Software Release 11.0

Release Notes and User Guide Supplement

PMP 100 and PTP 100 (FSK)
PMP 400 and PTP 200 (OFDM)

March 2011

Issue 1

Notices

See important regulatory and legal notices in Section 11 on Page 43.

Trademarks, Product Names, and Service Names

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

http://motorola.wirelessbroadbandsupport.com

Table of Contents

List of Tables

List of Figures

1   Introduction

1.1   RELEASE 11.0 OVERVIEW

Release 11.0 is a general release for all Canopy FSK and OFDM radios, including PMP 100, PMP 400/430, PTP 100, and PTP 200 Series modules.

The primary Release 11.0 feature is SM and AP support for the RADIUS (Remote Authentication Dial In User Service) protocol so that RADIUS can be used for

- o   SM Authentication
- o   SM Configuration
- o   Centralized AP and SM user name and password management

For information on other Release 11.0 features see section 4 on page 11.

For information on the RADIUS implementation see section 5 on page 13.

For improvements and issues resolved in Release 11.0 see section 6 on page 25.

For release open issues see section 7 on page 26.

Release 11.0 adds no additional features to BHMs or BHSs, but BHMs and BHSs may be upgraded to Release 11.0 if desired.

> **IMPORTANT!**
> Floating licenses **are not** supported when using RADIUS. If you are using floating licenses, you can upgrade to Release 11.0, but do not use RADIUS authentication mode.

Floating licenses are used in conjunction with Prizm or BAM to provide features to SMs. If you are using floating licenses currently and wish to convert them to fixed licenses so you can use RADIUS, please contact technical support.

Modules should be running Release 9.5 or Release 10.5 before upgrading to Release 11.0.

To upgrade modules and distribute certificates to SMs use CNUT 3.20.16.

To manage modules running Release 11.0, including managing features new to this release, use Wireless Manager 3.0. (Prizm does not support the new features.)

1.2   DOCUMENT CHANGE HISTORY

Issue 1   First Issue

1.3   ABBREVIATIONS

The following abbreviations and acronyms are used in these notes and related documentation:

AAA	Authentication, Authorization, and Accounting	**BH**	Backhaul Module
AES	Advanced Encryption Standard	**BHM**	Backhaul Module – Master
AP	Access Point	**BHS**	Backhaul Module – Slave
BAM	Bandwidth and Authentication Manager	**CA**	Certificate Authority
		CAP	Access Point Module

CEPT	Conference of European Post and Telecommunications	**MSCHAP**	Microsoft CHAP
CHAP	Challenge Handshake Authentication Protocol	**MSK**	Master Session Key
		MVID	Management VID
CIR	Committed Information Rate	**NAI**	Network Access Identier
CMM	Cluster Management Module	**NAS**	Network Access Server (the AP, in this system)
CNUT	Canopy Network Updater Tool		
CSM	Subscriber Module	**NAT**	Network Address Translation
CRL	Certificate Revocation List	**OFDM**	Orthogonal Frequency Division Multiplexing
DES	Data Encryption Standard		
DFS	Dynamic Frequency Selection	**OID**	SNMP Object Identifier
DHCP	Dynamic Host Configuration Protocol	**P7/P8/P9/P10/P11** Hardware Series	
DNS	Domain Name System	**PAP**	Password Authentication Protocol
EAP	Extensible Authentication Protocol	**PKI**	Public Key Infrastructure
EIRP	Equivalent Isotropically Radiated Power	**PMP**	Point to Multi-Point
		PTP	Point to Point
EFTA	European Free Trade Association	**PVID**	Port VID
EMSK	Extended Master Session Key	**RADIUS**	Remote Authentication Dial In User Service
ETSI	European Telecommunications Standards Institute		
		RF	Radio Frequency
EU	European Union	**RLAN**	Radio Local Area Network
FCC	US Federal Communications Commission	**SM**	Subscriber Module
		SNMP	Simple Network Management Protocol
FSK	Frequency Shift Keying	**SNR**	Signal to Noise Ratio
FTP	File Transfer Protocol	**TCP/IP**	Transmission Control Protocol/Internet Protocol
GPS	Global Positioning System		
HPAP	High Performance AP (PMP 430 AP)	**TLS**	Transport Layer Security
IC	Industry Canada	**TTLS**	Tunneled TLS
IETF	Internet Engineering Task Force	**VDC**	Volts Direct Current
IP	Internet Protocol	**VID**	VLAN ID
ISM	Industrial, Scientific, Medical	**VLAN**	Virtual LAN
LAN	Local Access Network	**VSA**	Vendor Specific Attribute
MAC	Media Access Controller	**WAN**	Wide Area Network
MIB	Management Information Base	**WM**	One Point Wireless Manager
MIR	Maximum Information Rate		

