REFERENCE INFORMATION

35 ADMINISTERING MODULES THROUGH TELNET INTERFACE

In the telnet administrative interface to a module, the Canopy platform supports the commands defined in Table 70. Many of these are not needed with CNUT.

Table 70: Supported telnet commands for module administration

Command	System help Definition	Notes
`addwebfile`	`Add a custom web file`	Syntax: **`addwebfile`** ***`filename`***. Copies the custom web file *`filename`* to non-volatile memory.
`burnfile`	`Burn flash from file`	Syntax: **`burnfile`** ***`filename`***. Updates the CPU firmware with a new image. User the image contained in *`filename`* if *`filename`* is provided. If provided, *`filename`* must match the module type (for example, `SMboot.bin` for a Subscriber Module or `APboot.bin` for an Access Point Module).
`cat`	`Concatenate and display.`	Syntax: **`cat`** ***`filename`***. Displays the contents of *`filename`*.
`clearsyslog`	`Clear the system event log`	Syntax: **`clearsyslog`**. Clears the system event log.
`clearwebfile`	`Clear all custom web files`	Syntax: **`clearwebfile`**. Deletes all *custom* web files.
`exit`	`Exit from telnet session`	Syntax: **`exit`**. Terminates the telnet interface session.
`fpga_conf`	`Update FPGA program`	Syntax: **`fpga_conf`**. Forces a module to perform a hard (FPGA and CPU) reset. (See reset.)
`ftp`	`File transfer application`	Syntax: **`ftp`**. Launches the ftp client application on the module.
`help`	`Display command line function help`	Syntax: **`help`**. Displays a list of available telnet commands and a brief description of each.
`jbi`	`Update FPGA program`	Syntax: **`jbi -aprogram`** ***`file.jbc`***. Updates the FPGA firmware with the new image contained in *`file.jbc`*.
`ls`	`List the contents of a directory`	Syntax: **`ls`**. Lists the file names of all files in the directory. Syntax: **`ls -l`**. Displays additional information, such as the sizes and dates of the files.
`lsweb`	`List Flash Web files`	Syntax: **`lsweb`**. Lists the file names of the saved custom web files.

Command	System help Definition	Notes
`ping`	`Send ICMP ECHO_REQUEST packets to network hosts`	Syntax: **`ping`** ***`IPaddress`***. Sends an ICMP ECHO_REQUEST to *`IPaddress`* and waits for a response. If a response is received, the system returns *`IPaddress`* `is alive`. If no response is received, the system returns `no answer from` *`IPaddress`*.
`reset`	`Reboot the unit`	Syntax: **`reset`**. Forces the module to perform a hard (FPGA and CPU) module reset. (See **`fpga_conf`**.)
`rm`	`Remove (unlink) files`	Syntax: **`rm`** ***`filename`***. Remove *`filename`*.
`syslog`	`Display system event log: syslog <optional filename>`	Syntax: **`syslog`**. Displays the contents of the system log. Syntax: **`syslog`** ***`filename`***. Saves the contents of the system log to *`filename`*. Caution: overwrites *`filename`* if it already exists.
`telnet`	`Telnet application`	Syntax: **`telnet`** ***`hostIPaddress`***. Launches the telnet client application on the Canopy module.
`tftp`	`tftp application`	Syntax: **`tftp`** ***`hostIPaddress`***. Launches the tftp client application on the Canopy module.
`update`	`Enable automatic SM code updating`	Syntax: **`update`** ***`actionlist.txt`***. Enables the automated update procedure that *`actionlist.txt`* specifies. (Supported for only the Access Point Module.)
`updateoff`	`Disable automatic SM code updating`	Syntax: **`updateoff`**. Disables the automated update procedure.
`version`	`Display the software version string`	Syntax: **`version`**. Displays the module version string, which contains the software/firmware/hardware versions, the module type, and the operating frequency.

36 LEGAL AND REGULATORY NOTICES

36.1 IMPORTANT NOTE ON MODIFICATIONS

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

36.2 NATIONAL AND REGIONAL REGULATORY NOTICES

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

This device complies with Part 15 of the US 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 US 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 Table 71:

Table 71: US FCC IDs and Industry Canada certification numbers

Module Types	Operating Frequency Range	Maximum Transmitter Output Power	Reflector or Antenna	FCC ID	Industry Canada Certification Number
SM AP	ISM 902 to 928 MHz	24 dBm (250 mW) 26 dBm (400 mW) 26 dBm (400 mW) 26 dBm (400 mW)	Canopy integrated antenna with 12 dBi gain Maxrad Model # Z1681, flat panel with 10 dBi gain Mars Model # MA-IS91-T2, flat panel with10 dBi gain MTI Model # MT-2630003/N, flat panel with 10 dBi gain	ABZ89FC5809	109W-9000ISM
SM AP BH	ISM 2400-2483.5 MHz	25 dBm (340 mW)	Allowed on SM and BH	ABZ89FC5808	109W-2400
SM AP BH	U-NII 5250-5350 MHz	23 dBm (200 mW)	Not Allowed	ABZ89FC3789	109W-5200
BH	U-NII 5250-5350 MHz	5 dBm (3.2 mW)	Recommended	ABZ89FC5807	109W-5210
SM AP BH	ISM 5725-5850 MHz	23 dBm (200 mW)	Allowed on SM and BH	ABZ89FC5804	109W-5700
AP	ISM 5725-5850 MHZ	21 dBM (125 mW)	Mars Model # MA-WC50-5H antenna with 15.5 dBi gain	ABZ89FT7622	none

36.2.2 Regulatory Requirements for CEPT Member States (http://www.cept.org)

When operated in accordance with the instructions for use, Motorola Canopy Wireless equipment operating in the 2.4 and 5.4 GHz bands is compliant with CEPT Recommendation 70-03 Annex 3 for Wideband Data Transmission and HIPERLANs. For compliant operation in the 2.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 100mW (20dBm). For compliant operation in the 5.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 1 W (30 dBm).

