information that is set in their Access Point.

The Canopy software uses *token buckets* to manage the bandwidth of each SM. Each SM employs two buckets: one for uplink and one for downlink throughput. These buckets are continuously being filled with tokens at a rate set by the **Sustained Data Rate** variable field in the AP.

4.2.1 Bandwidth and Authentication Manager (BAM)

Canopy systems offer the Bandwidth and Authentication Manager (BAM) to manage bandwidth *individually* for each SM registered to an AP. BAM allows the setting of Sustained Uplink Data Rate, Sustained Downlink Data Rate, Uplink Burst Allocation, and Downlink Burst Allocation for the individual SM.

BAM also provides secure SM authentication and user-specified DES encryption keys. BAM is an optional Canopy software product that operates on a networked PC.

4.2.2 Recharging Buckets

The **Burst Allocation** variable field in the AP sets the size of each bucket. This limits the maximum number of tokens that can fill a bucket.

If the SM transfers data at the Sustained Data Rate, then the bucket refills at the same rate, and burst is impossible. If the SM transfers data at a rate less than the Sustained Data Rate, then the bucket continues to fill with unused tokens. In this case, required bursting occurs at the rate determined by the number of unused tokens.

After a burst is completed, the bucket is recharged at the Sustained Data Rate. Short bursts recharge faster than large bursts.

4.2.3 Subscriber Module Perspective

Normal web browsing, e-mail, small file transfers, and short streaming video are rarely rate limited, depending on the bandwidth management settings in the AP or the BAM server. When the SM processes large downloads such as software upgrades and long streaming video, or a series of medium-size downloads, these transfer at a bandwidth higher than the Sustained Data Rate (unless no unused tokens remain in the bucket) until the burst limit is reached.

When the burst limit is reached, the data rate falls to the Sustained Data Rate setting. Then later, when the SM is either idle or transferring data at a rate slower than Sustained Data Rate, the burst limit recharges at the Sustained Data Rate.

4.2.4 Interaction of Burst Data and Sustained Data Settings

A Burst Allocation setting

- less than the Sustained Data Rate yields a Sustained Data Rate equal to the Burst Allocation. (See [Figure 5](#) and [Figure 7](#).)
- equal to the Sustained Data Rate negates the burst capability. (See [Figure 6](#).)
- at zero shuts off the data pipe. (See [Figure 8](#).)

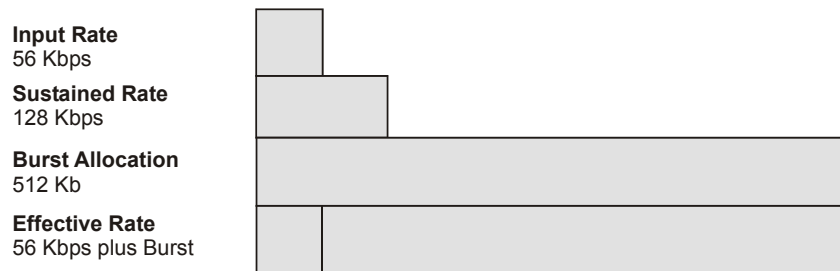


Figure 5: Burst Allocation vs. Sustained Rate, Example 1

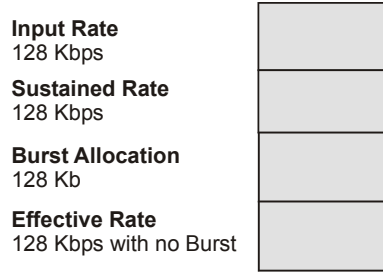


Figure 6: Burst Allocation vs. Sustained Rate, Example 2

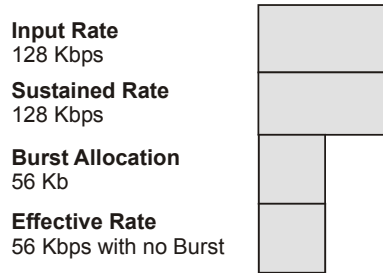


Figure 7: Burst Allocation vs. Sustained Rate, Example 3

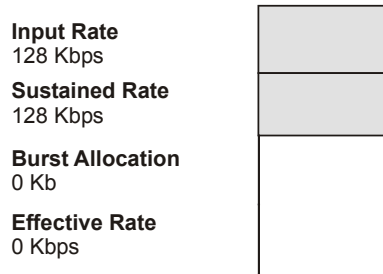


Figure 8: Burst Allocation vs. Sustained Rate, Example 4

4.3 HIGH-PRIORITY BANDWIDTH

To support low-latency traffic such as VoIP (Voice over IP), the Canopy system implements a high-priority channel. This channel does not affect the inherent latencies in the Canopy 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.

The Canopy system separates this traffic by recognizing the IPv4 Type of Service Low Latency bit (Bit 3). Bit 3 is set by a device outside the Canopy system. If this bit is set, the system sends the packet on the high-priority channel and services this channel before any normal traffic.

NOTE: To enable the high-priority channel, the operator must configure *all* high-priority parameters.

The high-priority channel is enabled by configuration of four parameters in the Configuration web page. These parameters are:

- **High Priority Uplink Percentage**
- **UAcks Reserved High**
- **DAcks Reserved High**
- **NumCtrlSlots Reserved High**

4.3.1 High Priority Uplink Percentage

The **High Priority Uplink Percentage** parameter defines the percentage of the uplink bandwidth to dedicate to low-latency traffic. When set, this percentage of RF link bandwidth is permanently allocated to low-latency traffic, regardless of whether low-latency traffic is present. The system provides no corresponding downlink parameter because scheduling algorithms in the AP allocate this bandwidth as needed.

4.3.2 UAcks Reserved High

The **UAcks Reserved High** parameter defines the number of slots used to acknowledge high-priority data that is received by an SM. The recommended setting for this parameter is 3. The recommended setting for the corresponding **TotalNumUAcksSlots** parameter is 6.

4.3.3 DAcks Reserved High

The **DAcks Reserved High** parameter defines the number of slots used to acknowledge high-priority data that is received by an AP. The recommended setting for this parameter is 3. The recommended setting for the corresponding **NumDackSlots** parameter is 6.

4.3.4 NumCtrlSlots Reserved High

The **NumCtrlSlots Reserved High** parameter defines the number of slots used to send control messages to an AP. The recommended setting for this parameter is 3. The recommended setting for the corresponding **NumCtrlSlots** parameter is 6.

4.3.5 Allocations to Downlink and Uplink

Figure 9 illustrates the format of the high-priority channel.

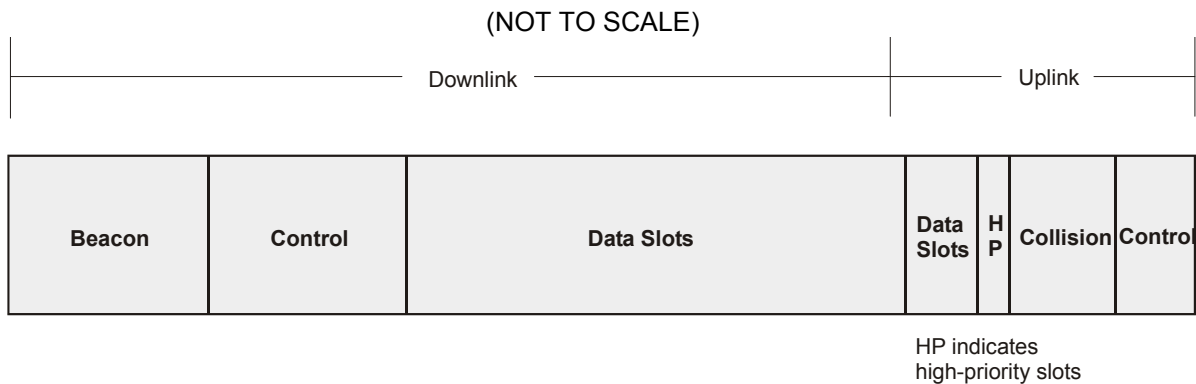


Figure 9: High-priority channel layout

Example Allocation

At AP default downlink-to-uplink settings (75% downlink and 25% uplink), if High Priority is set to 25%, then

- in the uplink, the total of reserved slots is equivalent to 25% (2 slots in this example) and
 - the bandwidth is 64 bytes per slot, repeated 400 times each second.
 - $[2 \text{ slots/instance}] \times [64 \text{ bytes/slot}] \times [8 \text{ bits/byte}] \times [400 \text{ instances/second}] = 409,600 \text{ bps}$
 $\approx 400 \text{ kbps}$ of uplink bandwidth
- in the downlink, the AP
 - does not reserve slots, but will service all high-priority bandwidth requests.
 - may become saturated by attempting to service too much high-priority traffic.
 - monitors the Low Latency TOS (Type of Service) bit, Bit 3, in the Ethernet frame.
 - prioritizes the traffic in the high-priority queue (when Bit 3 is set) according to the AP configuration settings for the high-priority channel.

4.4 BRANDING

The web-based interface screens on each Canopy module contain the Canopy logo. This logo can be replaced with a custom company logo. A file named `canopy.jpg` generates the Canopy logo.

Procedure 1: Replacing the Canopy logo

You can replace the Canopy logo as follows:

1. Copy your custom logo file to the name `canopy.jpg` on your system.
2. Use an FTP (File Transfer Protocol) session to transfer the new `canopy.jpg` file to the module, as in the example session shown in [Figure 10](#).

```
> ftp 169.254.1.1
Connected to 169.254.1.1
220 FTP server ready
Name (169.254.1.1: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
ftp> quit
221 Goodbye
```

Figure 10: Example FTP session

3. Use a `telnet` session to add the new `canopy.jpg` file to the file system, as in the example session shown in [Figure 11](#).

NOTE: Available `telnet` commands execute the following results:

- `addwebfile` adds a custom logo file to the file system.
- `clearwebfile` clears the customer logo file from the file system.
- `lsweb` lists the custom logo file and display the storage space available on the file system.

```

/-----\
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+> addwebfile canopy.jpg
Telnet +> lsweb

Flash Web files
/canopy.jpg      7867
free directory entries: 31
free file space: 55331

Telnet +> exit
```

Figure 11: Example telnet session to change screen logo

4.5 DENYING ALL REMOTE ACCESS

For a network where additional security is more important than ease of network administration, all remote access to an AP can be disabled as follows:

Procedure 2: Denying all remote access

1. Insert the override plug into the RJ-11 GPS sync port of the AP.
2. Power up or power cycle the AP.
3. Access the web page <http://169.254.1.1/lockconfig.html>.
4. Click the check box.
5. Save the changes.
6. Reboot the AP.
7. Remove the override plug.

RESULT: No access to this AP is possible through HTTP, SNMP, FTP, telnet, or over an RF link.

4.6 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 3: Reinstating remote access capability

1. Insert the override plug into the RJ-11 GPS sync port of the AP.
2. Power up or power cycle the AP.
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 AP.
7. Remove the override plug.

RESULT: Access to this AP is possible through HTTP, SNMP, FTP, telnet, or over an RF link.

4.7 SNMP

SNMPv2 (Simple Network Management Protocol Version 2) can be used to manage and monitor the Canopy 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.faqs.org/rfcs/rfc1902.html>.

4.7.1 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.

4.7.2 Managed Device

In SNMP, the managed device is the network element that operates on the agent software. In the Canopy 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.

4.7.3 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.

4.7.4 Dual Roles

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.

4.7.5 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 (Canopy module), 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 Canopy network, the manager issues these commands to the agents of more than one module (to all SMs in the operator network, for example).

4.7.6 Traps

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.

4.7.7 MIBS

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.

Paths

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).

Objects

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.

4.7.8 MIB-II

The standard MIB-II (Management Information Base systems and interface) objects are programmed into the Canopy 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 3](#):

Table 3: 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).

4.7.9 Canopy Enterprise MIB

For additional reporting and control, the Canopy Releases 3.2.5 and later provide the Canopy Enterprise MIB, which extends 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.

Procedure 4: Installing the Canopy Enterprise MIB files

To use this MIB, perform the following steps:

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 <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 five files from your Canopy software package directory into the `mibviewer/canopymibs` directory on the NMS (if necessary, first download the software package from <http://www.motorola.com/canopy>):
 - `whisp-tcv2-mib.txt` (Textual Conventions MIB), which defines Canopy system-specific textual conventions
 - `WHISP-GLOBAL-REG-MIB.txt` (Registrations MIB), which defines registrations for global items such as product identities and product components.
 - `WHISP-BOX-MIBV2-MIB.txt` (Box MIB), which defines module-level (AP, SM, and BH) objects.
 - `WHISP-APS-MIB.txt` (APs MIB), which defines objects that are specific to the AP or BH timing master.
 - `WHISP-SM-MIB.txt` (SM MIB), which defines objects that are specific to the SM or BH timing slave.
 - `CMM3-MIB.txt` (CMM3 MIB), which defines objects that are specific to the CMMmicro.
- NOTE:** The operator should not edit these MIB files in ASN.1. These files are intended for manipulation by only the NMS. However, the operator can view these files through a commercially available MIB viewer.
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.

4.7.10 Module Parameters for SNMP Implementation

Canopy modules provide the following Configuration web page parameters that govern SNMP access from the manager to the agent:

- **Display-Only Access**, which specifies the password that allows only viewing.
- **Full Access**, which specifies the password that allows both viewing and changing.
- **Community String**, which specifies the password for security between managers and the agent.

- **Accessing Subnet**, which specifies the subnet mask allows managers to poll the agents.
- **Trap Address**, which specifies the IP address of the NMS.

For more information about each of these fields, see the user document that supports the module.

4.7.11 Objects Defined in the Canopy Enterprise MIB

The Canopy Enterprise MIB defines objects for

- APs and BH timing masters
- SMs and BH timing slaves
- CMMmicros

AP, SM, and BH Objects

The objects that the Canopy Enterprise MIB defines for each AP and BH Timing Master are listed in [Table 4](#).

Table 4: Canopy Enterprise MIB objects for APs, SMs, and BHs

Object Name	Value Syntax	Operation Allowed
bhModulation	Integer	manage and/or monitor
bhTimingMode	Integer	manage and/or monitor
boxTemperature	DisplayString	monitor
bridgeEntryTimeout	Integer	manage and/or monitor
clearEventLog	Integer	manage and/or monitor
colorCode	Integer	manage and/or monitor
displayOnlyAccess	DisplayString	manage and/or monitor
fullAccess	DisplayString	manage and/or monitor
linkNegoSpeed	DisplayString	manage and/or monitor
pass1Status	DisplayString	monitor
pass2Status	DisplayString	monitor
reboot	Integer	manage and/or monitor
snmpMibPerm	Integer	manage and/or monitor
webAutoUpdate	Integer	manage and/or monitor
whispBoxBoot	DisplayString	monitor
whispBoxEsn	WhispMACAddress	monitor
whispBoxEvtLog	EventString	monitor
whispBoxFPGAVer	DisplayString	monitor

Object Name	Value Syntax	Operation Allowed
whispBoxSoftwareVer	DisplayString	monitor
whispBridgeAge	Integer	monitor
whispBridgeDesLuid	WhispLUID	monitor
whispBridgeExt	Integer	monitor
whispBridgeHash	Integer	monitor
whispBridgeMacAddr	MacAddress	monitor
whispBridgeTbErr	Integer	monitor
whispBridgeTbFree	Integer	monitor
whispBridgeTbUsed	Integer	monitor

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 5](#). The highlighted objects are commonly monitored by the manager. The traps provided in this set of objects are listed under [Traps Provided in the Canopy Enterprise MIB](#) on Page [38](#).