1.4   FEEDBACK ON DOCUMENTATION

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

1.5   TECHNICAL SUPPORT

Tip!   Do not clear the Event Log after you encounter issues. It may be useful to Technical Support, if you need to escalate the issue.

Here is the escalation path for resolution of a problem:

1. Check documentation:
   - These Release Notes
   - Motorola PMP Solutions Users Guide, available at http://motorola.wirelessbroadbandsupport.com/software.
2. Consider checking the Community Forum and Knowledge Base at http://motorola.wirelessbroadbandsupport.com/support/community.

3. Consider checking the Support Home Page at http://motorola.wirelessbroadbandsupport.com/support/technical.php

4. Escalate the problem to your supplier or reseller.

5. Escalate the problem to Technical Support or other designated Tier 3 technical support:

Email: EMS-EICC-RM@motorolasolutions.com

Phone:

U.S. and Canada   1-866-961-9288

Europe, Middle East, and Africa
Denmark	043682114
France	0157323434
Germany	06950070204
Italy	0291483230
Lithuania	880 030 828
Netherlands	0202061404
Norway	24159815
Portugal	0217616160
Spain	0912754787
Russia	810 800 228 41044
Saudi Arabia	800 844 5345
South Africa	0800981900
United Kingdom	0203 0277499
All other countries	+420 533 336 946

Latin and Central America
Argentina	0800-666-2789
Brazil	0800-891-4360
Columbia	01-800-912-0557
Mexico	001-800-942-7721
Peru	0800-70-086

All other countries   +420 533 336 946

Asia and Pacific
Australia	1 800 457 439
Northern China	10 800 713 0885
Southern China	10 800 130 0867
China, local DID	+86 21 6108 6109
Hong Kong	30 027 861
India	000 800 100 3098
Japan	221626765
Japan, PSTN	(81) 335 708 643
South Korea	080 681 0880
Malaysia	1 800 812 384
New Zealand	0 800 448 472
Philippines	63 29 003 057
Singapore	64 155 110
Taiwan	00 801 14 8690
Thailand	001 800 441 0950
Indonesia	001 803 015 20 20530
All other countries	+420 533 336 946

When you send e-mail or call, please include, as appropriate, software release on each module, IP addresses, MAC addresses, and features enabled, like NAT, VLAN, high priority channel, or CIR. You may be asked to run the Support Tool on CNUT or Prizm to provide a complete network picture.

2   Applicability

Release 11.0 is a general release recommended for all the products shown in Figure 1.

Modulation and Module Type	PMP Radio Series (Point-to-MultiPoint)	PTP Radio Series (Point-To-Point)
FSK AP/SM/BH	**PMP 100 Series** Frequencies: 900MHz, 2.4, 5.1, 5.2, 5.4, 5.7, 5.9, 6.050-GHz **Note**: P7 and P8 APs cannot be upgraded **Note**: AES P7 and P8 SMs cannot be upgraded (All DES SMs can be)	**PTP 100 Series** Frequencies: 2.4, 5.2, 5.4, 5.7-GHz **Note**: P7 and P8 BHs cannot be upgraded
OFDM AP/SM	**PMP 430 Series** Frequencies: 5.4-GHz PMP 54430 5.8-GHz PMP 58430	N/A N/A
OFDM AP/SM/BH	**PMP 400 Series** Frequencies: 4.9-GHz PMP 49400 5.4-GHz PMP 54400	**PTP 200 Series** Frequencies: 4.9-GHz PTP 49200 5.4-GHz PTP 54200

Figure 1: Applicable products

Not all products are available in all markets. Please check with your local reseller for availability.