The following countries have completely implemented CEPT Recommendation 70-03 Annex 3A (2.4 GHz band):

- EU & EFTA countries: Austria, Belgium, Denmark, Spain, Finland, Germany, Greece, Iceland, Italy, Ireland, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Switzerland, Sweden, UK
- New EU member states: Czech Republic, Cyprus, Estonia, Hungary, Lithuania, Latvia, Malta, Poland, Slovenia, Slovakia
- Other non-EU & EFTA countries: Bulgaria, Bosnia and Herzegovina, Turkey

The following countries have a limited implementation of CEPT Recommendation 70-03 Annex 3A:

- France **-** Outdoor operation at 100mW is only permitted in the frequency band 2400 to 2454 MHz;
  - Any outdoor operation in the band 2454 to 2483.5MHz shall not exceed 10mW (10dBm);
  - Indoor operation at 100mW (20dBm) is permitted across the band 2400 to 2483.5 MHz
- French Overseas Territories:
  - Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte – 100mW indoor & outdoor is allowed
  - Réunion and Guyana – 100mW indoor, no operation outdoor in the band 2400 to 2420MHz
- Italy - If used outside own premises, general authorization required
- Luxembourg **-** General authorization required for public service
- Romania - Individual license required. T/R 22-06 not implemented

Motorola Canopy Radios operating in the 2400 to 2483.5MHz band and 5470 to 5725 MHz band are categorized as “Class 2” devices within the EU and are marked with the class identifier symbol (!), denoting that national restrictions apply (for example, France). The French restriction in the 2.4 GHz band will be removed in 2011. Users are advised to contact their national administrations for the current status on the implementation of ECC DEC(04)08 for the 5.4GHz band.

This equipment is “CE” marked CE(!) to show compliance with the European Radio & Telecommunications Terminal Equipment (R&TTE) directive 1999/5/EC. The relevant Declaration of Conformity can be found at http://www.canopywireless.com/doc.php.

Where necessary, the end user is responsible for obtaining any National licenses required to operate this product and these must be obtained before using the product in any particular country. However, for CEPT member states, 2.4 GHz Wideband Data Transmission equipment has been designated exempt from individual licensing under decision ERC/DEC(01)07. For EU member states, RLAN equipment in both the 2.4 & 5.4GHz bands is exempt from individual licensing under Commission Recommendation 2003/203/EC. Contact the appropriate national administrations for details on the conditions of use for the bands in question and any exceptions that might apply. Also see http://www.ero.dk for further information.

36.2.3 European Union Notification

The 5.7 GHz connectorized product is a two-way radio transceiver suitable for use in Broadband Wireless Access System (WAS), Radio Local Area Network (RLAN), or Fixed Wireless Access (FWA) systems. It is a Class 2 device and uses operating frequencies that are not harmonized throughout the EU member states. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country.

This equipment is marked CE (!) 0977 to show compliance with the European R&TTE directive 1999/5/EC.

The relevant Declaration of Conformity can be found at http://www.canopywireless.com/doc.php.

A European Commission decision, which is to be implemented by Member States by 31 October 2005, makes the frequency band 5470-5725 MHz available in all EU Member States for wireless access systems. Under this decision, the designation of Canopy 5.4GHz products become "Class 1 devices" and these do not require notification under article 6, section 4 of the R&TTE Directive. Consequently, these 5.4GHz products are only marked with the CE symbol and may be used in any member state.

For further details, see http://europa.eu.int/information_society/policy/radio_spectrum/ref_documents/index_en.htm.

36.2.4 UK Notification

The 5.7 GHz connectorized product has been notified for operation in the UK, and when operated in accordance with instructions for use it is compliant with UK Interface Requirement IR2007. For UK use, installations must conform to the requirements of IR2007 in terms of EIRP spectral density against elevation profile above the local horizon in order to protect Fixed Satellite Services. The frequency range 5795-5815 MHz is assigned to Road Transport & Traffic Telematics (RTTT) in the U.K. and shall not be used by FWA systems in order to protect RTTT devices. UK Interface Requirement IR2007 specifies that radiolocation services shall be protected by a Dynamic Frequency Selection (DFS) mechanism to prevent co-channel operation in the presence of radar signals.

36.2.5 Belgium Notification

Belgium national restrictions in the 2.4 GHz band include

- EIRP must be lower than 100 mW
- For crossing the public domain over a distance > 300m the user must have the authorization of the BIPT.
- No duplex working

36.2.6 Luxembourg Notification

For the 2.4 GHz band, point-to-point or point-to-multipoint operation is only allowed on campus areas. 5.4GHz products can only be used for mobile services.

36.2.7 Czech Republic Notification

2.4 GHz products can be operated in accordance with the Czech General License No. GL-12/R/2000.

5.4 GHz products can be operated in accordance with the Czech General License No. GL-30/R/2000.

36.2.8 Norway Notification

Use of the frequency bands 5725-5795 / 5815-5850 MHz are authorized with maximum radiated power of 4 W EIRP and maximum spectral power density of 200 mW/MHz. The radio equipment shall implement Dynamic Frequency Selection (DFS) as defined in Annex 1 of ITU-R Recommendation M.1652 / EN 301 893. Directional antennae with a gain up to 23 dBi may be used for fixed point-to-point links. The power flux density at the border between Norway and neighbouring states shall not exceed - 122.5 dBW/m^2 measured with a reference bandwidth of 1 MHz.

Canopy 5.7 GHz connectorized products have been notified for use in Norway and are compliant when configured to meet the above National requirements. Users shall ensure that DFS functionality is enabled, maximum EIRP respected for a 20 MHz channel, and that channel spacings comply with the allocated frequency band to protect Road Transport and Traffic Telematics services (for example, 5735, 5755, 5775 or 5835 MHz are suitable carrier frequencies). Note that for directional fixed links, TPC is not required, conducted transmit power shall not exceed 30 dBm, and antenna gain is restricted to 23 dBi (maximum of 40W from the Canopy 5.7 GHz connectorized products).

36.2.9 Greece Notification

The outdoor use of 5470-5725MHz is under license of EETT but is being harmonized according to the CEPT Decision ECC/DEC/(04) 08, of 9th July. End users are advised to contact the EETT to determine the latest position and obtain any appropriate licenses.