Table 5: Canopy Enterprise MIB objects for APs and BH timing masters

Object Name	Value Syntax	Operation Allowed
actDwnFragCount	Gauge32	monitor
actDwnLinkIndex	Integer	monitor
actUpFragCount	Gauge32	monitor
apBeaconInfo	Integer	manage and/or monitor
asIP1	IpAddress	manage and/or monitor
asIP2	IpAddress	manage and/or monitor
asIP3	IpAddress	manage and/or monitor
authKey	DisplayString	manage and/or monitor
authMode	Integer	manage and/or monitor
berMode	Integer	manage and/or monitor
dAcksReservHigh	Integer	manage and/or monitor
dataSlotDwn	Integer	monitor
dataSlotUp	Integer	monitor

Object Name	Value Syntax	Operation Allowed
dataSlotUpHi	Integer	monitor
defaultGw	IpAddress	manage and/or monitor
downLinkEff	Integer	monitor
downLinkRate	Integer	monitor
dwnLnkAckSlot	Integer	monitor
dwnLnkAckSlotHi	Integer	monitor
dwnLnkData	Integer	manage and/or monitor
dwnLnkDataRate	Integer	manage and/or monitor
dwnLnkLimit	Integer	manage and/or monitor
encryptionMode	Integer	manage and/or monitor
expDwnFragCount	Gauge32	monitor
expUpFragCount	Gauge32	monitor
fpgaVersion	DisplayString	monitor
gpsInput	Integer	manage and/or monitor
gpsStatus	DisplayString	monitor
gpsTrap	Integer	manage and/or monitor
highPriorityUpLnkPct	Integer	manage and/or monitor
lanIp	IpAddress	manage and/or monitor
lanMask	IpAddress	manage and/or monitor
linkAirDelay	Integer	monitor
linkAveJitter	Integer	monitor
linkDescr	DisplayString	monitor
linkESN	PhysAddress	monitor
linkInDiscards	Counter32	monitor
linkInError	Counter32	monitor
linkInNUcastPkts	Counter32	monitor
linkInOctets	Counter32	monitor
linkInUcastPkts	Counter32	monitor
linkInUnknownProtos	Counter32	monitor

Object Name	Value Syntax	Operation Allowed
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
linkSpeed	Gauge32	monitor
linkTestAction	Integer	manage and/or monitor
linkTestDuration	Integer	manage and/or monitor
linkTestError	DisplayString	monitor
linkTestLUID	Integer	manage and/or monitor
linkTestStatus	DisplayString	monitor
linkTimeOut	Integer	monitor
maxDwnLinkIndex	Integer	monitor
maxRange	Integer	manage and/or monitor
numCtlSlots	Integer	manage and/or monitor
numCtlSlotsReserveHigh	Integer	manage and/or monitor
numCtrSlot	Integer	monitor
numCtrSlotHi	Integer	monitor
numDAckSlots	Integer	manage and/or monitor
numUAckSlots	Integer	manage and/or monitor

Object Name	Value Syntax	Operation Allowed
PhysAddress	PhysAddress	monitor
privatelp	IpAddress	manage and/or monitor
radioSlicing	Integer	monitor
radioTxGain	Integer	monitor
regCount	Integer	monitor
regTrap	Integer	manage and/or monitor
rfFreqCarrier	Integer	manage and/or monitor
sectorID	Integer	manage and/or monitor
sessionCount	Integer	monitor
softwareBootVersion	DisplayString	monitor
softwareVersion	DisplayString	monitor
testDuration	Integer	monitor
testLUID	Integer	monitor
txSpreading	Integer	manage and/or monitor
uAcksReservHigh	Integer	manage and/or monitor
upLinkEff	Integer	monitor
upLinkRate	Integer	monitor
upLnkAckSlot	Integer	monitor
upLnkAckSlotHi	Integer	monitor
upLnkDataRate	Integer	manage and/or monitor
upLnkLimit	Integer	manage and/or monitor
whispGPSStats	Integer	monitor

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 6](#). The highlighted objects are commonly monitored by the manager.

Table 6: Canopy Enterprise MIB objects for SMs and BH timing slaves

Object Name	Value Syntax	Operation Allowed
airDelay	Integer	monitor
alternateDNSIP	IpAddress	manage and/or monitor
arpCacheTimeout	Integer	manage and/or monitor
authKey	DisplayString	manage and/or monitor
authKeyOption	Integer	manage and/or monitor
calibrationStatus	DisplayString	monitor
defaultGw	IpAddress	manage and/or monitor
dhcpcdns1	IpAddress	monitor
dhcpcdns2	IpAddress	monitor
dhcpcdns3	IpAddress	monitor
dhcpCip	IpAddress	monitor
dhcpClientEnable	Integer	manage and/or monitor
dhcpClientLease	TimeTicks	monitor
dhcpCSMask	IpAddress	monitor
dhcpDfltRterIP	IpAddress	monitor
dhcpDomName	DisplayString	monitor
dhcpIPStart	IpAddress	manage and/or monitor
dhcpNumIPsToLease	Integer	manage and/or monitor
dhcpServerEnable	Integer	manage and/or monitor
dhcpServerLeaseTime	Integer	manage and/or monitor
dhcpServerTable	DhcpServerEntry	monitor
dhcpSip	IpAddress	monitor
dmzEnable	Integer	manage and/or monitor
dmzIP	IpAddress	manage and/or monitor
dnsAutomatic	Integer	manage and/or monitor

Object Name	Value Syntax	Operation Allowed
enable8023link	Integer	manage and/or monitor
hostIp	IpAddress	monitor
hostLease	TimeTicks	monitor
hostMacAddress	PhysAddress	monitor
jitter	Integer	monitor
lanIp	IpAddress	manage and/or monitor
lanMask	IpAddress	manage and/or monitor
naptEnable	Integer	manage and/or monitor
naptPrivateIP	IpAddress	manage and/or monitor
naptPrivateSubnetMask	IpAddress	manage and/or monitor
naptPublicGatewayIP	IpAddress	manage and/or monitor
naptPublicIP	IpAddress	manage and/or monitor
naptPublicSubnetMask	IpAddress	manage and/or monitor
naptRFPublicGateway	IpAddress	manage and/or monitor
naptRFPublicIP	IpAddress	manage and/or monitor
naptRFPublicSubnetMask	IpAddress	manage and/or monitor
networkAccess	Integer	manage and/or monitor
powerUpMode	Integer	manage and/or monitor
prefferedDNSIP	IpAddress	manage and/or monitor
radioDbm	DisplayString	monitor
radioSlicing	Integer	monitor
radioTxGain	Integer	monitor
registeredToAp	DisplayString	monitor
rfScanList	DisplayString	manage and/or monitor
rsi	Integer	monitor
sessionStatus	DisplayString	monitor
tcpGarbageCollectTmout	Integer	manage and/or monitor
timingPulseGated	Integer	manage and/or monitor
udpGarbageCollectTmout	Integer	manage and/or monitor

Ports Designations in SNMP

SNMP identifies the ports of the module as follows:

- Interface 1 represents the RF interface of the module. To monitor the status of Interface 1 is to monitor the traffic on the RF interface.
- Interface 2 represents the Ethernet interface of the module. To monitor the status of Interface 2 is to monitor the traffic on the Ethernet interface.

These interfaces can be viewed on the NMS through definitions that are provided in the standard MIB files.

4.7.12 Traps Provided in the Canopy Enterprise MIB

Canopy modules provide the following SNMP traps for automatic notifications to the NMS:

- whispGPSInSync, which signals a transition from not synchronized to synchronized.
- whispGPSOutSync, which signals a transition from synchronized to not synchronized.
- whispRegComplete, which signals registration complete.
- whispRegLost, which signals registration lost.

4.7.13 MIB Viewers

Any of several commercially available MIB viewers can facilitate management of these objects through SNMP. Some are available as open source software. The Canopy division does not endorse, support, or discourage the use of any these viewers.

To assist end users in this area, the Canopy division 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 Library section under Support at <http://www.motorola.com/canopy>. MRTG software is available at <http://mrtg.hdl.com/mrtg.html>.

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>

5 SITE PLANNING

The following considerations are critical in the choice of a location for the wireless network infrastructure.

Note: Since each site is unique, typically many additional considerations are critical.

5.1 SPECIFIC MOUNTING CONSIDERATIONS

The Canopy APs must be mounted

- 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).
- 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.
- away from high-RF energy sites (such as AM or FM stations, high-powered antennas, and live AM radio towers).

5.1.1 Lightning Protection

The network plan must include lightning protection. The following precautions are strongly recommended:

- Install a lightning protection system for the site.
- Observe all local and national codes that apply to grounding for lightning protection.
- Use a Canopy Surge Suppressor to protect equipment from surges on the Ethernet cable that is connected to the Canopy system.

5.1.2 Electrical Requirements

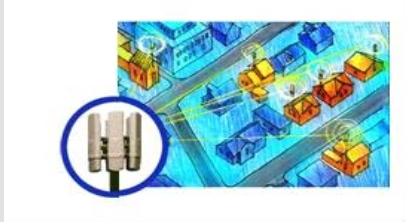
The network plan must also conform to applicable country and local codes, such as the NEC (National Electrical Code) in the U.S.A. If uncertain of code requirements, the planner should engage the services of a licensed electrician.

5.2 GENERAL RF CONSIDERATIONS

The network planner must account for the following general characteristics of RF transmission and reception.

5.2.1 Vertical Beam Width

The transmitted beam in the vertical dimension covers more area beyond the beam center. The Canopy System Calculator page [BeamwidthRadiiCalcPage.xls](#) automatically calculates the radii of the beam coverage area. Figure 12 displays an image of this file.



Canopy™ System Calculator

Automatically calculate

- Inner Radius of Vertical Beam Width
- Outer Radius of Vertical Beam Width
- Distance from near -3 dB to far -3 dB

from known

- Angle of Antenna Downward Tilt
- Elevation of Antenna
- Vertical Beam Width

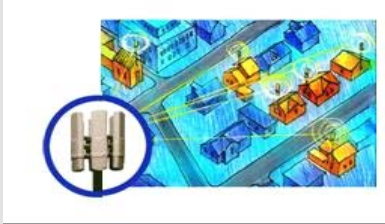
Determinants	Enter Values
Elevation of antenna (meters)	
Elevation of antenna (feet)	
Angle of antenna downward tilt (from 0-degree horizontal)	
Angle of vertical beam width (from -3 dB to -3 dB)	

Results	Read Values
Inner radius of vertical beam width (kilometers)	
Outer radius of vertical beam width (kilometers)	
Distance from near -3 dB to far -3 dB (kilometers)	
Inner radius of vertical beam width (miles)	
Outer radius of vertical beam width (miles)	
Distance from near -3 dB to far -3 dB (miles)	

Figure 12: Canopy System Calculator page for beam width

5.2.2 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). The Canopy System Calculator page [AntennaElevationCalcPage.xls](#) automatically calculates the minimum antenna elevation for these cases, presuming no landscape elevation difference from one end of the link to the other. Figure 13 displays an image of this file.



Canopy™ System Calculator

Automatically calculate
Minimum Antenna Elevation

from known
Distance from Transmitter to Receiver

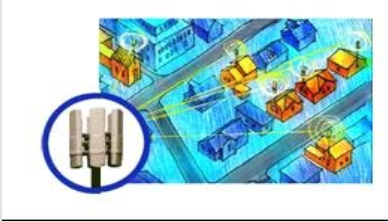
Determinants	Enter Values
Distance from transmitter to receiver (kilometers)	<input type="text"/>
Distance from transmitter to receiver (miles)	<input type="text"/>

Results	Read Values
Minimum antenna elevation (meters)	<input type="text"/>
Minimum antenna elevation (feet)	<input type="text"/>

Figure 13: Canopy System Calculator page for antenna elevation

5.2.3 Antenna Downward Tilt

The appropriate angle of antenna downward tilt is derived from both the distance between transmitter and receiver and the difference in their elevations. The Canopy System Calculator page [DowntiltCalcPage.xls](#) automatically calculates this angle. Figure 14 displays an image of this file.



Canopy™ System Calculator

Automatically calculate
Angle of Antenna Downward Tilt

from known
Distance from Transmitter to Receiver
Elevation of Transmitter
Elevation of Receiver

Determinants	Enter Values
Distance from transmitter to receiver (kilometers)	
Elevation of transmitter (meters)	
Elevation of receiver (meters)	
Distance from transmitter to receiver (miles)	
Elevation of transmitter (feet)	
Elevation of receiver (feet)	

Results	Read Values
Angle of antenna downward tilt (from metric calculation)	
Angle of antenna downward tilt (from English standard calculation)	

Figure 14: Canopy System Calculator page for antenna downward tilt

5.2.4 Fresnel Loss

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 signal strength of the transmitted signal to fade. Out-of-phase reflections and absorption of the signal result in signal cancellation.

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 15](#) illustrates an ideal Fresnel zone.

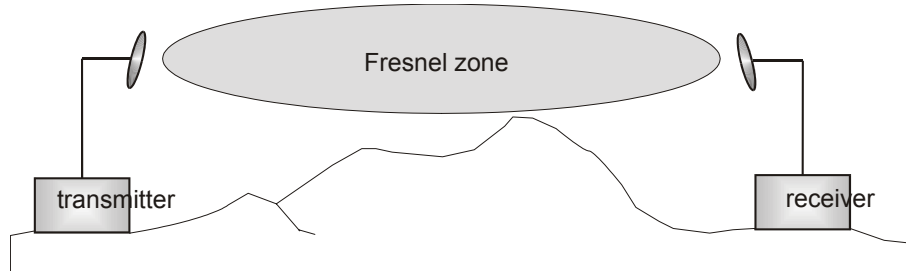
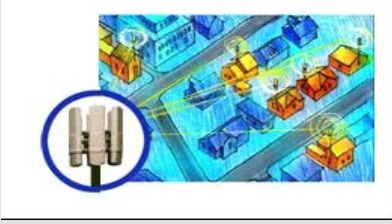


Figure 15: Fresnel zone

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 in the link path. [Figure 16](#) displays an image of this file.



Canopy™ System Calculator

Automatically calculate
Fresnel Zone (vertical dimension)

from known
 Distance from Transmitter to Receiver
 Distance from High-elevation Object to Receiver
 Frequency

Determinants	Enter Values
Distance from transmitter to receiver (kilometers)	
Distance from high-elevation object to receiver (kilometers)	
Distance from transmitter to receiver (miles)	
Distance from high-elevation object to receiver (miles)	
Frequency (GHz)	

Results	Read Values
Maximum Fresnel zone radius, midway between Tx and Rx (meters)	
Fresnel zone radius at object (meters)	
Minimum clearance required between line of sight and top of object (meters)	
Maximum Fresnel zone radius, midway between Tx and Rx (feet)	
Fresnel zone radius at object (feet)	
Minimum clearance required between line of sight and top of object (feet)	

Figure 16: Canopy System Calculator page for Fresnel zone dimensions

5.2.5 Free Space Path Loss

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.

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:

$$\text{system operating margin} = \text{Rx signal level} - \text{Rx sensitivity}$$

The Rx sensitivity of the AP is stated under [AP MODULE SPECIFICATIONS](#) on Page 100. The determinants in Rx signal level are illustrated in [Figure 17](#).