3   Upgrading to Release 11.0

Upgrade first to R11.0 then enable RADIUS settings if desired (or not). In most cases operators will want to upgrade to R11.0, then trial a friendly sector with RADIUS, then deploy RADIUS to their entire network.

R11.0 does not require using RADIUS. If upgrading a network from an old release, upgrading to R11.0 is recommended, even if not using RADIUS, so as to take advantage of features and fixes through R11.0.

Use version 3.20.16 of the Network Updater Tool (CNUT) to upgrade to Release 11.0. Version 3.20.16 supports distribution of certificates to SMs.

CNUT and its release notes can be downloaded from the Motorola wireless broadband support web site: http://motorola.wirelessbroadbandsupport.com/software/

Modules in operating sectors should be on Release 9.5 or 10.5 before upgrading to avoid upgrade issues.

3.1   OBTAINING CNUT UPGRADE PACKAGES

To download the Canopy software to your computer, perform the following steps:

1. Go to http://motorola.wirelessbroadbandsupport.com/software.
2. Follow the directions on that page to access the software download page.
3. On the software download page, select the appropriate package or packages. Options include
    - CANOPY11BUILDOFFICIAL_DES.pkg3
    - CANOPY11BUILDOFFICIAL_AES.pkg3
    - CANOPY11BUILDOFFICIAL_OFDM_DES.pkg3
    - CANOPY11BUILDOFFICIAL_OFDM_AES.pkg3
4. Click **Accept User Agreement and Request Download Links**.
    RESULT: You will receive an email with a link or links to the software.
5. In the email sent to you, click on the desired link or links.
    RESULT: The appropriate `.pkg3` package or packages will download to your computer.

For additional information on using CNUT, see the CNUT help file or click on the Help menu in the CNUT application.

3.2   NETWORK MANAGEMENT

Use One Point Wireless Manager to manage Motorola PMP and PTP networks, including managing the RADIUS features. For additional information, see http://motorola.wirelessbroadbandsupport.com/support/opws/software/

3.3   PMP 430 – OPTIONS FOR 5, 10, AND 20 MHZ CHANNEL SIZE
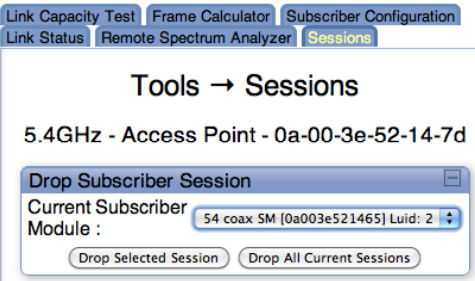
PMP 430 APs and SMs ship with software with a 10-MHz channel size. This can be changed to 5 or 20 MHz using CNUT. For an operating sector, use CNUT to change the channel size of the SMs first, then the AP. For SMs being deployed into an operating sector, use CNUT to set the channel size before deploying the SMs.

To set the channel size, use the Update > Configure > HPAP Channel Bandwidth menu on CNUT. See the latest CNUT release notes for additional information.

4 Features

Release 11.0 adds the features listed in Table 1.