36.2.10 Brazil Notification

Local regulations do not allow the use of 900 MHz, 2.4 GHz, or 5.2 GHz Canopy modules in Brazil, nor do they allow the use of passive reflectors on 5.4 or 5.7 GHz Canopy Access Points.

For compliant operation in the 5.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 1 W (30 dBm). When using the passive reflector along with a 5.4 GHz Canopy radio, the transmitter output power of the radio must be configured no higher than 5 dBm. When not using the passive reflector, the transmitter output power of the radio must be configured no higher than 23 dBm.

The operator is responsible for enabling the DFS feature on any Canopy 5.4 GHz radio, and re-enabling it if the module is reset to factory defaults.

Important Note

This equipment operates as a secondary application, so it has no rights against harmful interference, even if generated by similar equipment, and cannot cause harmful interference on systems operating as primary applications.

36.2.11 Australia Notification

900 MHz modules must be set to transmit and receive only on 922 or 923 MHz so as to stay within the ACMA approved band of 915 MHz to 928 MHz for the class license and not interfere with other approved users.

After taking into account antenna gain (in dBi), 900 MHz modules’ transmitter output power (in dBm) must be set to stay within the legal regulatory limit of 30 dBm (1 W) EIRP for this 900 MHz frequency band.

36.3 EXPOSURE

See Preventing Overexposure to RF on Page 169.

36.4 EQUIPMENT DISPOSAL

Waste (Disposal) of your Electronic and Electric Equipment

Please do not dispose of Electronic and Electric Equipment or Electronic and Electric Accessories with your household waste. In some countries or regions, collection systems have been set up to handle waste of electrical and electronic equipment. In European Union countries, please contact your local equipment supplier representative or service centre for information about the waste collection system in your country.

36.5 LEGAL NOTICES

36.5.1 Software License Terms and Conditions

ONLY OPEN THE PACKAGE, OR USE THE SOFTWARE AND RELATED PRODUCT IF YOU ACCEPT THE TERMS OF THIS LICENSE. BY BREAKING THE SEAL ON THIS DISK KIT / CDROM, OR IF YOU USE THE SOFTWARE OR RELATED PRODUCT, YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SOFTWARE OR RELATED PRODUCT; INSTEAD, RETURN THE SOFTWARE

TO PLACE OF PURCHASE FOR A FULL REFUND. THE FOLLOWING AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR ENTITY), AND MOTOROLA, INC. (FOR ITSELF AND ITS LICENSORS). THE RIGHT TO USE THIS PRODUCT IS LICENSED ONLY ON THE CONDITION THAT YOU AGREE TO THE FOLLOWING TERMS.

Now, therefore, in consideration of the promises and mutual obligations contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby mutually acknowledged, you and Motorola agree as follows:

Grant of License. Subject to the following terms and conditions, Motorola, Inc., grants to you a personal, revocable, non-assignable, non-transferable, non-exclusive and limited license to use on a single piece of equipment only one copy of the software contained on this disk (which may have been pre-loaded on the equipment)(Software). You may make two copies of the Software, but only for backup, archival, or disaster recovery purposes. On any copy you make of the Software, you must reproduce and include the copyright and other proprietary rights notice contained on the copy we have furnished you of the Software.

Ownership. Motorola (or its supplier) retains all title, ownership and intellectual property rights to the Software and any copies,

including translations, compilations, derivative works (including images) partial copies and portions of updated works. The Software is Motorola’s (or its supplier's) confidential proprietary information. This Software License Agreement does not convey to you any interest in or to the Software, but only a limited right of use. You agree not to disclose it or make it available to anyone without Motorola’s written authorization. You will exercise no less than reasonable care to protect the Software from unauthorized disclosure. You agree not to disassemble, decompile or reverse engineer, or create derivative works of the Software, except and only to the extent that such activity is expressly permitted by applicable law.

Termination. This License is effective until terminated. This License will terminate immediately without notice from Motorola or judicial resolution if you fail to comply with any provision of this License. Upon such termination you must destroy the Software, all accompanying written materials and all copies thereof, and the sections entitled Limited Warranty, Limitation of Remedies and Damages, and General will survive any termination.

Limited Warranty. Motorola warrants for a period of ninety (90) days from Motorola’s or its customer’s shipment of the Software to you that (i) the disk(s) on which the Software is recorded will be free from defects in materials and workmanship under normal use and (ii) the Software, under normal use, will perform substantially in accordance with Motorola’s published specifications for that release level of the Software. The written materials are provided "AS IS" and without warranty of any kind. Motorola's entire liability and your sole and exclusive remedy for any breach of the foregoing limited warranty will be, at Motorola's option, replacement of the disk(s), provision of downloadable patch or replacement code, or refund of the unused portion of your bargained for contractual benefit up to the amount paid for this Software License.

THIS LIMITED WARRANTY IS THE ONLY WARRANTY PROVIDED BY MOTOROLA, AND MOTOROLA AND ITS LICENSORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OF IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. MOTOROLA DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN REPRESENTATIONS MADE BY MOTOROLA OR AN AGENT THEREOF SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. MOTOROLA DOES NOT WARRANT ANY SOFTWARE THAT HAS BEEN OPERATED IN EXCESS OF SPECIFICATIONS, DAMAGED, MISUSED, NEGLECTED, OR IMPROPERLY INSTALLED. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Limitation of Remedies and Damages. Regardless of whether any remedy set forth herein fails of its essential purpose, IN NO EVENT SHALL MOTOROLA OR ANY OF THE LICENSORS, DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES OF THE FOREGOING BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL OR SIMILAR DAMAGES

WHATSOEVER (including, without limitation, damages for loss of business profits, business interruption, loss of business information and the like), whether foreseeable or unforeseeable, arising out of the use or inability to use the Software or accompanying written materials, regardless of the basis of the claim and even if Motorola or a Motorola representative has been advised of the possibility of such damage. Motorola's liability to you for direct damages for any cause whatsoever, regardless of the basis of the form of the action, will be limited to the price paid for the Software that caused the damages. THIS LIMITATION WILL NOT APPLY IN CASE OF PERSONAL INJURY ONLY WHERE AND TO THE EXTENT THAT APPLICABLE LAW REQUIRES SUCH LIABILITY. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Maintenance and Support. Motorola shall not be responsible for maintenance or support of the software. By accepting the license granted under this agreement, you agree that Motorola will be under no obligation to provide any support, maintenance or service in connection with the Software or any application developed by you. Any maintenance and support of the Related Product will be provided under the terms of the agreement for the Related Product.