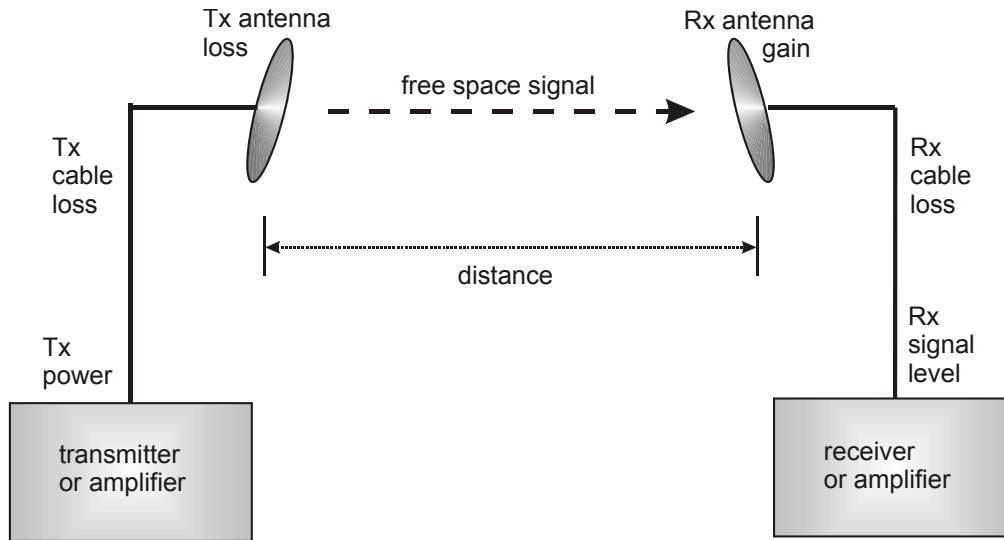



Figure 17: Determinants in Rx signal level

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.

The Canopy System Calculator page [PathLossCalcPage.xls](#) automatically calculates free space path loss. [Figure 18](#) displays an image of this page.



Canopy™ System Calculator

Automatically calculate
Free Space Path Loss

from known
Distance from Transmitter to Receiver
Frequency

Determinants	Enter Values
Distance from transmitter to receiver (kilometers)	<input type="text"/>
Distance from transmitter to receiver (miles)	<input type="text"/>
Frequency (GHz)	<input type="text"/>

Results	Read Values
Free space path loss from metric input (dB)	<input type="text"/>
Free space path loss from English standard input (dB)	<input type="text"/>

Figure 18: Canopy System Calculator page for path loss

5.2.6 Loss Due to Foliage

The foliage of trees and plants causes additional signal loss. Seasonal density, moisture content of the foliage, and other factors such as wind may change the amount of loss. Caution should be exercised when a link is used to transmit through this type of environment.

5.2.7 Carrier-to-Interference Ratio

The C/I (Carrier-to-Interference) ratio defines how much signal advantage must be engineered into the radio link to tolerate an interfering transmission.

Note: The C/I ratio is typically a design feature of the radio.

5.3 CANOPY COMPONENT PROLIFERATION

The network planner must account for the coordination of both initial and future Canopy modules.

5.3.1 Subscriber Modules

The planner must always consider the distribution of SMs as relative to the distribution of APs and clusters.

5.3.2 Access Point Modules

The number of APs deployed can vary from site to site, based on the locations of SMs that these modules must reach. The mounting scheme can also vary from site to site. The APs need not be mounted adjacent to each other. For example, on a three-legged tower, two APs can be mounted to each tower leg.

5.3.3 Access Point Clusters

Each AP cluster requires a CMM for seamless operation within the entire Canopy system. Thus the network planner should consider the number and locations of CMMs that will be deployed as the Canopy network grows.

5.4 AP UPDATE OF SM SOFTWARE RELEASE

In Release 4.1 and later releases, the operator can upgrade to a later release any SM that operates on Release 4.0 or later. To do so, the operator uses the FTP (File Transfer Protocol) and telnet utilities. The interval required for each SM update is approximately four minutes.

Procedure 5: Auto-updating SMs

To upgrade SMs to a later release, the operator performs the following steps:

1. FTP the file SMboot.bin, FPGA, and the action list to AP, as shown in [Figure 19](#).

```
< ls
062403_D40.jbc APASboot.bin BH10boot.bin
SMboot.bin
41actionlist.txt APboot.bin BH20boot.bin
> ftp 172.16.1.1
Connected to 172.16.1.1.
220 FTP server ready
Name (172.16.1.1:user):
331 Guest login ok
Password:
230 Guest login ok, access restrictions apply.
Remote system type is Type:.
ftp> binary
200 Type set to I.
ftp> put SMboot.bin
local: SMboot.bin remote: SMboot.bin
500 'EPSV': command not understood.
227 Entering Passive Mode (172,16,1,1,4,1)
150 Opening BINARY mode data connection for SMboot.bin
100% |*****| 712 KB 229.55
KB/s 00:00 ETA
226 Transfer complete.
729668 bytes sent in 00:03 (209.57 KB/s)
ftp> put 062403_D40.jbc
```



```

local: 062403_D40.jbc remote: 062403_D40.jbc
227 Entering Passive Mode (172,16,1,1,4,2)
150 Opening BINARY mode data connection for 062403_D40.jbc
100% |*****| 156 KB 219.48
KB/s 00:00 ETA
226 Transfer complete.
159859 bytes sent in 00:00 (156.18 KB/s)
ftp> put 41actionlist
local: 41actionlist remote: 41actionlist
ftp: local: 41actionlist: No such file or directory
ftp> put 41actionlist.txt
local: 41actionlist.txt remote: 41actionlist.txt
227 Entering Passive Mode (172,16,1,1,4,3)
150 Opening BINARY mode data connection for 41actionlist.txt
100% |*****| 53 58.81
KB/s 00:00 ETA
226 Transfer complete.
53 bytes sent in 00:00 (0.25 KB/s)
ftp> exit
221 Goodbye.

```

Figure 19: FTP to AP for SM auto-update

2. Update the SMs in a telnet session to the AP, as shown in [Figure 20](#).

```

> telnet 172.16.1.1
Trying 172.16.1.1...
Connected to 172.16.1.1.
Escape character is '^]'.
/-----\
C A N O P Y
Motorola Broadband Wireless Technology Center
(Copyright 2001, 2002 Motorola Inc.)
Telnet+> update 41actionlist.txt

```

Figure 20: Telnet to AP for SM auto-update

3. In the **Canopy Boot Version** field of the Status page of each SM that was targeted for update, confirm that the SM has been updated.

4. Turn off updating in a telnet session to the AP, as shown in [Figure 21](#).

RESULT: All SMs that are registered to the AP are upgraded to the later release.

```
> telnet 172.16.1.1
Trying 172.16.1.1...
Connected to 172.16.1.1.
Escape character is '^]'.
/-----\
C A N O P Y
Motorola Broadband Wireless Technology Center
(Copyright 2001, 2002 Motorola Inc.)
Telnet+> updateoff
Back on the original Telnet session:
13:15:40 UT : 11/10/03 : AutoUpdate currently Disabled.
Telnet+>
```

Figure 21: Telnet to AP to turn off SM auto-update

5.5 CHANNEL PLANS

For 5.2- 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. This allows the operator to customize the channel layout for interoperability where other Canopy equipment is collocated.



Regardless of whether 2.4-, 5.2-, or 5.7-GHz modules are deployed, channel separation between modules should be at least 20 MHz.

5.5.1 Physical Proximity

A BH and an AP that operate in the same frequency band should be separated by at least 100 feet (30 meters). At closer distances, the frame structures that these modules transmit and receive cause interference.

A BH and an AP on the same tower, or separated by less than 100 feet (30 meters), require a CMM. The CMM properly synchronizes all Canopy modules to prevent interference and desensing of the modules.

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

5.5.2 Spectrum Analysis

In Release 4.1 and later releases, the operator can

- use an SM as a spectrum analyzer.
- view a table that shows power level in RSSI and dBm for each frequency throughout the entire 20-MHz range, regardless of limited selections in the **Custom RF Frequency Scan Selection List** field of the Configuration page.
- select an AP channel that minimizes interference from other RF equipment.

This functionality can be used during the alignment of an SM, but is especially helpful for frequency selection during site planning.



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 after a 15-minute interval has elapsed.

Procedure 6: Enabling spectrum analysis

The Spectrum Analyzer in SM and BHS feature provides this functionality. To enable this functionality, the operator performs the following steps:

1. Access the Expanded Stats page of the SM.
2. On the Expanded Stats page, click **Spectrum Analyzer**.
3. On the Spectrum Analyzer page, click **Enable**.

RESULT: The feature is enabled.

4. Click **Enable** again.

RESULT: The system measures RSSI and dBm for each frequency.

5. Repeatedly click **Enable**.

RESULT: The system repeats the measurement and refreshes the displayed data until the spectrum analysis mode times out, 15 minutes after the mode was invoked in Step 3.

5.5.3 Power Reduction to Mitigate Interference

In Release 4.1 and later releases, where any module (SM, AP, BH timing master, or BH timing slave) is close enough to another module that self-interference is possible, the operator can set the AP to operate at 18 dB less than full power.



The following procedure can cause the SM to drop an active RF link to a module that is too far from the low-power AP. If a link is dropped when **Power Control** is set to **Low**, the link can be re-established by only Ethernet access.

Procedure 7: Invoking the low power mode

The Power Control feature provides this functionality. To enable this functionality, the operator performs the following steps:

1. Access the Configuration page of the module.
2. In the **Power Control** parameter, click **Low**.
3. Click **Save Changes**.
4. Click **Reboot**.
5. Access the Alignment page of a registered SM.
6. Assess whether the desired links for this module achieve
 - RSSI greater than 700.
 - jitter value between 0 and 4 in Release 4.0 and later releases or between 5 and 9 in any earlier release.

7. Access the Link Test 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 Configuration page of the module.
 - c. in the **Power Control** parameter, click **Full**.
 - d. click **Save Changes**.

5.5.4 2.4-GHz AP Channels

Channel selections for the AP in the 2.4-GHz band depend on whether the AP is deployed in cluster. Channel selections for the BH are not similarly limited.

2.4-GHz BH and Single AP Available Channels

A BH or a single 2.4-GHz AP can operate in 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 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. The network planner 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, the planner 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, the plan should allow at least 20 MHz of separation between channels. See [Spectrum Analysis](#) on Page 50.

5.5.5 5.2-GHz AP Channels

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

5.2-GHz Single AP Available Channels

A single 5.2-GHz AP can operate in the following channels, which are separated by 5-MHz increments as advised in the caution above.

(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 channels of *adjacent* APs should be separated by at least 20 MHz. However, 25 MHz of separation is advised.

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
-------	-------	-------

5.5.6 5.7-GHz AP Channels

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

5.7-GHz Single AP Available U-NII Channels

A single 5.7-GHz AP can operate in the following U-NII channels, which are separated by 5-MHz increments as advised in the caution above.

(All Frequencies in GHz)

5.745	5.765	5.785	5.805
5.750	5.770	5.790	
5.755	5.775	5.795	
5.760	5.780	5.800	

The channels of *adjacent* APs should be separated by at least 20 MHz. However, 25 MHz of separation is recommended.

5.7-GHz AP Cluster Recommended U-NII Channels

Four non-overlapping U-NII channels are recommended for use in a 5.7-GHz AP cluster:

(All Frequencies in GHz)

5.745	5.765	5.785	5.805
-------	-------	-------	-------

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

5.7-GHz Single AP Available ISM/U-NII Channels

A single 5.7-GHz AP enabled for ISM/U-NII frequencies can operate in the following channels, which are separated by 5-MHz increments as advised in the caution above.

(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.

5.7-GHz AP Cluster Recommended ISM/U-NII Channels

Six non-overlapping ISM/U-NII channels are recommended for use in a 5.7-GHz AP cluster:

(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 enabled for ISM/U-NII frequencies 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.

5.5.7 Example Channel Plans for AP Clusters

Examples for assignment of frequency channels and sector IDs are provided in [Table 7](#), [Table 8](#), and [Table 9](#). Each frequency is reused on the sector that is at a 180° offset. The entry in the Symbol column refers to the layout in [Figure 22](#) on Page 57.

NOTE: For more information on sector IDs, see [Configuration Page](#) on Page 78.

Table 7: 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 8: 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 9: Example 5.7-GHz 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

5.5.8 Multiple Access Points Clusters

When deploying multiple AP clusters in a dense area, consider aligning the clusters as shown in [Figure 22](#). However, this is only a recommendation. An installation may dictate a different pattern of channel assignments.

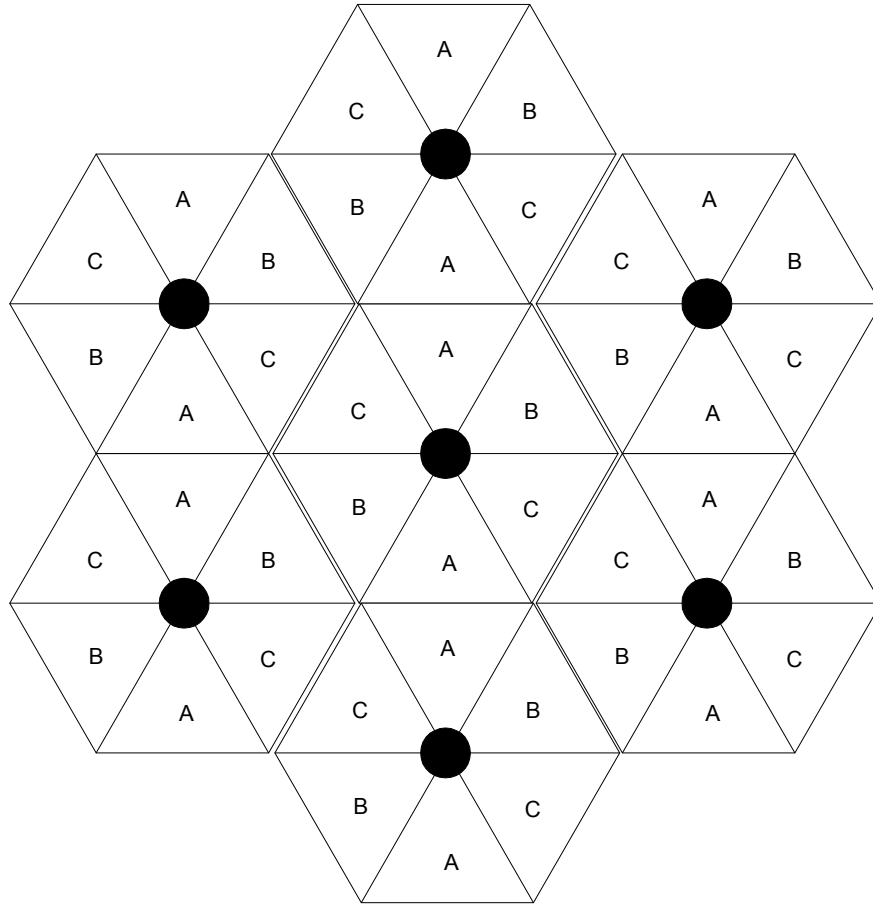


Figure 22: Example layout of 7 Access Point clusters

6 IP NETWORK PLANNING

A proper IP addressing method is critical to the operation and security of a Canopy network. The following information provides the background for the planner or operator to select an appropriate method.

6.1 GENERAL IP ADDRESSING CONCEPTS

Basic concepts of IP addressing and subnet masks are required for networking.

6.1.1 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.

6.1.2 Subnet Mask

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.

6.1.3 Example IP Address and Subnet Mask

In [Figure 23](#), 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 23: 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.

6.1.4 Subnet Classes

A subnet is classified as either a Class A, Class B, or Class C network. Subnet masks that classify the network are shown in [Table 10](#).

Table 10: Subnet masks for Network Classes A, B, and C

Class	Network Portion	Host Portion
A	11111111	00000000 00000000 00000000
B	11111111 11111111	00000000 00000000
C	11111111 11111111 11111111	00000000

Identification of Subnet Class

Subnet masks are not shipped in the IP packet. The packet contains only the 32-bit IP address of the destination. For this reason, information devices rely on assumption to distinguish between

- the portion of the IP address that identifies the network address
- the portion of the IP address that identifies the host.