Table 1: Release 11.0 Features

Regions Affected	Products Affected	Feature	Description	See for Details
All Regions	AP and SM	Support for the RADIUS protocol.	RADIUS can be used for SM authentication, SM configuration, and centralized AP and SM user name and password management.	Section 5
All Regions	AP and SM	From AP GUI or SNMP, drop all sessions in the sector.	From the AP's Tools > Sessions tab, sessions to all SMs in the sector can be dropped. This forces all SMs in the sector to register again to an AP. Note that a session to a single selected SM can also be dropped.	-
All Regions	SM with NAT enabled	Data entry checking	Data entry checking now prevents mistakenly setting the same IP address for both the LAN Interface and the Remote Configuration Interface on an SM with NAT enabled. These parameters are configured on the SM's Configuration > NAT tab.	-
All Regions	PMP 100	Can configure 40 mile max range on FSK AP.	On the AP's Configuration > Radio tab, the **Max Range** can now be configured up to 40 miles (instead of the previous max of 30 miles). Note, this does not change the transmit power of the radio, does not change the RF operation, and due to the additional turnaround time in the frame will reduce capacity and throughput to some degree.	-
All Regions	PMP 100	Can configure SM receive target level up to -40 dBm on FSK AP.	On the AP's Configuration > Radio tab, the **SM Receive Target Level** can now be configured up to -40 dBm (instead of the previous limit of -55 dBm). Note, this does not change the transmitter power of the AP, nor the sensitivity of the AP or the SM – it just allows a "hotter" SM receive target level if RF design requires it.	-

Regions Affected	Products Affected	Feature	Description	See for Details
All Regions	AP and SM	Display AP's site name on SM	On the SM's Home > General Status tab, the **Registered AP** field now displays the SNMP Site Name of the AP as well as the AP's MAC address. (SNMP Site Names are configured on a radio's Configuration > SNMP tab in the **Site Name** field.)	-

5   RADIUS for PMP

Release 11.0 adds support for the RADIUS (Remote Authentication Dial In User Service) protocol supporting Authentication, Authorization, and Accounting (AAA). The following topics are covered in this document:

- o   An overview of the Canopy RADIUS implementation
- o   Description of the operation of RADIUS with Canopy and the various configurable parameters and their settings
- o   Procedures for specific tasks associated with configuring Canopy for RADIUS
- o   Reference material, especially information on VSAs and OIDs.

The information **does not**

- o   Provide substantial background on the RADIUS protocol. A solid understanding of RADIUS is assumed, or should be gained from other sources.
- o   Provide detailed information on setting up a RADIUS server. This information should be gained from other sources, including the vendor or provider of the RADIUS server.

A typical course of action to prepare for the migration to RADIUS is

- o   Study these release notes
- o   Gain any additional knowledge needed on RADIUS and your specific RADIUS server from outside sources and install your RADIUS server and database.
- o   Experiment with a test system in the lab or field
- o   Develop a migration plan for your network
- o   Migrate your network to RADIUS

5.1   RADIUS IMPLEMENTATION OVERVIEW

5.1.1   RADIUS Functions

RADIUS protocol support provides the following functions:

- o   **SM Authentication** allows only known SMs onto the network (blocking "rogue" SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to "rogue" APs). RADIUS authentication is used for SMs, but not used for APs, BHMs, or BHSs.
- o   **SM Configuration** configures authenticated SMs with MIR (Maximum Information Rate), CIR (Committed Information Rate), High Priority, and VLAN (Virtual LAN) parameters from the RADIUS server when an SM registers to an AP.
- o   **Centralized AP and SM user name and password management** allows AP and SM usernames and access levels (Administrator, Installer, Technician) to be centrally administered in the RADIUS server instead of on each radio and tracks access events (logon/logoff) for each username on the RADIUS server. BHMs and BHSs do not support RADIUS accounting. This accounting does *not* track and report specific configuration actions performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as the Motorola One Point Wireless Manager. This accounting is *not* the ability to perform accounting functions on the subscriber/end user/customer account.

5.1.2   Tested RADIUS Servers

The Canopy RADIUS implementation has been tested and is supported on

- o   FreeRADIUS, Version 2.1.8
- o   Aradial RADIUS, Version 5.1.12

    Note, Aradial 5.3 has a bug that prevents "remote device login", so doesn't support the user name and password management feature.

5.2   CONFIGURING AP AND SM FOR RADIUS SM AUTHENTICATION

Configuring Canopy for RADIUS authentication requires configuring both the AP and the SMs.

5.2.1   AP - Choosing Authentication Mode and Configuring for Authentication Servers

On the AP's Configuration > Security tab as shown in Figure 2: AP's Configuration > Security tab, select the **RADIUS AAA Authentication Mode**. The following describes the other **Authentication Mode** options for reference, and then the **RADIUS AAA** option.