Transfer. In the case of software designed to operate on Motorola equipment, you may not transfer the Software to another party except: (1) if you are an end-user, when you are transferring the Software together with the Motorola equipment on which it operates; or 2) if you are a Motorola licensed distributor, when you are transferring the Software either together with such Motorola equipment or are transferring the Software as a licensed 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 US Government.

Right to Audit. Motorola shall have the right to audit annually, upon reasonable advance notice and during normal business hours, your records and accounts to determine compliance with the terms of this Agreement.

Export Controls. You specifically acknowledge that the software may be subject to United States and other country export control laws. You shall comply strictly with all requirements of all applicable export control laws and regulations with respect to all such software and materials.

US Government Users. If you are a US Government user, then the Software is provided with "RESTRICTED RIGHTS" as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at FAR 52 227-19 or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, as applicable.

Disputes. You and Motorola hereby agree that any dispute, controversy or claim, except for any dispute, controversy or claim involving intellectual property, prior to initiation of any formal legal process, will be submitted for non-binding mediation, prior to initiation of any formal legal process. Cost of mediation will be shared equally. Nothing in this Section will prevent either party from resorting to judicial proceedings, if (i) good faith efforts to resolve the dispute under these procedures have been unsuccessful, (ii) the dispute, claim or controversy involves intellectual property, or (iii) interim relief from a court is necessary to prevent serious and irreparable injury to that party or to others.

General. Illinois law governs this license. The terms of this license are supplemental to any written agreement executed by both parties regarding this subject and the Software Motorola is to license you under it, and supersedes all previous oral or written communications between us regarding the subject except for such executed agreement. It may not be modified or waived except in writing and signed by an officer or other authorized representative of each party. If any provision is held invalid, all other provisions shall remain valid, unless such invalidity would frustrate the purpose of our agreement. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent action in the event of future breaches.

36.5.2 Hardware Warranty in U.S.

Motorola U.S. offers a warranty covering a period of one year from the date of purchase by the customer. If a product is found defective during the warranty period, Motorola will repair or replace the product with the same or a similar model, which may be a reconditioned unit, without charge for parts or labor.

36.5.3 Limit of Liability

IN NO EVENT SHALL MOTOROLA BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.) IN NO CASE SHALL MOTOROLA'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

37 ADDITIONAL RESOURCES

Canopy provides two additional resources where you can raise questions and find answers:

- Canopy Community Forums at http://motorola.canopywireless.com/support/community/.
  This resource facilitates communication with other users and with authorized Canopy experts. Available forums include General Discussion, Network Monitoring Tools, and Suggestions.
- Canopy Knowledge Base at http://motorola.canopywireless.com/support/knowledge.
  This resource facilitates exploration and searches, provides recommendations, and describes tools. Available categories include
  - General (Answers to general questions provide an overview of the Canopy system.)
  - Product Alerts
  - Helpful Hints
  - FAQs (frequently asked questions)
  - Hardware Support
  - Software Support
  - Tools

38 HISTORY OF DOCUMENTATION

This section is a placeholder where changes for Issue 2 and later of this *Canopy System Release 8 User Guide* will be listed.

GLOSSARY

~. The command that terminates an SSH Secure Shell session to another server. Used on the Bandwidth and Authentication Manager (BAM) master server in the database replication setup.

10Base-T Technology in Ethernet communications that can deliver 10 Mb of data across 328 feet (100 meters) of CAT 5 cable.

100Base-TX Technology in Ethernet communications that can deliver 100 Mb of data across 328 feet (100 meters) of CAT 5 cable.

169.254.0.0 Gateway IP address default in Canopy modules.

169.254.1.1 IP address default in Canopy modules.

169.254.x.x IP address default in Microsoft and Apple operating systems without a DHCP (Dynamic Host Configuration Protocol) server.

255.255.0.0 Subnet mask default in Canopy modules and in Microsoft and Apple operating systems.

802.3 An IEEE standard that defines the contents of frames that are transferred through Ethernet connections. Each of these frames contains a preamble, the address to which the frame is sent, the address that sends the frame, the length of the data to expect, the data, and a checksum to validate that no contents were lost.

802.11 The IEEE standard for wireless local area networks.

802.15 The IEEE standard for wireless personal area networks.

Access Point Cluster Two to six Access Point Modules that together distribute network or Internet services to a community of 1,200 or fewer subscribers. Each Access Point Module covers a 60° sector. This cluster covers as much as 360°. Also known as AP cluster.

Access Point Module Also known as AP. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.

ACT/4 Second-from-left LED in the module. In the operating mode, this LED is lit when data activity is present on the Ethernet link. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.

Activate To provide feature capability to a module, but not to *enable* (turn on) the feature in the module. See also Enable.

Address Resolution Protocol Protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.

Advanced Encryption Standard
Over-the-air link option that provides extremely secure wireless connections. Advanced Encryption Standard (AES) uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.

AES
See Advanced Encryption Standard.

Aggregate Throughput
The sum of the throughputs in the uplink and the downlink.

AP
Access Point Module. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.

APA
Access Point module address.

Apache
A trademark of Apache Software Foundation, used with permission.

APAS
Access Point Authentication Server. Licensed to authenticate SMs that attempt to register to it. The AP licensed as APAS may or may not have authentication *enabled* (turned on). See also Activate and Enable.

API
Application programming interface for web services that supports Prizm integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system.

APs MIB
Management Information Base file that defines objects that are specific to the Access Point Module or Backhaul timing master. See also Management Information Base.

ARP
Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.