IP systems developed a form of logic to make this determination:

- Class A network addresses always have the first bit of the IP address set to 0.
- Class B network addresses always have their first bit set to 1 and their second bit set to 0.
- Class C network addresses always have their first two bits set to 1 and the third bit set to 0.

With this logic, an information device can identify the subnet mask to apply to the IP address and where to route the data.

6.2 DYNAMIC OR STATIC ADDRESSING

For any computer to communicate with a Canopy 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.

NOTE: If an IP address that is set in the AP 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.

6.2.1 When a DHCP Server is Not Found

The following is a synopsis of an Internet Draft available at <http://www.ietf.org/internet-drafts/draft-ietf-zeroconf-ipv4-linklocal-05.txt>. This draft describes how Microsoft and Apple operating systems react when a DHCP server is not found on the network.

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 online 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).

6.3 AP MODULE ADDRESS ASSIGNMENT

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

- not assigned a routable IP address.
- assigned a routable IP address only if a firewall is present to protect the AP.

From the factory, each Canopy module—AP, BH, or SM—is assigned a unique MAC (Media Access Control) address and the following default networking information:

- IP address of 169.254.1.1
- Subnet mask of 255.255.0.0
- Network gateway of 169.254.0.0

6.3.1 Operator Assignment of IP Addresses

The Canopy network operator assigns IP (Internet Protocol) addresses to computers and network components, by either *static* or *dynamic* IP addressing. The operator also must identify the appropriate subnet mask and network gateway to each module.



The operator must first know how the service provider assigns IP addresses on this network.

7 AP MODULE INSTALLATION

The following steps are required to install a Canopy AP:

1. [Unpacking the Canopy Products](#). See Page 61.
2. [Cabling the AP](#). See Page 62.
3. [Configuring the AP](#). See Page 67.
4. Installing the AP and, optionally, the CMM and GPS (Global Positioning System) antenna. See [Installing the AP](#) on Page 70.
5. [Verifying System Performance](#) See Page 72.

7.1 UNPACKING THE CANOPY PRODUCTS

Upon receipt, carefully inspect all shipping boxes for signs of damage. If you find damage, immediately notify the transportation company.

Unpack the equipment, making sure that all of the components ordered have arrived. Saving all the packing materials is recommended. These can be used to either return products or transport the equipment to and from installation sites.

7.1.1 Component Layout

The simple design of the Canopy AP allows for easy deployment. As shown [Figure 24](#), the base cover of the module snaps off when a lever on the back of the base cover is depressed. This exposes the Ethernet and GPS sync connectors and diagnostic LEDs.

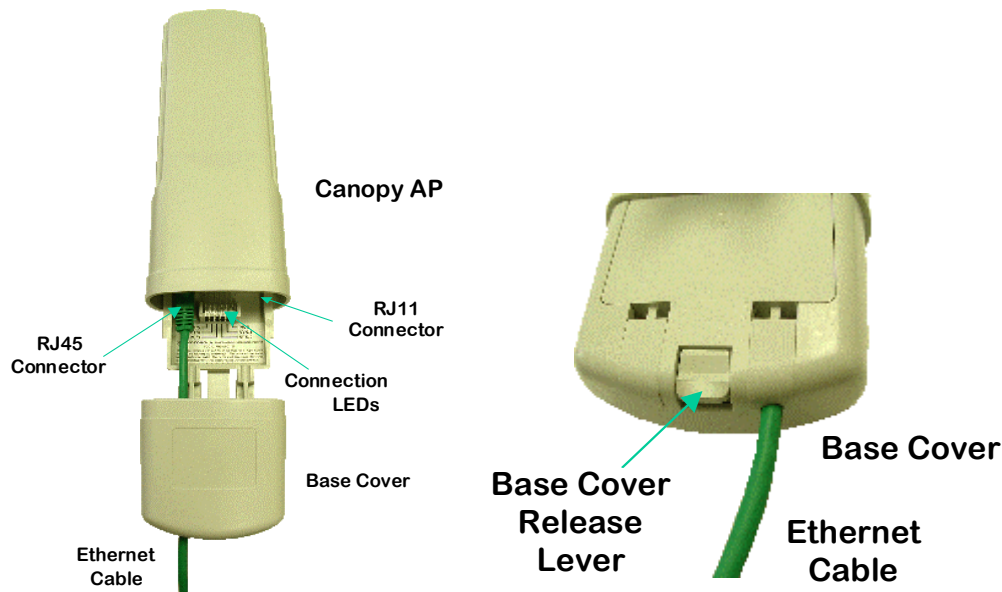


Figure 24: Canopy AP base cover, attached and detached

7.1.2 Diagnostic LEDs

The diagnostic LEDs report the following information about the current status of the AP, as described in [Table 11](#).

NOTE: [Table 11](#) identifies the LEDs in order of their left-to-right position as the cable connections face downward.

Table 11: Status information that LEDs provide

Label	Color when Active	Status Information Provided	Notes
LNK/5	green	Ethernet link	Continuously lit when link is present.
ACT/4	orange	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	orange	Presence of sync	Always lit on the AP.
PWR	red	DC power	Always lit when power is correctly supplied.

7.2 CABLING THE AP

The use of shielded cable for all Canopy infrastructure associated with Backhaul, Access Point, and CMMs is *strongly* recommended. The environment these modules operate in often has significant unknown or varying RF energy. Operator experience consistently indicates that the additional cost of shielded cabling is more than compensated by predictable operation and reduced costs for troubleshooting and support.

7.2.1 Standards for Wiring

The following information describes the wiring standards for installing a Canopy system. All diagrams use the EIA/TIA-568B color standard.

Either RJ-45 straight-thru or RJ-45 crossover cable can be used to connect a (network interface card), hub, router, or switch to a module. Canopy modules that are currently available can auto-sense whether the Ethernet cable in a connection is wired as straight-thru or crossover. Some modules that were sold earlier do not.

Table 12 identifies by MAC address whether a module auto-senses the Ethernet cable type.

Table 12: Module auto-sensing per MAC address

Module Type	MAC Address (ESN) of Non Auto-sensing Module	MAC Address (ESN) of Auto-Sensing Module
2.4-GHz modules	(no ESNs)	(all ESNs)
5.2 Modules	≤ 0a003e0021c8	≥ 0a003e0021c9
5.7 Modules	≤ 0a003ef00f79	≥ 0a003ef00f79a



Where a non auto-sensing module is used

- use an RJ-45 straight-thru cable to connect to a NIC (network interface card).
- use an RJ-45 crossover cable to connect to a hub, switch, or router.

Where the Canopy AC wall adapter is used

- the +V is +11.5 VDC to +30 VDC, with a nominal value of +24 VDC.
- the maximum Ethernet cable run is 328 feet (100 meters).

7.2.2 Recommended Tools

The following tools may be needed for cabling the AP:

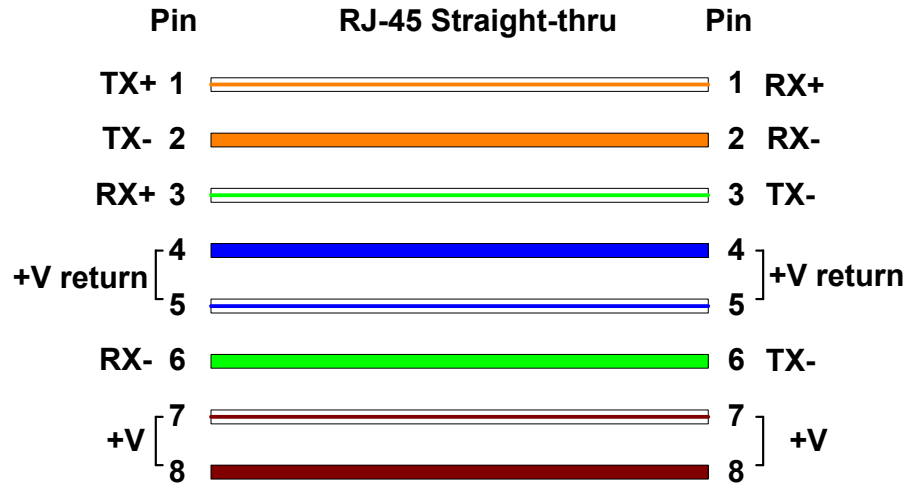
- RJ-11 crimping tool
- RJ-45 crimping tool
- electrician scissors
- wire cutters
- cable testing device.

7.2.3 Connector Wiring

The following diagrams correlate pins to wire colors and illustrate crossovers where applicable.

RJ-45 Straight-thru Ethernet Cable

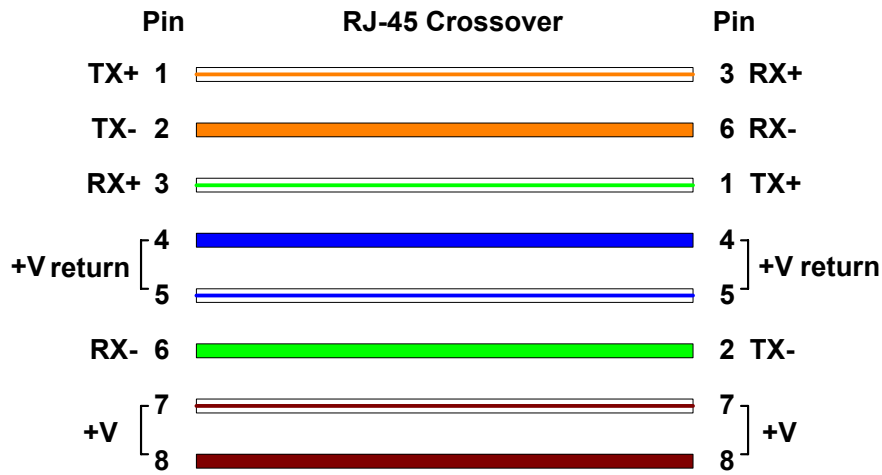
Pin 1 →	white / orange	← Pin 1
Pin 2 →	orange	← Pin 2
Pin 3 →	white / green	← Pin 3
Pin 4 →	blue	← Pin 4
Pin 5 →	white / blue	← Pin 5
Pin 6 →	green	← Pin 6
Pin 7 →	white / brown	← Pin 7
Pin 8 →	brown	← Pin 8



Pins 7 and 8 are used to carry power to the Canopy modules.

RJ-45 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



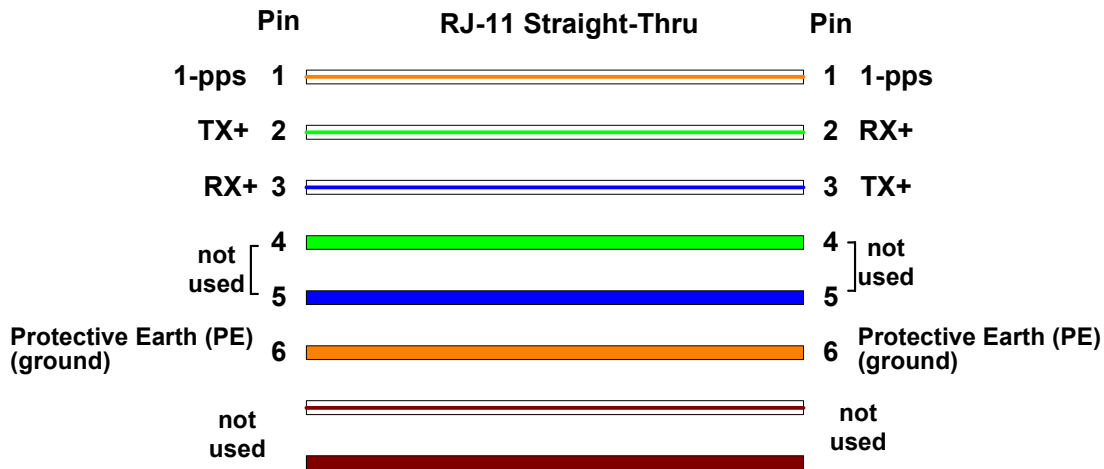
Pins 7 and 8 are used to carry power to the Canopy modules.

RJ-11 Straight-thru GPS sync cable

An RJ-11 cable is commonly used to connect a device to a phone line. This cable resembles the RJ-45 Ethernet cable except for a thinner cord and smaller plug. The Canopy system uses an RJ-11 cable to connect the AP or BH to GPS synchronization. Presuming CAT 5 cable and 6-pin RJ-11 connectors, the following diagram shows the wiring of the cable for GPS 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.



7.2.4 Overriding IP Address and Password Setting

Canopy systems offer a plug that allows the operator to temporarily override some AP settings and thereby regain control of the module. This plug is needed for access to the module in any of the following cases:

- The operator has 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 26 and [Reinstating Remote Access Capability](#) on Page 26.)
- Local access is desired for a module that has had the 802.3 link disabled in the Configuration page of the module.

This override plug resets the LAN1 IP address to 169.254.1.1. The plug allows the operator access the module through the default configuration *without changing* the configuration. The operator can then view and reset any non-default values.

Acquiring the Override Plug

The operator 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>.

Procedure 8: Fabricating an override plug

To fabricate 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 follows:

Pin 1 → white / orange	← Pin 1
Pin 2 → white / green	← Pin 2
Pin 3 → white / blue	← Pin 3
Pin 4 → green	← Pin 6
Pin 5 → blue	← Pin 5
Pin 6 → orange	← Pin 4

Using the Override Plug

The operator can regain access to the module as follows:

Procedure 9: Regaining access to the module

To use the override plug

1. Insert the override plug into the RJ-11 GPS sync port of the AP.
2. Apply power to the module through the Ethernet cable.

RESULT: The module reboots with the default IP address of 169.254.1.1, password fields blank, and all other configuration values as previously set.

3. Set passwords as desired.
4. Change configuration values if desired.
5. Save the settings.
6. Remove the override plug.
7. Power cycle the module.

7.2.5 Wiring to Extend Network Sync

The following procedure can be used to extend network sync by one additional hop, as described under [Passing Sync](#) on Page 16. Where a collocated module receives sync over the air, the collocated modules can be wired to pass the sync as follows:

Procedure 10: Extending network sync

1. Connect the GPS Sync ports of the collocated modules with RJ-11 cable.
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.

7.3 CONFIGURING THE AP

To put configuration changes into effect in any case, the operator must:



1. Make the change(s) on the web page of the module.
2. Click the **Save** button to temporarily save the change(s).
3. Click the **Reboot** button to reboot the module and implement the change(s).

Either of two methods is used to configure each AP:

- to use the Quick Start feature of the product. For more information on Quick Start, see [Quick Start Page](#) on Page 74
- to manually set each parameter

7.3.1 Configuration from the Factory

From the factory, the AP is configured to *not transmit* on any frequency. This configuration ensures that an operator does not accidentally turn on an unsynchronized AP.

Site synchronization of APs is required because

- Canopy modules:
 - transmit or receive, but not at the same time.
 - use TDD (Time Division Duplexing) to distribute signal access of the downlink and uplink frames.
- when one AP transmits while another receives signal, the transmitting module may interfere with or desense the receiving module. In this context, interference is self-interference (within the same Canopy network).

See [Synchronization](#) on Page 16.

7.3.2 GUI Access Difficulty

Proxy settings in the web browser may prevent access to the Canopy system GUI (graphical user interface). This can occur when the computer has used a proxy server address and port to configure a Canopy module. In this case, perform the following procedure to toggle the computer to not use the proxy setting.

GUI Access Procedure

Perform the following steps to access the GUI of this module.

Procedure 11: Bypassing proxy settings to gain 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 an alternate web browser is used, the menu selections differ from the above.

7.3.3 Configuration Procedure

This procedure includes both required and optional settings.

Required Steps

Perform the following steps to configure the AP:

Procedure 12: Setting mandatory Configuration page parameters

1. Remove the base cover of the AP. (See [Figure 24](#) on Page 61.)
2. In the powered down state, connect the Ethernet cable to the Ethernet port on both the AP and the computer.
3. Connect a power source to the AP.