Disabled

Requires no authentication. Any SM (except an SM that itself has been configured to *require* RADIUS authentication by enabling **Lock AAA** as described below) will be allowed to register to the AP.

Authentication Server (BAM)

Authentication Server in this instance refers to BAM. Authentication with BAM will be required for an SM to register to the AP. Only SMs listed by MAC address in the BAM database will be allowed to register to the AP.

When **Authentication Server** is selected, up to 5 **Authentication Server** (BAM) IP addresses can be configured. The IP address(es) configured here must match the IP address(es) of the BAM(s).

AP Pre-Shared Key

Canopy offers a pre-shared key authentication option. In this case, an identical key must be entered in the **Authentication Key** field on the AP's Configuration > Security tab and in the **Authentication Key** field on each desired SM's Configuration > Security tab.

RADIUS AAA

To support RADIUS authentication of SMs, on the AP's Configuration > Security tab select **RADIUS AAA.** Only properly configured SMs with a valid certificate will be allowed to register to the AP.

When **RADIUS AAA** is selected, up to 3 **Authentication Server** (RADIUS Server) IP addresses and **Shared Secrets** can be configured. The IP address(es) configured here must match the IP address(es) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not splitting the database. If Server 1 doesn't respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network, and does not progress trying the other servers.

The default IP address is 0.0.0.0 (which obviously won't match any RADIUS server). The default **Shared Secret** is "CanopySharedSecret". The **Shared Secret** can be up to 32 ASCII characters (no diacritical marks or ligatures, for example).
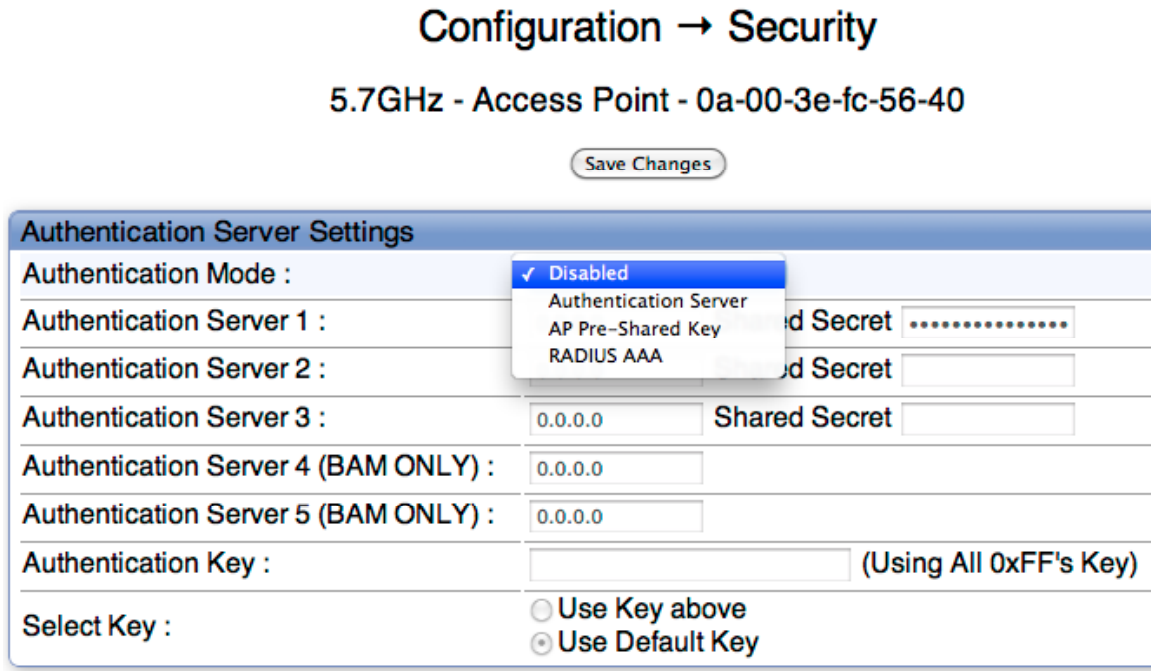
Figure 2: AP's Configuration > Security tab

5.2.2   SM Authentication Mode – Require RADIUS or Follow AP

Refer to Figure 3: SM's Configuration > Security tab to see the GUI options.