ASN.1
Abstract Syntax Notation One language. The format of the text files that compose the Management Information Base.

Attenuation
Reduction of signal strength caused by the travel from the transmitter to the receiver, and caused by any object between. In the absence of objects between, a signal that has a short wavelength experiences a high degree of attenuation nevertheless.

Authentication Key
Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f, padded with leading zeroes in Release 4.2.3 and later. This key must be unique to the individual SM.

Backhaul Module Also known as BH. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module. See also Backhaul Timing Master and Backhaul Timing Slave.

Backhaul Timing Master Backhaul Module that sends network timing (synchronization) to another Backhaul Module, which serves as the Backhaul timing slave.

Backhaul Timing Slave Backhaul Module that receives network timing (synchronization) from another Backhaul Module, which serves as the Backhaul timing master.

BAM Bandwidth and Authentication Manager. A Canopy software product that operates on a Linux server to manage bandwidth, high-priority channel, and VLAN settings individually for each registered Subscriber Module. This software also provides secure Subscriber Module authentication and user-specified encryption keys. The upgrade path for this product is to Prizm Release 2.0 or later.

BER Bit Error Rate. The ratio of incorrect data received to correct data received.

BH Backhaul Module. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module.

Bit Error Rate Ratio of incorrect data received to correct data received.

Box MIB Management Information Base file that defines module-level objects. See also Management Information Base.

BRAID Stream cipher that the TIA (Telecommunications Industry Association) has standardized. The secret keys in both modules communicate with each other to establish the Data Encryption Standard key. See Data Encryption Standard.

Bridge Network element that uses the physical address (not the logical address) of another to pass data. The bridge passes the data to either the destination address, if found in the simple routing table, or to all network segments other than the one that transmitted the data. Canopy modules are Layer 2 bridges except that, where NAT is enabled for an SM, the SM is a Layer 3 switch. Compare to Switch and Router, and see also NAT.

Bridge Entry Timeout Field Value that the operator sets as the maximum interval for no activity with another module, whose MAC address is the Bridge Entry. This interval should be longer than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

Buckets Theoretical data repositories that can be filled at preset rates or emptied when preset conditions are experienced, such as when data is transferred.

Burst Preset amount limit of data that may be continuously transferred.

C/I Ratio Ratio of intended signal (carrier) to unintended signal (interference).

Canopy A trademark of Motorola, Inc.

canopy.xml File that stores specifications for the Bandwidth and Authentication Manager (BAM) GUI.

Carrier-to-interference Ratio Ratio of intended reception to unintended reception.

CarSenseLost Field This field displays how many carrier sense lost errors occurred on the Ethernet controller.

CAT 5 Cable Cable that delivers Ethernet communications from module to module. Later modules auto-sense whether this cable is wired in a straight-through or crossover scheme.

cdf Canopy Data Formatter tool that creates an initial ESN Data Table. Inputs for this tool include a list of SM ESNs and default values of sustained data rates and burst allocations for each listed ESN.

chkconfig A command that the Linux® operating system accepts to enable MySQL® and Apache™ Server software for various run levels of the mysqld and httpd utilities.

CIR See Committed Information Rate.

Cluster Management Module Module that provides power, GPS timing, and networking connections for an AP cluster. Also known as CMM. If this CMM is connected to a Backhaul Module, then this CMM is the central point of connectivity for the entire site.

CMM Cluster Management Module. A module that provides power, GPS timing, and networking connections for an Access Point cluster. If this CMM is connected to a Backhaul Module (BH), then this CMM is the central point of connectivity for the entire site.

CodePoint See DiffServ.

Color Code Field Module parameter that identifies the other modules with which communication is allowed. The range of values is 0 to 255. When set at 0, the Color Code does not restrict communications with any other module.

Committed Information Rate For an SM or specified group of SMs, a level of bandwidth that can be guaranteed to never fall below a specified minimum. In the Canopy implementation, this is controlled by the Low Priority Uplink CIR, Low Priority Downlink CIR, High Priority Uplink CIR, and High Priority Downlink CIR parameters.

Community String Field Control string that allows a network management station to access MIB information about the module.

CPE Customer premises equipment.

CRCError Field This field displays how many CRC errors occurred on the Ethernet controller.

CRM Customer relationship management system.

Data Encryption Standard Over-the-air link option that uses secret 56-bit keys and 8 parity bits. Data Encryption Standard (DES) performs a series of bit permutations, substitutions, and recombination operations on blocks of data.

Date of Last Transaction A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM. Expressed in the database output as DLT.

Dell A trademark of Dell, Inc.

Demilitarized Zone Internet Protocol area outside of a firewall. Defined in RFC 2647. See http://www.faqs.org/rfcs/rfc2647.html.

DES Data Encryption Standard. An over-the-air link option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data.

Desensed Received an undesired signal that was strong enough to make the module insensitive to the desired signal.

DHCP Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the Canopy system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.

Diffraction Partial obstruction of a signal. Typically diffraction attenuates a signal so much that the link is unacceptable. However, in some instances where the obstruction is very close to the receiver, the link may be acceptable.

DiffServ Differentiated Services, consistent with RFC 2474. A byte in the type of service (TOS) field of packets whose values correlates to the channel on which the packet should be sent. The value is a numeric code point. Canopy maps each of 64 code points to values of 0 through 7. Three of these code points have fixed values, and the remaining 61 are settable. Values of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities. Among the settable parameters, the values are set in the AP for all downlinks within the sector and in the SM for each uplink.

Disable

To turn off a feature in the module after both the feature activation file has *activated* the module to use the feature and the operator has *enabled* the feature in the module. See also Activate and Enable.

DLT

Date of last transaction. A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM.

DMZ

Demilitarized Zone as defined in RFC 2647. An Internet Protocol area outside of a firewall. See http://www.faqs.org/rfcs/rfc2647.html.

Dynamic Host Configuration Protocol

Protocol defined in RFC 2131 that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus Dynamic Host Configuration Protocol reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the Canopy system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.

Electronic Serial Number

Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.

Element Pack

A license for Prizm management of a multi-point sector and covers the AP and up to 200 SMs, a backhaul link, or an Powerline LV link.