RESULT: When power is applied to a Canopy 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 [Diagnostic LEDs](#) on Page 62.

4. Based on the origination source of the sync pulse for this AP, set the **Sync Input** parameter. See [Sync Input](#) on Page 79.
5. Assign an RF frequency for the module to transmit. See [RF Frequency Carrier](#) on Page 79.
6. Assign values for uplink and downlink bandwidth capping. See
 - [Sustained Uplink Data Rate](#) on Page 81.
 - [Uplink Burst Allocation](#) on Page 81.
 - [Sustained Downlink Data Rate](#) on Page 81.
 - [Downlink Burst Allocation](#) on Page 81.

NOTE: If the AP is in a cluster with other modules, then this parameter *must* be set exactly the same on all modules.

7. Assign an IP address to the module for the target network, and assign an appropriate subnet mask and network gateway. See
 - [LAN1 Network Interface Configuration, IP Address](#) on Page 87.
 - [LAN1 Network Interface Configuration, Subnet Mask](#) on Page 87.
 - [LAN1 Network Interface Configuration, Gateway IP Address](#) on Page 87.
8. Configure the appropriate color code on the AP so that SMs can register. (The SM color codes must match the AP color code for registration.) See [Color Code](#) on Page 81.
9. Configure the maximum range at which the AP can register an SM. See [Max Range](#) on Page 81.

NOTE: If the AP is in a cluster with other modules, then this parameter *must* be set exactly the same on all modules.

Optional Steps

In addition, the operator can perform the following optional steps:

Procedure 13: Setting optional Configuration page parameters

1. Assign as many as several passwords to prevent unauthorized users from connecting to the web-based interface of the AP. From the factory, no default password is assigned and password protection is turned off.
 - Passwords can be from 1 to 16 characters. Any combination of characters is allowed, except for the following special characters:

“ , . ‘ { } / \
; : [] () ` ~

- Either of two types of passwords can be configured: display-only or full-access.

The display-only password allows the operator to view the current status of the module. The full-access password allows the operator to both view the current status and change the module configuration. The red lettering to the right of the entry fields indicates that a password is set, but does not allow the operator see the password. For a description of interactions between settings of these types of passwords, see [Display-Only Access](#) on Page 82 and [Full Access](#) on Page 82.

NOTE: If the operator forgets either the password or the IP address for the module, a Canopy system override plug can be used to regain access. For details, see [Overriding IP Address and Password Setting](#) on Page 66.

2. Populate the **Site Name**, **Site Location**, and **Site Contact** fields. This is for only information purposes. See
 - [Site Name](#) on Page 85.
 - [Site Contact](#) on Page 85.
 - [Site Location](#) on Page 86.

7.4 INSTALLING THE AP

NOTE: When power is applied to a Canopy 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.

To install the Canopy AP, perform the following steps:

Procedure 14: Installing the AP

1. Remove the base cover of the AP. (See [Figure 24](#) on Page 61.)
2. In the powered down state, attach the cables to the AP. (See [Cabling the AP](#) on Page 62.)
3. 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. Mounting can be done with stainless steel hose clamps or another equivalent fastener.

NOTE: Canopy products offer no software utility for alignment of APs or Backhaul timing master modules.

4. 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.)
5. Using stainless steel hose clamps or equivalent fasteners, lock the AP in the proper direction and downward tilt.



One AP in each AP cluster must be connected to a CMM. For a module that is connected to a CMMmicro, the **Sync Input** parameter in the Configuration web page must be configured to **Sync to Received Signal (Power Port)**. For a module that is connected to a CMM2, the **Sync Input** parameter in the Configuration web page must be configured to **Sync to Received Signal (Timing Port)**.

6. For a single AP that is collocated with a CMM, connect the module to an Ethernet/Power port on the CMM, as shown in [Figure 25](#).

RESULT: When power is applied to a Canopy 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 [Diagnostic LEDs](#) on [Page 62](#).

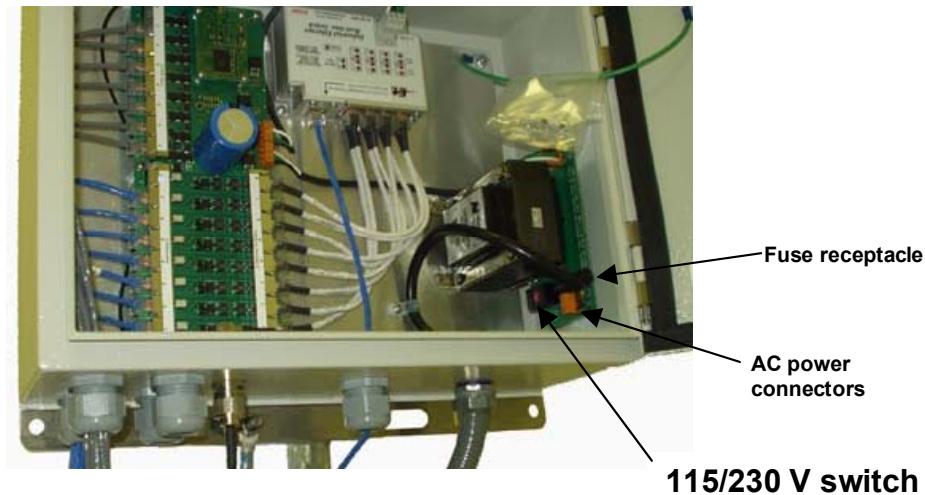


Figure 25: Location of 115-/230-volt switch

NOTE: The AC power connectors are labeled **N** for Neutral, **L** for Line, and **PE** for Protective Earth ↓ or ground. The maximum thickness of wire to be used is 4 mm² or 12 AWG.

For a single AP that is not collocated with a CMM, connect the module to a power supply.

RESULT: When power is applied to a Canopy 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 [Diagnostic LEDs](#) on Page 62.

For an AP cluster, connect the GPS sync port cable of at least one AP to the CMM.

7.5 VERIFYING SYSTEM PERFORMANCE

To verify the performance of the Canopy system after the APs have been installed, perform the following steps:

Procedure 15: Verifying system performance

1. Access the web-based interface for each AP by opening `http://<ip-address>`, where the `<ip-address>` is the address of the individual module.
2. In the menu on the left-hand side of the web page, click on **GPS Status**.
3. Verify that the AP is seeing and tracking satellites. (To generate the timing pulse, the module must track at least 4 satellites.)
4. Take an SM into the area surrounding the newly installed AP cluster.
5. At a clear line of sight in each sector, verify that the SM registers to each installed AP.

NOTE: The SM must have the same color code as the AP for successful registration.

6. When the SM is registered, verify
 - a. the frequency of the AP to which the SM is registered.
 - b. the Sector ID of the AP to which the SM is registered.

8 USER INTERFACE PAGES

The Canopy AP interface provides a series of web pages to configure and monitor the unit. The following is a quick reference to the interface screens.

NOTE: These screens are subject to change by subsequent software versions.

Access to the web-based interface is available only through a computer that is directly connected or connected through a network to the AP. If the computer is not connected to a network when configuring the module on a bench, disabling the proxy setting in the computer may be required.

In the address bar of your browser, enter the IP address of the AP (default is 169.254.1.1).

8.1 QUICK START PAGE

A standard Quick Start screen is displayed in [Figure 26](#).

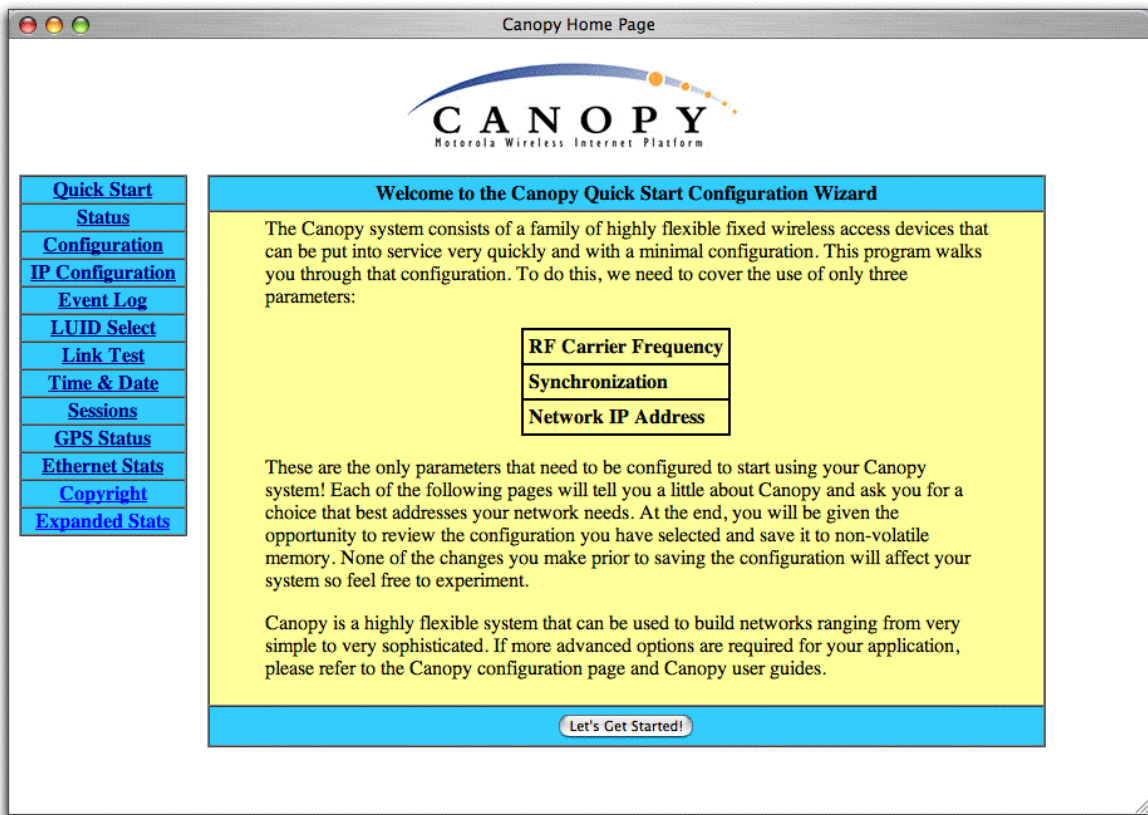


Figure 26: Quick Start screen

8.1.1 Quick Start Available Pages

Buttons on the left-hand side of the Quick Start page provide access to the following other pages:

Quick Start
Status
Configuration
IP Configuration
Event Log
LUID Select
Link Test
Time & Date
Sessions
GPS Status
Ethernet Stats
Expanded Stats

8.1.2 Quick Start Operator Options

Quick Start is a wizard that helps the operator to perform a basic configuration that places an AP into service. Only the following parameters must be configured:

- **RF Carrier Frequency**
- **Synchronization**
- **Network IP Address**

In each page under Quick Start, the operator can

- specify the settings that best address the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Experimentation with the interface is encouraged. Unless the configuration is saved, none of the changes affect the system.

8.2 STATUS PAGE

An example of a Status screen is displayed in [Figure 27](#).

Device Information	
Device type	5.2GHz - Multipoint - Access Point - 0a-00-3e-00-29-37
Software Version	CANOPY4.1 Nov 04 2003 10:38:27 AP-DES
Software Boot Version	CANOPYBOOT 1.1
FPGA Version	06240308 (DES)
Uptime	00:01:57
System Time	12:01:10 11/21/2003
Ethernet Interface	100Base-TX Full Duplex
Access Point Stats	
Registered SM Count	0
GPS Sync Pulse Status	Generating Sync
Site Information	
Site Name	No Site Name
Site Contact	No Site Contact

Figure 27: Status screen

The Status page provides information on the operation of the module. This is the default web page for the module.

8.2.1 Status Parameters

The Status page provides the following parameters:

Device Type

This field indicates the type of the Canopy module. Values include the frequency band of the module, the protocol that is used, and the MAC address of the module.

Software Version

This field indicates the software release that is operated on the module, the release date of the software, the time, and whether the module is secured by DES or AES encryption (see [Security Features](#) on Page 19). When requesting technical support, provide the information from this field.

Software Boot Version

This field indicates the CANOPYBOOT version number.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When requesting 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. 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.

Ethernet Interface

This field indicates the configuration of the Ethernet interface on the module.

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 that the AP is receiving 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 Canopy system.

Site Name

This field indicates the name of the physical module. The operator can assign or change this name on the Configuration web 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. The operator can provide or change this information on the Configuration web page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

8.3 CONFIGURATION PAGE

An example of a Configuration screen is displayed in [Figure 27](#).

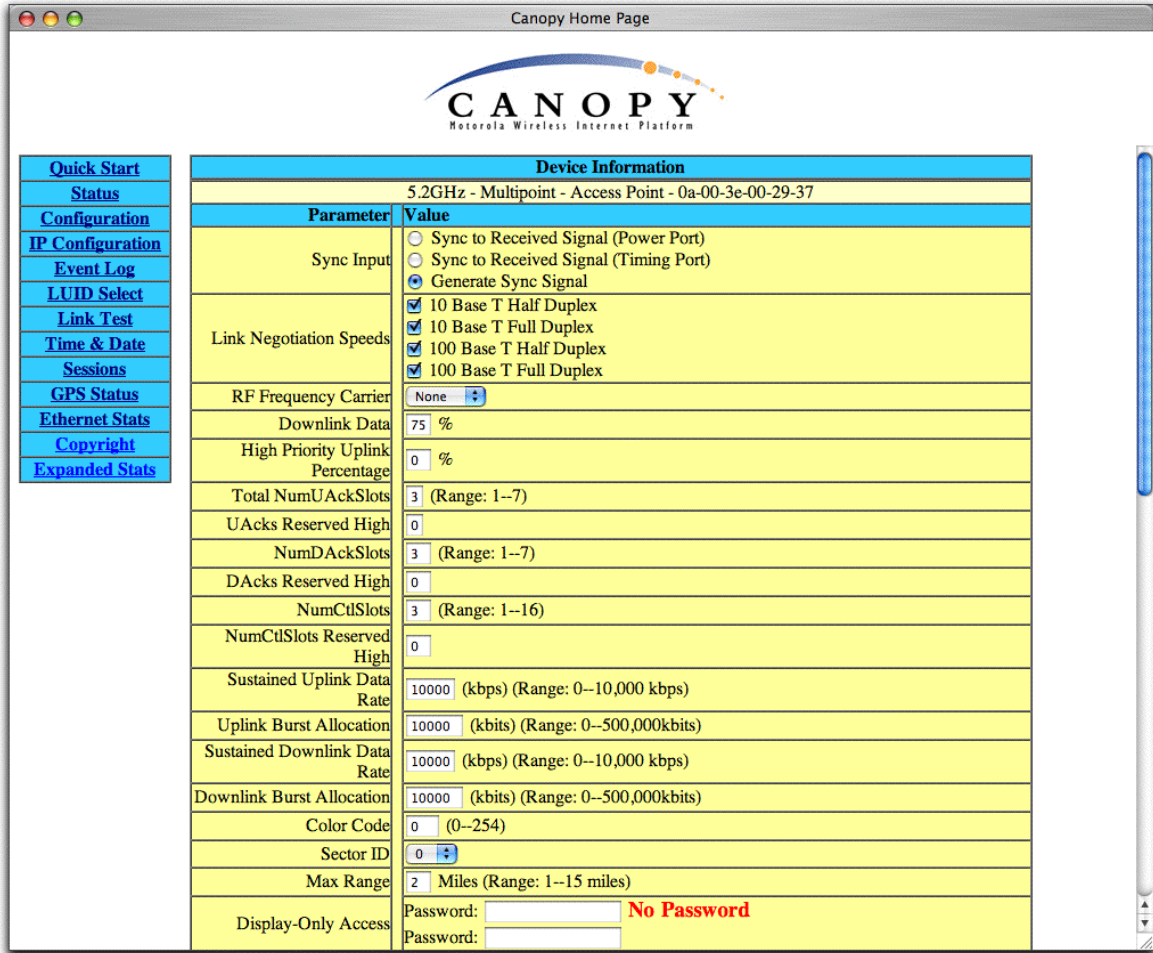


Figure 28: Configuration screen

The Configuration web page contains all of the configurable parameters that define how the module operates. The first line of information on the Configuration screen echoes the **Device Type** from the Status web page.