If it is desired that an SM will only authenticate to an AP that is using RADIUS, on the SM's Configuration Security tab set **Lock AAA** to **Enabled**. With **Lock AAA** enabled, an SM will not register to an AP that has any **Authentication Mode** other than **RADIUS AAA** selected.

If it is desired that an SM use the authentication method configured on the AP it is registering to, set **Lock AAA** to **Disabled.** With **Lock AAA** disabled, an SM will attempt to register using whichever **Authentication Mode** is configured on the AP it is attempting to register to.

Note, requiring SMs to use RADIUS by enabling **Lock AAA** avoids the security issue of SMs possibly registering to "rogue" APs which have authentication disabled.

Configuration → Security

5.7GHz - Subscriber Module - 0a-00-3e-fe-ed-df

(Save Changes)

Authentication Key Settings   ⊟

Authentication Key :   [   ] (Using All 0xFF's Key)

Select Key :   ○ Use Key above
                              ● Use Default Key

AAA Authentication Settings   ⊟

Lock AAA :   ○ Enabled
                              ● Disabled

Phase 1 :   [EAPTTLS ▼]

Phase 2 :   [MSCHAPv2 ▼]

Identity/Realm :   ○ Enable Realm
                              ● Disable Realm
                              Identity [anonymous]   @ Realm [canopy.net]

Username :   [0a-00-3e-fe-ed-df]   (Use Default Username)

Password :   [••••••••]

Confirm Password :   [   ]

Figure 3: SM's Configuration > Security tab

5.2.3   SM - Phase 1 (Outside Identity) parameters and settings

Refer to Figure 3: SM's Configuration > Security tab to see the GUI options.

The only protocol supported for the **Phase 1** (Outside Identity) phase of authentication is EAPTTLS (Extensible Authentication Protocol Tunneled Transport Layer Security).

Configure an outer Identity in the **Username** field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity **Username** is "anonymous". The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.

If Realms are being used, select **Enable Realm** and configure an outer identity in the **Identity** field and a Realm in the **Realm** field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default **Identity** is "anonymous". The **Identity** can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default **Realm** is "canopy.net". The **Realm** can also be up to 128 non-special alphanumeric characters.

5.2.4   SM - Phase 2 (Inside Identity) parameters and settings

Refer to Figure 3: SM's Configuration > Security tab to see the GUI options.

Select the desired **Phase 2** (Inside Identity) authentication protocol from the **Phase 2** options of **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol), and **MSCHAP (**Microsoft's version of CHAP, version 2 is used). The protocol must be consistent with the authentication protocol configured on the RADIUS server.

Enter a **Username** for the SM. This must match the username configured for the SM on the RADIUS server. The default **Username** is the SM's MAC address. The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.

Enter the desired password for the SM in the **Password** and **Confirm Password** fields.**.** The **Password** must match the password configured for the SM on the RADIUS server. The default **Password** is "password". The **Password** can be up to 128 non-special (no diacritical markings) alphanumeric characters.

5.3   HANDLING CERTIFICATES

5.3.1   Certificate management on SMs.

The default public Canopy and PMP 320 certificates are loaded into SMs automatically during the upgrade to Release 11.0. The default certificates are not secure and are intended for use during lab and field trials as part of gaining experience with the RADIUS functionality, or as an option during debug. For secure operation, an operator will want to create or procure their own certificates.

Refer to Figure 4: Certificate Management on SM's Configuration > Security tab to see the GUI options.

Up to 2 certificates can be resident on an SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate's description block on the Configuration > Security tab. To restore fhe 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate Settings** parameter block and reboot the radio.