Enable

To turn on a feature in the module after the feature activation file has *activated* the module to use the feature. See also Activate.

Engine

Bandwidth and Authentication Manager (BAM) interface to the AP and SMs. Unique sets of commands are available on this interface to manage parameters and user access. Distinguished from SSE. See also SSE.

ESN

Electronic Serial Number. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.

ESN Data Table

Table in which each row identifies data about a single SM. In tab-separated fields, each row stores the ESN, authentication key, and QoS information that apply to the SM. The operator can create and modify this table. This table is both an input to and an output from the Bandwidth and Authentication Manager (BAM) SQL database, and should be identically input to redundant BAM servers.

/etc/services

File that stores telnet ports on the Bandwidth and Authentication Manager (BAM) server.

EthBusErr Field

This field displays how many Ethernet bus errors occurred on the Ethernet controller.

Ethernet Protocol Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.

Fade Margin The difference between strength of the received signal and the strength that the receiver requires for maintaining a reliable link. A higher fade margin is characteristic of a more reliable link. Standard operating margin.

FCC Federal Communications Commission of the U.S.A.

Feature Activation Key Software key file whose file name includes the ESN of the target Canopy module. When installed on the module, this file *activates* the module to have the feature *enabled* or disabled in a separate operator action.

Field-programmable Gate Array Array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.

File Transfer Protocol Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. Defined in RFC 959. See http://www.faqs.org/rfcs/rfc959.html.

FPGA Field-programmable Gate Array. An array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.

Frame Spreading Transmission of a beacon in only frames where the receiver expects a beacon (rather than in every frame). This avoids interference from transmissions that are not intended for the receiver.

Frame Timing Pulse Gated Field Toggle parameter that prevents or allows the module to continue to propagate GPS sync timing when the module no longer receives the timing.

Free Space Path Loss Signal attenuation that is naturally caused by atmospheric conditions and by the distance between the antenna and the receiver.

Fresnel Zone Space in which no object should exist that can attenuate, diffract, or reflect a transmitted signal before the signal reaches the target receiver.

FSK Frequency Shift Keying, a variation of frequency modulation to transmit data, in which two or more frequencies are used.

FTP File Transfer Protocol, defined in RFC 959. Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. See http://www.faqs.org/rfcs/rfc959.html.

Global Positioning System Network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.

GPS Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.

GPS/3 Third-from-left LED in the module. In the operating mode for an Access Point Module or Backhaul timing master, this LED is continuously lit as the module receives sync pulse. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.

GUI Graphical user interface.

High-priority Channel Channel that supports low-latency traffic (such as Voice over IP) over low-latency traffic (such as standard web traffic and file downloads). To recognize the latency tolerance of traffic, this channel reads the IPv4 Type of Service Low Latency bit.

HTTP Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web. Defined in RFC 2068. See http://www.faqs.org/rfcs/rfc2068.html.

ICMP Internet Control Message Protocols defined in RFC 792, used to identify Internet Protocol (IP)-level problems and to allow IP links to be tested. See http://www.faqs.org/rfcs/rfc792.html.

indiscards count Field How many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)

inerrors count Field How many inbound packets contained errors that prevented their delivery to a higher-layer protocol.

innucastpkts count Field How many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.

inoctets count Field How many octets were received on the interface, including those that deliver framing information.

Intel A registered trademark of Intel Corporation.

inucastpkts count Field How many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.

inunknownprotos count Field How many inbound packets were discarded because of an unknown or unsupported protocol.

IP
Internet Protocol defined in RFC 791. The Network Layer in the TCP/IP protocol stack. This protocol is applied to addressing, routing, and delivering, and re-assembling data packets into the Data Link layer of the protocol stack. See http://www.faqs.org/rfcs/rfc791.html.

IP Address
32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.

IPv4
Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.

ISM
Industrial, Scientific, and Medical Equipment radio frequency band, in the 900-MHz, 2.4-GHz, and 5.8-GHz ranges.

Jitter
Timing-based measure of the reception quality of a link. An acceptable link displays a jitter value between 0 and 4 for a 10-Mbps Backhaul timing slave in Release 4.0 and later, between 0 and 9 for a 20-Mbps Backhaul timing slave, or between 5 and 9 for any Subscriber Module or for a Backhaul timing slave in any earlier release.

L2TP over IPSec
Level 2 Tunneling Protocol over IP Security. One of several virtual private network (VPN) implementation schemes. Regardless of whether Subscriber Modules have the Network Address Translation feature (NAT) enabled, they support VPNs that are based on this protocol.

Late Collision Field
This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision. A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.

Latency Tolerance
Acceptable tolerance for delay in the transfer of data to and from a module.

Line of Sight
Wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.

Linux
A registered trademark of Linus Torvalds.

LNK/5
Furthest left LED in the module. In the operating mode, this LED is continuously lit when the Ethernet link is present. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.

Logical Unit ID
Final octet of the 4-octet IP address of the module.

LOS
Line of sight. The wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.

LUID Logical Unit ID. The final octet of the 4-octet IP address of the module.

MAC Address Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.

Management Information Base Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).

Master Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul module that provides synchronization over the air to another Backhaul module (a Backhaul timing slave) and applies to a Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically copied onto a redundant BAM server (BAM slave). In each case, the master is not a product. Rather, the master is the role that results from deliberate configuration steps.

Maximum Information Rate The cap applied to the bandwidth of an SM or specified group of SMs. In the Canopy implementation this is controlled by the Sustained Uplink Data Rate, Uplink Burst Allocation, Sustained Downlink Data Rate, and Downlink Burst Allocation parameters.

Media Access Control Address Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.

MIB Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).

MIR See Maximum Information Rate.

MySQL A registered trademark of MySQL AB Company in the United States, the European Union, and other countries.

mysqladmin A command to set the administrator and associated password on the Bandwidth and Authentication Manager (BAM) server.

mysql-server Package group that enables the SQL Database Server application in the Red Hat® Linux® 9 operating system to provide SQL data for Bandwidth and Authentication Manager (BAM) operations.