8.3.1 Configuration Parameters

The Configuration page provides the following parameters:

Sync Input

The operator specifies the type of synchronization for this AP to use.

The operator selects **Sync to Received Signal (Power Port)** to set this AP to receive GPS sync from a connected CMMmicro.

The operator selects **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.

The operator selects **Generate Sync Signal** where the AP does not receive sync, and no other AP or BHM is active within the link range. For link range information, see [Table 2](#) on Page 15.

Link Negotiation Speeds

The operator specifies the type of link speed desired 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.

RF Frequency Carrier

The operator specifies the frequency that the module will 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

- [2.4-GHz AP Channels](#) on Page 52.
- [5.2-GHz AP Channels](#) on Page 53.
- [5.7-GHz AP Channels](#) on Page 54.

Downlink Data

The operator specifies the percentage of the aggregate throughput that is needed 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%.



If the AP is in cluster, then this parameter must be set exactly the same on all other modules in the cluster.

High Priority Uplink Percentage

The operator specifies the percentage of the uplink bandwidth to dedicate to low-latency traffic. When set, this percentage of RF link bandwidth is permanently allocated to low-latency traffic, regardless of the amount of low-latency traffic that is present. No corresponding downlink parameter is settable. Scheduling algorithms allocate the corresponding downlink percentage.

NOTE: Parameter settings for the high-priority channel require careful consideration because bandwidth that is allocated to this channel decreases bandwidth on the regular channel, regardless of whether high-priority traffic exists. See [High-Priority Bandwidth](#) on Page 22.

Where the high-priority channel is desired, *all* high-priority parameters must be set. If all are not set, then the high-priority channel is not active.

Total NumUAckSlots

The operator specifies how many slots are used to acknowledge data that an SM receives. The default value of this parameter is 3. This value should be kept, except when the operator anticipates a high amount of traffic. If the value of 3 is entered for the following (**Uacks Reserved High**) parameter, then this parameter should be set to 6. The allowed range for this parameter is 1 to 7.



If the AP is in cluster, then this parameter must be set exactly the same on all other modules in the cluster.

Uacks Reserved High

The operator specifies how many slots are used to acknowledge high-priority data that an SM receives. This parameter should be set only when the high-priority channel is used. In this case, the recommended value of this parameter is 3.

NumDAckSlots

The operator specifies how many slots are used to acknowledge data that the AP receives. The default value of this parameter is 3. This value should be kept, except when the operator anticipates a high amount of traffic. If the value of 3 is entered for the following (**Dacks Reserved High**) parameter, then this parameter should be set to 6. The allowed range for this parameter is 1 to 7.



If the AP is in cluster, then this parameter must be set exactly the same on all other modules in the cluster.

Dacks Reserved High

The operator specifies how many slots are used to acknowledge high-priority data that the AP receives. This parameter should be set only when the high-priority channel is used. In this case, the recommended value of this parameter is 3.

NumCtlSlots

The operator specifies how many slots are used to send control messages to an AP. The default value of this parameter is 3. This value should be kept, except when the operator anticipates a high amount of traffic. If the value of 3 is entered for the following (**NumCtlSlots Reserved High**) parameter, then this parameter should be set to 6. The allowed range for this parameter is 1 to 16.



If the AP is in cluster, then this parameter must be set exactly the same on all other modules in the cluster.

NumCtlSlots Reserved High

The operator specifies how many slots are used to send control messages to an AP. This parameter should be set only when the high-priority channel is used. In this case, the recommended value of this parameter is 3.

NOTE: A description of the interactions between sustained and burst data settings for the following parameters is provided in [Interaction of Burst Data and Sustained Data Settings](#) on Page 21.

Sustained Uplink Data Rate

The operator specifies the rate at which each SM registered to this AP is capped in the uplink direction. The default rate is 10,000 kbps. This default imposes no restriction on the uplink.

Uplink Burst Allocation

The operator specifies the maximum amount of data that each SM is allowed to transmit at one time. The default amount is 10,000 kb.

Sustained Downlink Data Rate

The operator specifies the rate at which transmissions from the AP to any registered SM is capped. The default rate is 10,000 kbps. This default imposes no restriction on the uplink.

Downlink Burst Allocation

The operator specifies the maximum amount of data that the Access Point can transmit to any registered SM at one time. The default amount is 10,000 kb.

Color Code

The operator specifies 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. Color code allows the operator to segregate an individual network or neighbor Canopy networks.

Color code also allows the operator to force an SM to register to only a specific AP, even if the SM can reach multiple APs. On all Canopy modules, the default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

Sector ID

The operator specifies a number to associate with this AP. The Sector ID does not affect the operation of the AP.

On the AP Eval Data web page of the SM, the **Sector ID** field identifies the AP that the SM sees. For efficient and accurate network management, the operator is advised to

- assign a unique Sector ID to each sector in an AP cluster.
- repeat the assignment pattern throughout the entire Canopy system.

Max Range

The operator enters a number of miles that specifies the furthest distance from which an SM is allowed to register. Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. If the AP is in cluster, then this parameter on all units *must* be set exactly the same. The default Max Range is 2 miles.

NOTE: A value of 15 for this parameter decreases the number of available data slots by 1.

Display-Only Access

The operator enters the same password in both **Display-Only Access** fields for verification. When used, the display-only password allows only viewing activities on the module.

This protection interacts with the **Full Access** password protection as follows:

- If the display-only password is set and the **Full Access** password *is not*, then:
 - The display-only password is tied to telnet and FTP sessions to the module.
 - Anyone who enters the display-only password can view *or change* activities. This configuration *is not* recommended.
- If the **Full Access** password is also set, then the **Full Access** password is tied to telnet and FTP sessions.
- If the display-only password *is not* set and the **Full Access** password is, then no password is required to view activities on the module.
- If neither password is set, then anyone can view or change activities. This configuration *is not* recommended.

If the operator-assigned **Display-Only Access** password is forgotten, then the operator 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 IP Address and Password Setting](#) on Page 66.

Full Access

The operator enters the same **Full Access** password in both fields for verification. When used, the **Full Access** password

- allows both viewing and change activities on the module.
- is tied to telnet and FTP sessions to the module.

When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, the user name `root` must be entered in addition to the password.

If the operator-assigned **Full Access** password is forgotten, then the operator 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 IP Address and Password Setting](#) on Page 66.

NOTE: The operator can unset either password (revert the access to no password required). To do so, the operator types a space into the field and reboots the module. Any password must be entered twice to allow the system to verify that that the password is not mistyped. After any password is set and a reboot of the module has occurred, a **Password Set** indicator appears to the right of the field.

CANOPY Motorola Wireless Internet Platform	
Webpage Auto Update	0 Seconds (0 = Disable Auto Update)
Airlink Security	<input checked="" type="radio"/> Encryption Disabled <input type="radio"/> Encryption Enabled
SM Scan Privacy	<input type="checkbox"/> Disable SM Display of AP Eval Data
Authentication Mode	Authentication Not Available
Authentication Server IPs	0.0.0.0 0.0.0.0 0.0.0.0
Bridge Entry Timeout	25 Minutes (Range : 25 -- 1440 Minutes)
AP Background BER Mode	<input checked="" type="radio"/> No BER Stream <input type="radio"/> Send BER Stream
Power Control	<input type="radio"/> Low <input checked="" type="radio"/> Normal
SNMP	
Community String	Canopy
Accessing Subnet	0.0.0.0 / 0
Trap Address	0.0.0.0
Trap Enable	<input type="checkbox"/> Sync Status <input type="checkbox"/> Session Status
Permission	<input checked="" type="checkbox"/> Read Only
Update Application Information	
Update Application Address	0.0.0.0
Transmit Spreading Configuration	
Transmit Frame Spreading	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Site Information	
Site Name	No Site Name
Site Contact	No Site Contact
Site Location	No Site Location
<input type="button" value="Save Changes"/> <input type="button" value="Undo Saved Changes"/> <input type="button" value="Set to Factory Defaults"/>	
<input type="button" value="Reboot"/>	

Figure 29: Configuration screen, continued

As shown in Figure 29, the Configuration page continues with the following parameters:

Webpage Auto Update

The operator enters 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.

Airlink Security

The operator specifies the type of air link security to be used on 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.

SM Scan Privacy

When the SM Scan Privacy feature is enabled, the operator can use this field to suppress the display of data about this AP on the AP Eval Data page of all SMs that register.

Authentication Mode

If the optional Bandwidth and Authentication Manager (BAM) server is implemented, then the operator can use this field to select from among the following authentication modes:

- **Authentication Not Available if not using the BAM**—no SM is allowed to authenticate.
- **Authentication Enabled**—any SM can authenticate in the BAM server.
- **Authentication Optional**—an SM that is not compatible with the BAM server can access the wireless network through this AP.

Authentication Server IPs

If the optional BAM server is implemented, then the operator enters the IP addresses of one or more BAM servers that perform authentication for SMs that are registered to this AP.

Bridge Entry Timeout

The operator specifies 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.



An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

AP Background BER Mode

The operator chooses whether continuous BER (Bit Error Rate) data collection should be turned on. When the AP Background BER Mode is turned on, the operator can read the bit error rate on the subscriber side to assess the quality of a registered link. Two caveats apply to this setting:

- If the AP is in cluster, then the AP Background BER Mode must be set exactly the same on all other modules in the cluster.
- When the AP Background BER Mode is turned on, the aggregate available bandwidth decreases by approximately 200 kbps. For this reason, BER data collection should be limited to diagnostic intervals.

Power Control

In Release 4.1 and later releases, the operator selects either

- **Low** to set the BH timing master to operate at 18 dB less than full power to reduce the possibility of self-interference with a nearby module.
- **Normal** to allow the BH timing master to operate at full power.



Selection of **Low** can cause the BH to drop an active RF link to a module that is too far from the low-power BH. If a link is dropped when Power Control is set to **Low**, the link can be re-established by only Ethernet access.

See [Power Reduction to Mitigate Interference](#) on Page 51.

Community String

The operator specifies a control string that allows an SNMP management server to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

Accessing Subnet

The operator specifies the network that is allowed to access SNMP information from the module. The following two types of information must be entered:

- the network IP address in the form xxx.xxx.xxx.xxx
- the CIDR (Classless Interdomain Routing) prefix length in the form /xx (for example, 198.32.0.0/16 where /16 is a subnet mask of 255.255.0.0).

NOTE: For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.”

The default treatment is to allow all networks access.

Trap Address

The operator specifies the IP address (xxx.xxx.xxx.xxx) of an SNMP management server to which trap information should be sent. Trap information informs the monitoring system that something has occurred. For example, trap information is sent:

- After a reboot of the module.
- When an SNMP management server 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

The operator can select either **Sync Status** or **Session Status** to enable SNMP traps.

Permission

The operator can set this parameter to **Read Only** to disallow any parameter changes by the SNMP.

Update Application Address

For capabilities in future software releases, the operator can enter the address of the server to access for software updates on this AP and registered SMs.

Transmit Frame Spreading

If the operator selects this option, SMs between two APs can register in the assigned AP (not the other AP). If all SMs operate on Release 4.0 or later, then selection of this option is strongly recommended.

With this selection, 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.

Site Name

The operator specifies 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 SNMP management server. The buffer size for this field is 128 characters.

Site Contact

The operator enters contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by an SNMP management server. The buffer size for this field is 128 characters.

Site Location

The operator enters 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 SNMP management server. The buffer size for this field is 128 characters.

8.3.2 Configuration Buttons

The Configuration page provides the following buttons:

Save Changes

When the operator clicks this button, any changes that have been made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When the operator clicks this button, any changes that have been made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When the operator clicks this button, all configurable parameters are reset to the factory settings.

Reboot

When the operator clicks this button, the module reboots. When the operator has changed parameters in the Configuration page, the system highlights **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

8.4 IP CONFIGURATION PAGE

An example of the IP Configuration screen is displayed in [Figure 30](#).

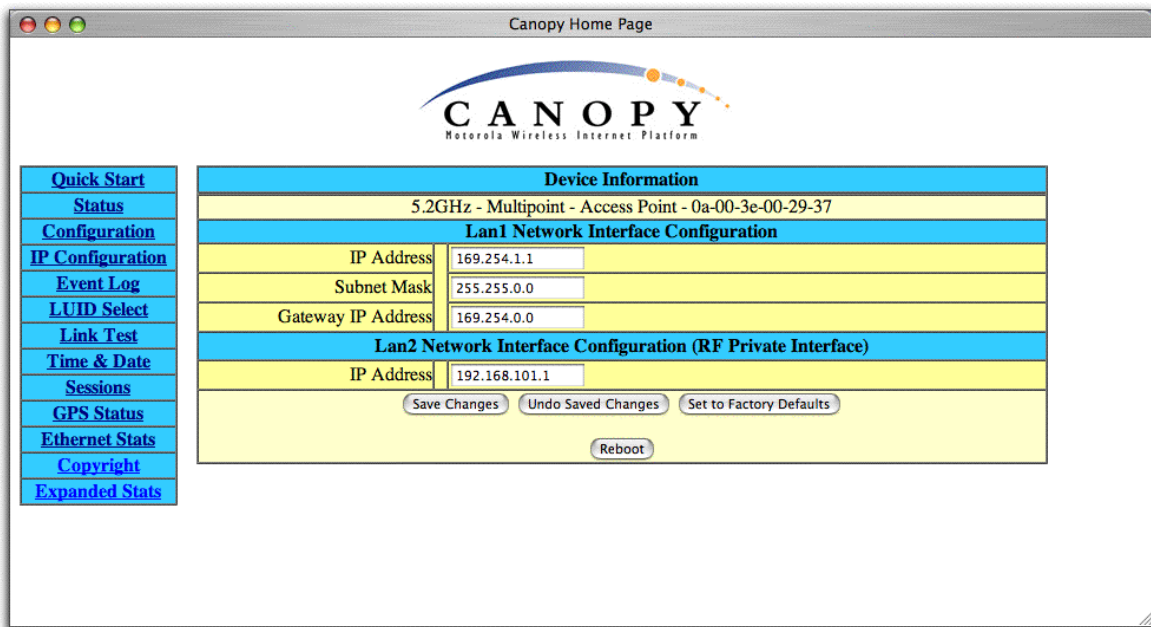


Figure 30: IP Configuration screen

8.4.1 IP Configuration Parameters

The IP Configuration page provides the following parameters:

LAN1 Network Interface Configuration, IP Address

The operator enters the *non-routable* IP address that will be associated with the Ethernet connection on this module. (The default IP address from the factory is 169.254.1.1.) If the operator-assigned IP address is forgotten, then the operator 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 IP Address and Password Setting](#) on Page 66.

LAN1 Network Interface Configuration, Subnet Mask

The operator enters an appropriate subnet mask for the module to communicate on the network. The default subnet mask is 255.255.255.0. See [General IP Addressing Concepts](#) on Page 58.

LAN1 Network Interface Configuration, Gateway IP Address

The operator enters the appropriate gateway for the module to communicate with the network. The default gateway is 169.254.0.0.