To upload a certificate manually to an SM, first load it in a known place on your PC or network drive, then click on a **Delete** button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on **Choose File,** browse to the location of the certificate, and click the **Import Certificate** button, and then reboot the radio to use the new certificate.

When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used.

The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system.
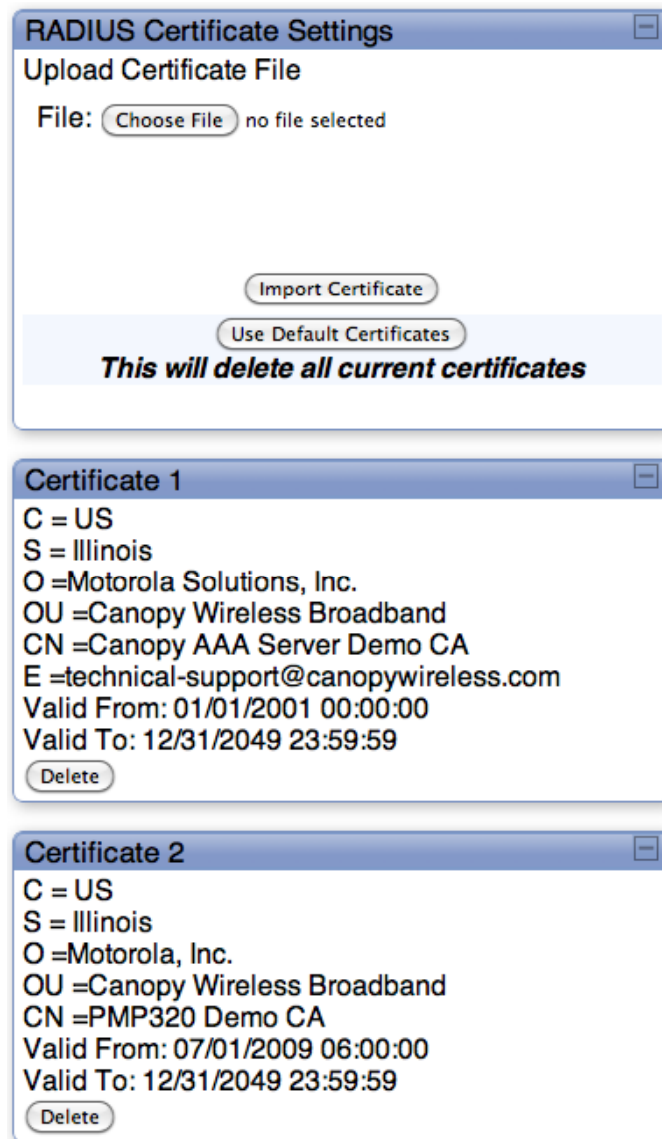
Figure 4: Certificate Management on SM's Configuration > Security tab

5.3.2   Using CNUT to distribute certificates to SMs

CNUT Release 3.20.16 supports distribution of certificates to SMs. Please see the CNUT documentation for additional information.

5.4   CONFIGURING YOUR RADIUS SERVER FOR SM AUTHENTICATION

Your RADIUS server will need to be configured to use the following:

- o   EAPTTLS as the Phase 1/Outer Identity protocol.
- o   If **Enable Realm** is selected on the SM's Configuration > Security tab, then the same **Realm** as appears there (or access to it).
- o   The same Phase 2 (Inner Identity) protocol as configured on the SM's Configuration > Security tab under **Phase 2** options.

- o The username and password for each SM configured on each SM's Configuration > Security tab.
- o An IP address and NAS shared secret that is the same as the IP address and **Shared Secret** configured on the AP's Configuration > Security tab for that RADIUS server.
- o A server private certificate, server key, and CA certificate that complement the public certificates distributed to the SMs, as well as the Canopy dictionary file that defines Vendor Specific Attributes (VSAa). Default certificate files and the dictionary file are available from the software site: http://motorola.wirelessbroadbandsupport.com/software/ after entering your name, email address, and either Customer Contract Number or the MAC address of a module covered under the 12 month warranty.