NAT Network Address Translation defined in RFC 1631. A scheme that isolates Subscriber Modules from the Internet. See http://www.faqs.org/rfcs/rfc1631.html.

NBI See Northbound Interface.

NEC
National Electrical Code. The set of national wiring standards that are enforced in the U.S.A.

NetBIOS
Protocol defined in RFC 1001 and RFC 1002 to support an applications programming interface in TCP/IP. This interface allows a computer to transmit and receive data with another host computer on the network. RFC 1001 defines the concepts and methods. RFC 1002 defines the detailed specifications. See http://www.faqs.org/rfcs/rfc1001.html and http://www.faqs.org/rfcs/rfc1002.html.

Network Address Translation
Scheme that defines the Access Point Module as a proxy server to isolate registered Subscriber Modules from the Internet. Defined in RFC 1631. See http://www.faqs.org/rfcs/rfc1631.html.

Network Management Station
Monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects).

NMS
Network Management Station. A monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects).

Northbound Interface
The interface within Prizm to higher-level systems. This interface consists of a Simple Network Management Protocol (SNMP) agent for integration with a network management system (NMS); a Simple Object Access Protocol (SOAP) XML-based application programming interface (API) for web services that supports integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system; and console automation that allows such higher-level systems to launch and appropriately display the PrizmEMS management console in a custom-developed GUI.

Object
Network variable that is defined in the Management Information Base.

OptiPlex
A trademark of Dell, Inc.

OSS
Operations support system, such as a customer relationship management (CRM), billing, or provisioning system. The application programming interface (API) for Prizm supports integrating Prizm with an OSS.

outdiscards count Field
How many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)

outerrors count Field
How many outbound packets contained errors that prevented their transmission.

outnucastpkts count Field
How many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.

outoctets count Field How many octets were transmitted out of the interface, including those that deliver framing information.

outucastpkts count Field How many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.

Override Plug Device that enables the operator to regain control of a module that has been locked by the No Remote Access feature, the 802.3 Link Disable feature, or a password or IP address that cannot be recalled. This device can be either fabricated on site or ordered.

Pentium A registered trademark of Intel Corporation.

php-mysql Package group that enables the Web Server application in the Red Hat® Linux® 9 operating system to provide data from the SQL Database Server application as PHP in the Bandwidth and Authentication Manager (BAM) GUI.

Point-to-Point Protocol Standards that RFC 1661 defines for data transmittal on the Internet. Also known as PPP or PTP. See http://www.faqs.org/rfcs/rfc1661.html.

Power Control Feature in Release 4.1 and later that allows the module to operate at less than 18 dB less than full power to reduce self-interference.

PPTP Point to Point Tunneling Protocol. One of several virtual private network implementations. With the Network Address Translation (NAT) feature enabled, Subscriber Modules *do not* support VPNs that are based on this protocol. With NAT disabled, they do support VPNs that are based on this protocol.

Prizm The Canopy software product that allows users to partition their entire Canopy networks into criteria-based subsets and independently monitor and manage those subsets. Prizm Release 1.0 and later includes a Northbound Interface to higher-level systems. Prizm Release 2.0 and later integrates Canopy Bandwidth and Authentication Manager (BAM) functionality and supports simple migration of a pre-existing authentication, bandwidth, and VLAN settings into the Prizm database.

Protective Earth Connection to earth (which has a charge of 0 volts). Also known as ground.

Proxy Server Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer, which has an IP address that is not unique or not registered.

PTMP Point-to-Multipoint Protocol defined in RFC 2178, which specifies that data that originates from a central network element can be received by all other network elements, but data that originates from a non-central network element can be received by only the central network element. See http://www.faqs.org/rfcs/rfc2178.html.

PTP

Point-to-Point Protocol. The standards that RFC 1661 defines for data transmittal on the Internet. See http://www.faqs.org/rfcs/rfc1661.html.

QoS

Quality of Service. A frame field that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields.

Quality of Service

A frame bit that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields. Also known as QoS.

Quick Start

Interface page that requires minimal configuration for initial module operation.

Radio Signal Strength Indicator

Relative measure of the strength of a received signal. An acceptable link displays an Radio Signal Strength Indicator (RSSI) value of greater than 700.

Random Number

Number that the Bandwidth and Authentication Manager (BAM) generates, invisible to both the SM and the network operator, to send to the SM as a challenge against an authentication attempt.

Reader

A registered trademark of Adobe Systems, Incorporated.

Recharging

Resumed accumulation of data in available data space (buckets). See Buckets.

Red Hat

A registered trademark of Red Hat, Inc.

Reflection

Change of direction and reduction of amplitude of a signal that encounters an object larger than the wavelength. Reflection may cause an additional copy of the wavelength to arrive at after the original, unobstructed wavelength arrives. This causes partial cancellation of the signal and may render the link unacceptable. However, in some instances where the direct signal cannot be received, the reflected copy may be received and render an otherwise unacceptable link acceptable.

Registrations MIB

Management Information Base file that defines registrations for global items such as product identities and product components. See also Management Information Base.

repl-m

A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) master server, uses SFTP to copy both the database and the `repl-s` script to a BAM slave server, and remotely executes the `repl-s` script on the BAM slave server. See Master, Slave, `repl-s`, Secure Shell, and SFTP.

repl-s A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) slave server. See Master, Slave, and `repl-m`.

RES Result. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server.

RetransLimitExp Field This field displays how many times the retransmit limit has expired.

RF Radio frequency. How many times each second a cycle in the antenna occurs, from positive to negative and back to positive amplitude.

RJ-11 Standard cable that is typically used for telephone line or modem connection.

RJ-45 Standard cable that is typically used for Ethernet connection. This cable may be wired as straight-through or as crossover. Later Canopy modules auto-sense whether the cable is straight-through or crossover.

Router Network element that uses the logical (IP) address of another to pass data to only the intended recipient. Compare to Switch and Bridge.

RPM Red Hat® Package Manager.

rpm A command that the Linux® operating system accepts to identify the version of Linux® software that operates on the Bandwidth and Authentication Manager (BAM) server.