LAN2 Network Interface Configuration (RF Private Interface), IP Address

The operator should not change this parameter from the default *AP* private IP address of 192.168.101.1. A flat Class C 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

If the private IP address of the *AP* is changed, then the new address must

- designate a Class C subnet that is not used for anything else.
- have the form xxx.xxx.xxx.1, where 1 is the value of the last octet of the address.

NOTE: An SM is not required to have an operator-assigned IP address where space is limited for subnet allocation. 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.

8.4.2 IP Configuration Buttons

The IP Configuration page provides the following buttons:

Save Changes

When the operator clicks this button, any changes that have been made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When the operator clicks this button, any changes that have been made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When the operator clicks this button, all configurable parameters are reset to the factory settings.

Reboot

When the operator clicks this button, the module reboots. When the operator has changed parameters in the Configuration page, the system highlights **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

8.5 EVENT LOG PAGE

An example of an Event Log page is displayed in [Figure 31](#).

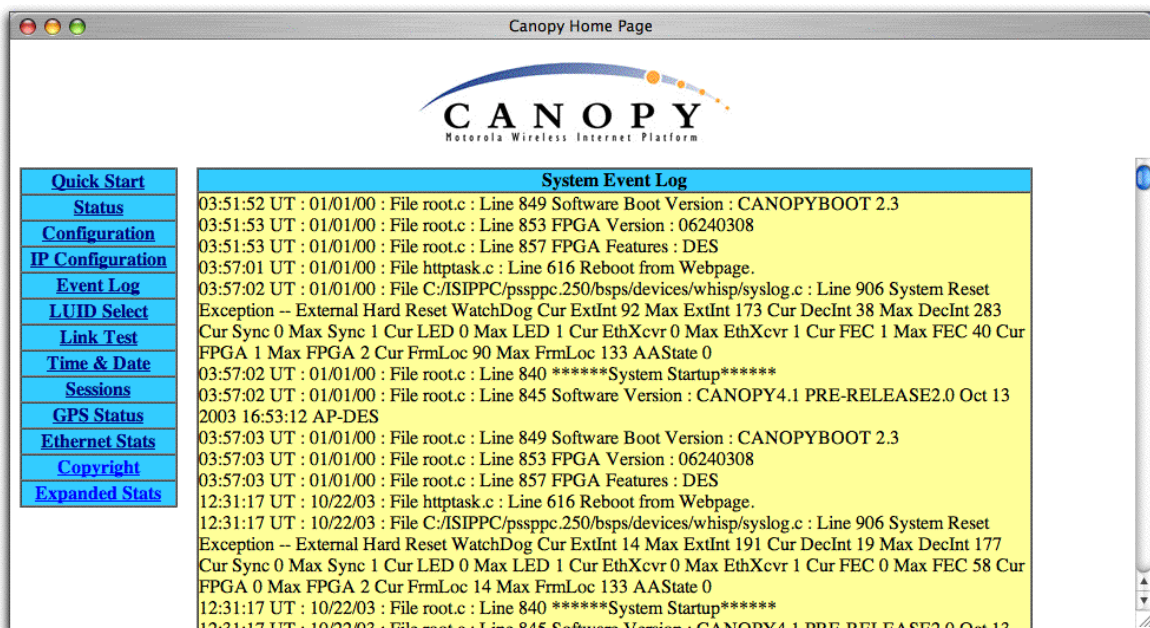


Figure 31: Event Log screen

This page may contain information that can be useful under the guidance of Canopy technical support. For this reason, the operator *should not* clear the contents of this page before contacting technical support.

8.5.1 Event Log Operator Option

The Event Log page provides only one button for the operator:

Clear Event Log

When the operator clicks this button, all of the Event Log data is cleared.

8.6 LUID SELECT PAGE

An example of an LUID Select screen is displayed in [Figure 32](#).

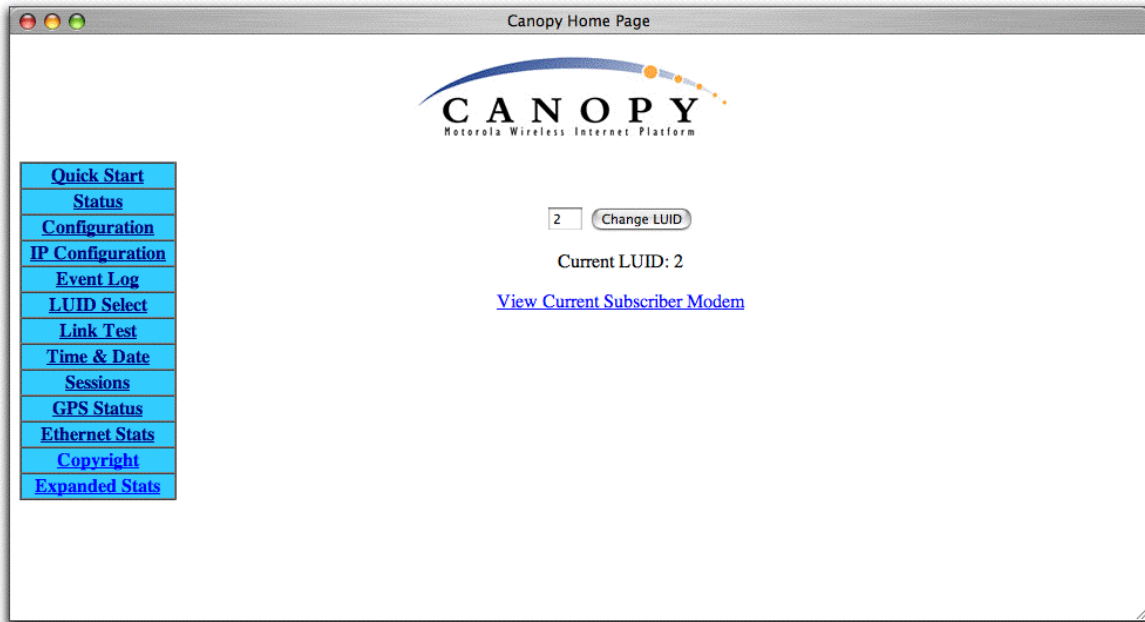


Figure 32: LUID Select screen

This web page allows the operator to view the web pages of registered SMs over the RF link.

Procedure 16: Viewing web pages for a selected SM

To view the pages for a selected SM, the operator

1. visits the Sessions web page to find the LUID (logical unit ID) that identifies the SM.
2. returns to the LUID Select web page.
3. enters the LUID into the **Change LUID** field (if the LUID differs from the LUID shown on the **Current LUID** line).
4. clicks the **Change LUID** button.
5. clicks **View Current Subscriber Modem** to access the SM.

8.7 LINK TEST PAGE

An example of the Link Capacity Test screen is displayed in [Figure 33](#).

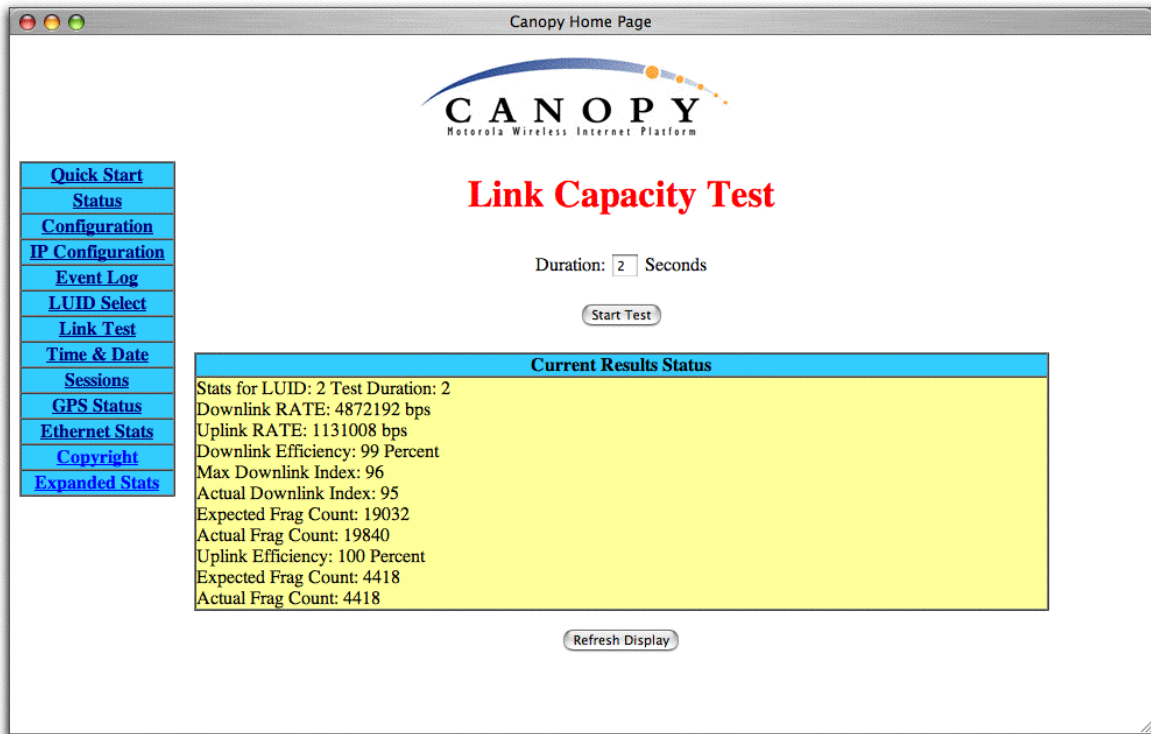


Figure 33: Link Test screen

The Link Capacity Test page allows the operator to measure the throughput and efficiency of the RF link between two Canopy modules.

Procedure 17: Testing a link

To test a link using this page, the operator

1. enters into the **Duration** field how long (in seconds) the RF link should be tested.
2. clicks the **Start Test** button.
3. clicks the **Refresh Display** button (if the web page is not set to automatically refresh).
4. views the results of the test.

8.7.1 Key Link Capacity Test Fields

The key fields in the test results are:

- **Downlink RATE**, expressed in bits per second
- **Uplink RATE**, expressed in bits per second
- **Downlink Efficiency**, expressed as a percentage
- **Uplink Efficiency**, expressed as a percentage.

8.7.2 Capacity Criteria for the Link

A Canopy system link is acceptable only if the efficiencies that the link test confirms are greater than 90% in both the uplink and downlink direction. When a new link is installed, a link test should be executed to ensure that the efficiencies are within this recommended guideline.

8.7.3 High-priority Bandwidth Planning

High-priority bandwidth planning information for uplink and downlink allocation is provided under [High-Priority Bandwidth](#) on Page 22.

8.8 TIME & DATE PAGE

An example of the Time & Date web page is displayed in [Figure 34](#).

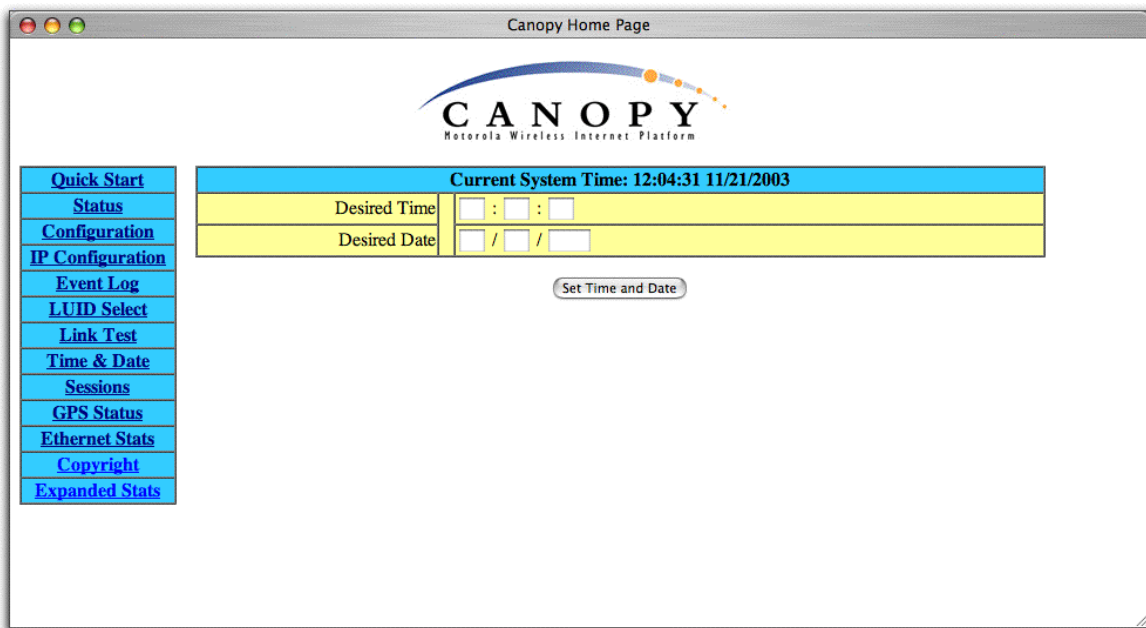


Figure 34: Time & Data screen

The Time & Date web page allows the operator to set the time and date for the AP. The operator must set the time and date whenever both

- the AP is not connected to a CMM.
- a power cycle of the AP has occurred.

The format for entry is

Time *hh:mm:ss*
Date *mm/dd/yyyy*
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

To set the time and date, the operator

1. enters the appropriate information in the format shown above.
2. clicks the **Set Time and Date** button.

8.9 SESSIONS PAGE

An example of the Sessions page is displayed in [Figure 35](#).

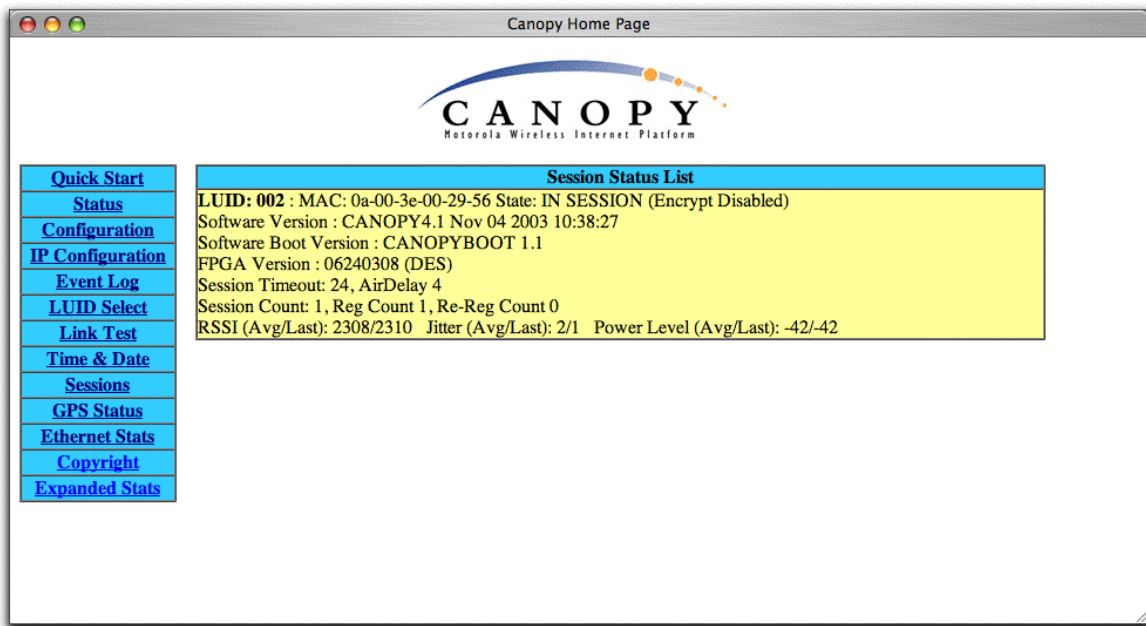


Figure 35: Example Sessions page data

The Session web page provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a Canopy system.

8.9.1 Sessions Parameters

The Sessions page 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 number to the SM. If an SM loses registration with the AP and then regains registration, the will retain the same LUID.

NOTE: The LUID association is lost when a power cycle of the AP occurs.

MAC

This field displays the MAC address (or electronic serial number) of the SM.

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.

Software Version

This field displays the software release that operates on the SM, the release date of the software, the time, and whether the module is secured by DES or AES encryption (see [Security Features](#) on Page 19). When requesting technical support, provide the information from this field.

An unpopulated **Software Version** parameter indicates a version earlier than Version 3.1.

Software Boot Version

This field indicates the CANOPYBOOT version number.

FPGA Version

This field displays the version of FPGA that runs on the SM. An unpopulated FPGA Version parameter indicates that a version earlier than Version 082002 runs on the SM.

Session Timeout

This field indicates the maximum interval in hours that the SM may sustain a single session with this AP.

AirDelay

This field displays the distance of the SM from the AP. To derive the distance in meters, the operator multiplies the displayed number by 0.3048. To derive the distance in feet, the operator multiplies the displayed number by 49.

Session Count

This field displays how many sessions the SM has had with the AP. If the number of sessions is far greater than the number that other SMs registered to the AP have had, then this SM may have an installation problem.

Reg Count

This field displays how many registration request messages the AP has received from the SM. If the number of these messages is far greater than the number from other SMs registered to the AP, then this SM may have an installation problem.

Re-Reg Count

This field displays how many registration request messages the AP has received from the SM that is already in session. If the number of these messages is far greater than the number from other SMs that are both registered to the AP and in session, then this SM may have an installation problem.

RSSI (Avg/Last)

This field displays the average and the latest RSSI (received signal strength indicator) value for the SM.

Jitter (Avg/Last)

This field displays the average and the latest jitter value for the SM.

Power Level (Avg/Last)

This field displays the average and the latest power level set for the SM.

8.10 GPS STATUS PAGE

An example of the GPS Status screen is displayed in [Figure 36](#).

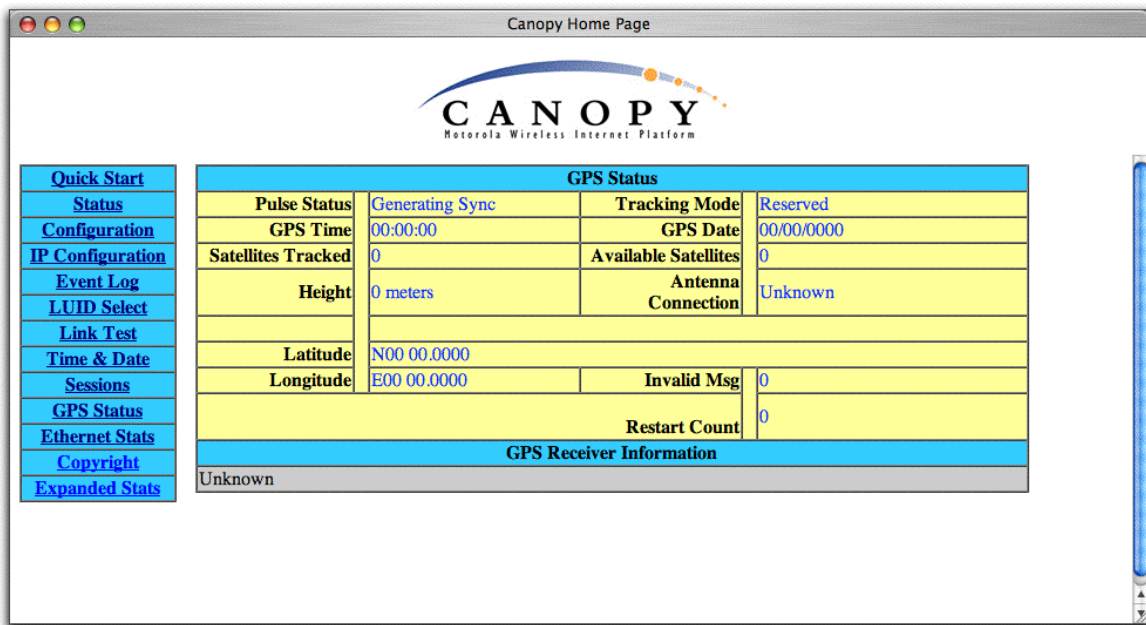


Figure 36: GPS Status screen

If the AP is configured to **Sync to Received Signal (Power Port)** and is connected to a CMMmicro, or is configured to **Sync to Received Signal (Timing Port)** and is connected to a CMM2, then the GPS Status web page provides information about satellites that are seen and tracked. See [Sync Input](#) on Page 79.

This page also displays the state of the antenna in the **Antenna Status** field as either Unknown or OK. This information may be helpful in a decision of whether to climb a tower to diagnose a perceived antenna problem.

8.11 ETHERNET STATS PAGE

The Ethernet Stats web page reports TCP throughput and error information for the Ethernet connection of the SM.

8.11.1 Ethernet Stats Parameters

The Ethernet Stats page provides the following parameters:

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.



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.

8.12 EXPANDED STATS PAGE

The Expanded Stats web page provides statistics that the Canopy module collects. To facilitate troubleshooting, a Canopy technical support representative may ask the operator for specific information from this web page.

The Expanded Stats page includes a link to a Reg Failed SMs web page, which provides

- the MAC address of each SM that attempted to register with this AP but failed.
- the time of the attempt.
- the reason for the failure.

A power cycle or reboot drops the contents of this page.

8.13 REG FAILED SMS PAGE

An example of the Reg Failed SMs screen is displayed in [Figure 37](#).

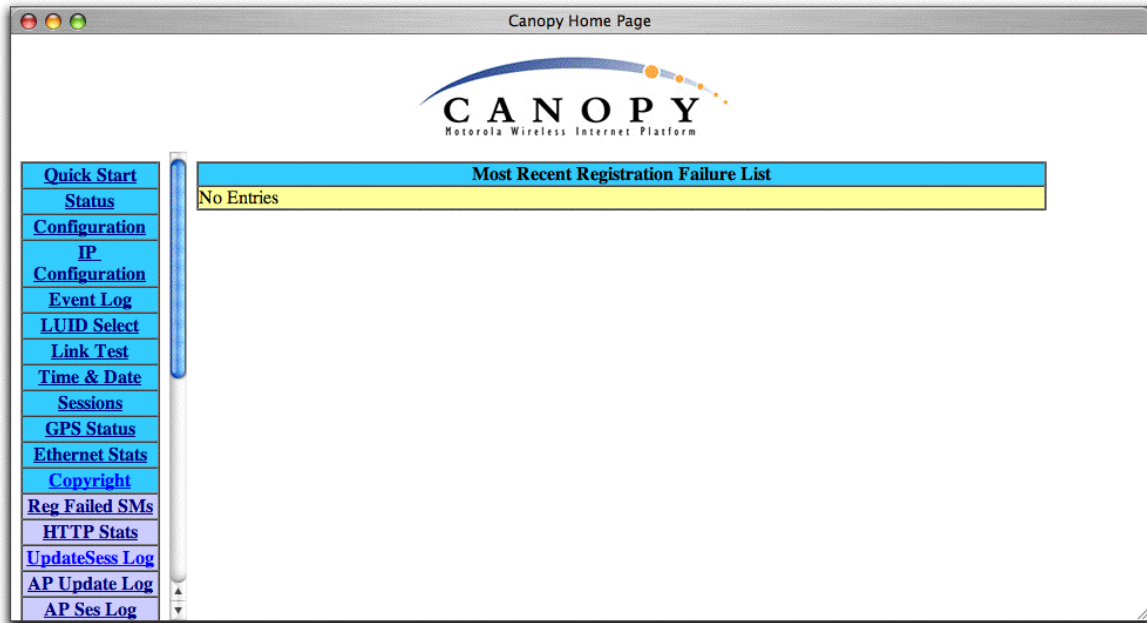


Figure 37: Reg Failed SMs screen

The Reg Failed SMs web page identifies SMs that have recently attempted and failed to register to this AP.

8.14 BRIDGE TABLE PAGE

An example of the Bridge Table screen is displayed in [Figure 38](#).

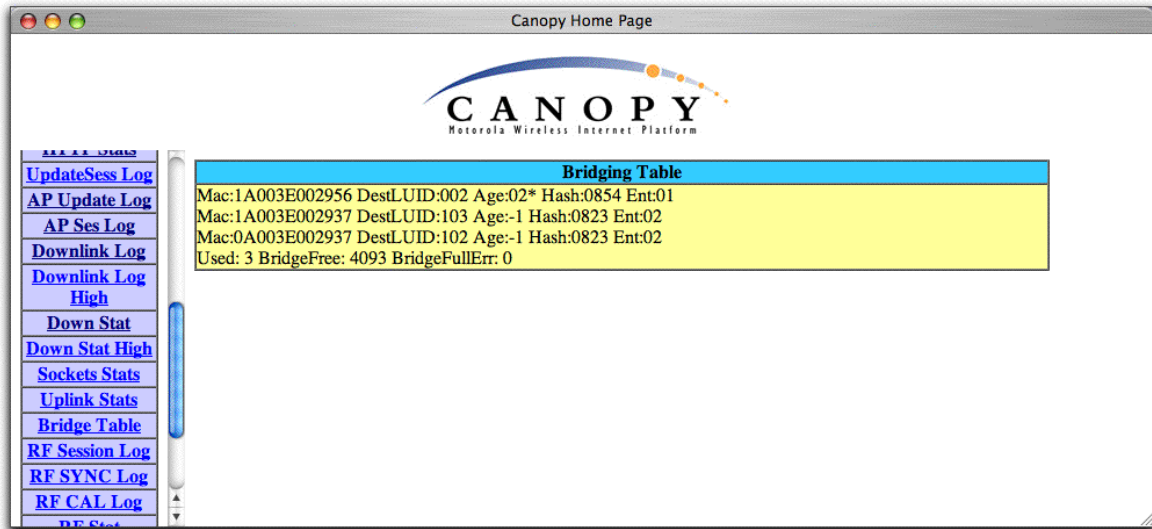


Figure 38: Bridge Table screen

If NAT (network address translation) is not active on this AP, then the Bridge Table web page provides the MAC addresses of the SMs for which this AP serves as a Layer 2 bridge.

9 CANOPY SYSTEM ACCESSORIES

The following accessories are available to use with the Canopy system. To purchase accessories, contact an authorized Canopy systems dealer unless otherwise noted.

- Universal mounting bracket
- Passive reflector dishes
- 102 – 132 VAC power supply with North American plug (Part Number ACPS110)
- 100 – 240 VAC power supply with North American, UK, and Euro plugs (Part Number ACPSSW-02)
- Cable assemblies for the Canopy system. These can be ordered from Best-Tronics Manufacturing, Inc. at <http://www.best-tronics.com/motorola>.

NOTE: For the RF environment in which Canopy BHs, APs, and CMMs typically operate, the use of shielded cable is *strongly* recommended for infrastructure cables that connect these modules.

10 AP MODULE SPECIFICATIONS

Table 13 provides the specifications of the Canopy AP.

Table 13: Specifications

Specification	Canopy System Range
Frequency Band Ranges	ISM: 2.4 to 2.4835 GHz U-NII: 5.25 to 5.35 GHz and 5.725 to 5.825 GHz ISM: 5.725 to 5.850 GHz
Access Method	TDD/TDMA
Signaling Rate	10 Mbps
Maximum Aggregate Throughput for 2.4-, 5.2-, and 5.7-GHz SMs	Downlink: 4.6 Mbps at default allocation of 75%, but variable based on packet size. Uplink: 1.6 Mbps at default allocation of 25%, but variable based on packet size.
Modulation Type	High-index 2-level FSK (Frequency Shift Keying) (Optimized for interference rejection)
Carrier to Interference (C/I)	3 dB nominal
Receiver Sensitivity	-83 dBm at 10^{-4} BER
Operating Range	Up to 2 miles (3.2 km) with integrated antenna in the 5.2-GHz band. Up to 5 miles (8 km) with integrated antenna in the 2.4-GHz band Up to 10 miles (16 km) with SM mounted to passive reflector in the 5.7-GHz band. Up to 15 miles (24 km) with SM mounted to passive reflector on the SM in the 2.4-GHz band.
Transmitter Power	~23 dBm Meets FCC U-NII/ISM and IC LELAN ERP Limit.
Antenna	Integrated patch. Vertically polarized. 60° x 60° beam width.
Antenna Gain	7 dB
F/B Ratio	15 dB
DC Power	0.3 A @ 24 VDC (7.2 watts) typical. 0.35 A @ 24 VDC (8.4 watts) maximum (long cable runs, high ambient temperature, high transmit ratio). Set by downlink percentage.

Specification	Canopy System Range
Ethernet, GPS sync, and GPS coax cables	The use of cables that are rated for the operation temperature of the product and that conform to UV light protection specifications is mandatory. The use of shielded cables is strongly recommended. For information about the supplier of these cables, see CANOPY SYSTEM ACCESSORIES on Page 99.
Interface	10/100BaseT, half/full duplex. Rate auto-negotiated (802.3 compliant).
Protocols Used	IPV4, UDP, TCP, ICMP, Telnet, HTTP, FTP, SNMP, DES. Optionally, AES.
Protocols Supported	Switched Layer 2 Transport with support for all common Ethernet protocols, such as IPV6, NetBIOS, DHCP, IPX.
Software Upgrade Path	Remotely downloaded into flash memory
Network Management	HTTP, telnet, FTP, SNMP
Operation Temperature	-40° F to +131° F (-40° C to +55° C)
Weight	1 lb (0.45 kg) without passive reflector
Reflector Dish Weight	6.5 lb (2.9 kg) with assembly, without module
Dimensions	11.75" H x 3.4" W x 3.4" D (29.9 cm H x 8.6 cm W x 8.6 cm D)
Reflector Dish Dimensions	18" H x 24" W (45.7 cm H x 61.0 cm W)
Mean Time Between Failure (MTBF)	40 years
Mean Time to Repair (MTTR)	15 minutes

11 HISTORY OF CHANGES IN THIS DOCUMENT

Issue 4 introduced the following changes:

- Information that supports Release 4.1 features
- Information that supports 2.4-GHz modules

Issue 3 introduced the following changes:

- AES (Advanced Encryption Standard) security product description
- 5.7-GHz ISM support of 6 channels (increased from 4 with 5.7-GHz U-NII)
- 5.7-GHz ISM frequencies approved for use in Canada as in the U.S.A.
- Maximum Access Point Module power increased to 8.4 watts
- Strong recommendation of shielded cables for all infrastructure cabling that connects
 - Access Point Modules (APs)
 - Backhaul Modules (BHs)
 - Cluster Management Modules (CMMs).
- List of MAC (Media Access Control) addresses for older modules that *do not* automatically sense the cabling scheme (These modules require the installer to correctly choose whether to use straight-thru or crossover cables.)

Issue 2 introduced the following changes:

- Updates in the Notices section for
 - European Community Notification.
 - RF Exposure.
 - software license terms and conditions.
- Internationalization of measurement units to provide metric units aside the English units
- Updates for new hardware features, to reflect that modules that are shipped from the publication date forward
 - auto-sense the Ethernet termination (Either a straight-thru or crossover RJ-45 cable can be used to connect to either a network interface card or a hub, switch, or router.)
 - include additional cable openings to facilitate shielded cable installation.
- Description of the Canopy Bandwidth and Authentication Manager (BAM) and BAM features, which provide bandwidth and security above what an AP without the BAM provides.
- Changes in specifications to
 - reflect the expanded lower temperature limit (-40°F/-40°C) for all equipment.
 - provide clarifications for and add information about the CE Listing for the European Community.