RSSI Radio Signal Strength Indicator. A relative measure of the strength of a received signal. An acceptable link displays an RSSI value of greater than 700.

RxBabErr Field This field displays how many receiver babble errors occurred.

RxOverrun Field This field displays how many receiver overrun errors occurred on the Ethernet controller.

SDK *PrizmEMS™ Software Development Kit (SDK)*—the document that provides server administrator tasks, GUI developer information for console automation that allows higher-level systems to launch and appropriately display the Prizm management console. The SDK also describes the how to define new element types and customize the Details views.

Secure Shell A trademark of SSH Communications Security.

Self-interference Interference with a module from another module in the same network.

SES/2

Third-from-right LED in the module. In the Access Point Module and Backhaul timing master, this LED is unused. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.

Session Key

Software key that the SM and Bandwidth and Authentication Manager (BAM) separately calculate based on that both the authentication key (or the factory-set default key) and the random number. BAM sends the session key to the AP. Neither the subscriber nor the network operator can view this key. See also Random Number.

SFTP

Secure File Transfer Protocol.

Simple Network Management Protocol

Standard that is used for communications between a program (agent) in the network and a network management station (monitor). Defined in RFC 1157. See http://www.faqs.org/rfcs/rfc1157.html.

skey

Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f. This key must be unique to the individual SM. Also known as authentication key.

Slave

Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul slave that receives synchronization over the air from another Backhaul module (a Backhaul timing master) and applies to a redundant Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically overwritten by a copy from the primary BAM server (BAM master). In each case, the slave is not a product. Rather, the slave is the role that results from deliberate configuration steps.

SM

Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.

SM MIB

Management Information Base file that defines objects that are specific to the Subscriber Module or Backhaul timing slave. See also Management Information Base.

SNMP

Simple Network Management Protocol, defined in RFC 1157. A standard that is used for communications between a program (agent) in the network and a network management station (monitor). See http://www.faqs.org/rfcs/rfc1157.html.

SNMP Trap

Capture of information that informs the network monitor through Simple Network Management Protocol of a monitored occurrence in the module.

SOAP Simple Object Access Protocol (SOAP). The protocol that the Northbound Interface in Prizm uses to support integration of Prizm with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system

SSE Bandwidth and Authentication Manager (BAM) interface to the SQL server. Unique sets of commands are available on this interface to manage the BAM SQL database and user access. Distinguished from Engine. See also Engine.

Standard Operating Margin See Fade Margin.

Static IP Address Assignment Assignment of Internet Protocol address that can be changed only manually. Thus static IP address assignment requires more configuration time and consumes more of the available IP addresses than DHCP address assignment does. RFC 2050 provides guidelines for the static allocation of IP addresses. See http://www.faqs.org/rfcs/rfc2050.html. See also DHCP.

su - A command that opens a Linux® operating system session for the user `root`.

Subnet Mask 32-bit binary number that filters an IP address to reveal what part identifies the network and what part identifies the host. The number of subnet mask bits that are set to 1 indicates how many leading bits of the IP address identify the network. The number of subnet mask bits that are set 0 indicate how many trailing bits of the IP address identify the host.

Subscriber Module Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.

Sustained Data Rate Preset rate limit of data transfer.

Switch Network element that uses the port that is associated with the physical address of another to pass data to only the intended recipient. Compare to Bridge and Router.

SYN/1 Second-from-right LED in the module. In the Access Point Module or Backhaul timing master, as in a registered Subscriber Module or Backhaul timing slave, this LED is continuously lit to indicate the presence of sync. In the operating mode for a Subscriber Module or Backhaul timing slave, this LED flashes on and to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.

Sync GPS (Global Positioning System) absolute time, which is passed from one module to another. Sync enables timing that prevents modules from transmitting or receiving interference. Sync also provides correlative time stamps for troubleshooting efforts.

TCP

Alternatively known as Transmission Control Protocol or Transport Control Protocol. The Transport Layer in the TCP/IP protocol stack. This protocol is applied to assure that data packets arrive at the target network element and to control the flow of data through the Internet. Defined in RFC 793. See http://www.faqs.org/rfcs/rfc793.html.

tcp

Transport Control type of port. The Canopy system uses Port 3306:tcp for MySQL® database communications, Port 9080:tcp for SSE `telnet` communications, and Port 9090:tcp for Engine `telnet` communications.

TDD

Time Division Duplexing.

TDMA

Time Division Multiple Access.

telnet

Utility that allows a client computer to update a server. A firewall can prevent the use of the `telnet` utility to breach the security of the server. See http://www.faqs.org/rfcs/rfc818.html, http://www.faqs.org/rfcs/rfc854.html and http://www.faqs.org/rfcs/rfc855.html.

Textual Conventions MIB

Management Information Base file that defines Canopy system-specific textual conventions. See also Management Information Base.

Time of Last Transaction

A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM. Expressed in the database output as TLT.

TLT

Time of last transaction. A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM.

TNAF

Total number of authentication requests failed. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate but was denied by BAM.

TNAR

Total number of authentication requests. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate, regardless of whether the attempt succeeded.

Tokens

Theoretical amounts of data. See also Buckets.

TOS

8-bit field in that prioritizes data in a IP transmission. See http://www.faqs.org/rfcs/rfc1349.html.

TxUnderrun Field This field displays how many transmission-underrun errors occurred on the Ethernet controller.

UDP User Datagram Protocol. A set of Network, Transport, and Session Layer protocols that RFC 768 defines. These protocols include checksum and address information but does not retransmit data or process any errors. See http://www.faqs.org/rfcs/rfc768.html.

udp User-defined type of port.

U-NII Unlicensed National Information Infrastructure radio frequency band, in the 5.1-GHz through 5.8-GHz ranges.

VID VLAN identifier. See VLAN.

VLAN Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.

VPN Virtual private network for communication over a public network. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes is possible. With the Network Address Translation feature (NAT) enabled, SMs on Canopy System Release 4.2 or later support L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs, but *do not* support PPTP (Point to Point Tunneling Protocol) VPNs. With NAT disabled, SMs support all types of VPNs.