5.5 CONFIGURING YOUR RADIUS SERVER FOR SM CONFIGURATION

Table 2 lists Canopy Vendor Specific Attributes (VSAs) along with VSA numbers and other details. The associated SM GUI page, tab, and parameter is listed to aid cross-referencing and understanding of the VSAs.

A RADIUS dictionary file is available from the software site: http://motorola.wirelessbroadbandsupport.com/software/. The RADIUS dictionary file defines the VSAs and their values and is usually imported into the RADIUS server as part of server and database setup.

Table 2: Canopy RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Req'd	Value	
SM GUI Page > Tab > Parameter				Default	Size
MS-MPPE-Send-Key	26.311.16	-	Y	-	
-				-	-
MS-MPPE-Recv-Key	26.311.17	-	Y	-	
-				-	-
Motorola-Canopy-LPULCIR	26.161.1	integer	N	0-20000 kbps	
Configuration > Quality of Service > Low Priority Uplink CIR				0 kbps	32 bits
Motorola-Canopy-LPDLCIR	26.161.2	integer	N	0-20000 kbps	
Configuration > Quality of Service > Low Priority Downlink CIR				0 kbps	32 bits
Motorola-Canopy-HPULCIR	26.161.3	integer	N	0-20000 kbps	
Configuration > Quality of Service > Hi Priority Uplink CIR				0 kbps	32 bits
Motorola-Canopy-HPDLCIR	26.161.4	integer	N	0-20000 kbps	
Configuration > Quality of Service > Hi Priority Uplink CIR				0 kbps	32 bits
Motorola-Canopy-HPENABLE	26.161.5	integer	N	0-disable, 1-enable	
Configuration > Quality of Service > Hi Priority Channel Enable/Disable				0	32 bits
Motorola-Canopy-ULBR	26.161.6	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Sustained Uplink Data Rate				dependent on radio feature set	32 bits

Name	Number	Type	Req'd	Value	
SM GUI Page > Tab > Parameter				**Default**	**Size**
Motorola-Canopy-ULBL	26.161.7	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Uplink Burst Allocation				dependent on radio feature set	32 bits
Motorola-Canopy-DLBR	26.161.8	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Sustained Downlink Data Rate				dependent on radio feature set	32 bits
Motorola-Canopy-DLBL	26.161.9	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Downlink Burst Allocation				dependent on radio feature set	32 bits
Motorola-Canopy-VLLEARNNEN	26.161.14	integer	N	0-disable, 1-enable	
Configuration > VLAN > Dynamic Learning				1	32 bits
Motorola-Canopy-VLFRAMES	26.161.15	integer	N	0-all, 1-tagged, 2-untagged	
Configuration > VLAN > Allow Frame Types				0	32 bits
Motorola-Canopy-VLIDSET	26.161.16	integer	N	VLAN Membership (1-4094)	
Configuration > VLAN Membership				0	32 bits
Motorola-Canopy-VLAGETO	26.161.20	integer	N	5 - 1440 minutes	
Configuration > VLAN > VLAN Aging Timeout				25 mins	32 bits
Motorola-Canopy-VLIGVID	26.161.21	integer	N	1 – 4094	
Configuration > VLAN > Default Port VID				1	32 bits
Motorola-Canopy-VLMGVID	26.161.22	integer	N	1 – 4094	
Configuration > VLAN > Management VID				1	32 bits
Motorola-Canopy-VLSMMGPASS	26.161.23	integer	N	0-disable, 1-enable	
Configuration > VLAN > SM Management VID Pass-through				1	32 bits
Motorola-Canopy-BCASTMIR	26.161.24	integer	N	0-50000+ kbps, 0=disabled	
Configuration > Quality of Service > Broadcast/Multicast Uplink Data Rate				dependent on radio feature set	32 bits
Motorola-Canopy-UserLevel	26.161.50	integer	N	1-Technician, 2-Installer, 3-Administrator	
Account > Add User > Level				0	32 bits
Note about VSA numbering: 26 connotes Vendor Specific Attribute, per RFC 2865 26.311 is Microsoft Vendor Code, per IANA 26.161 is Motorola Vendor Code, per IANA					

5.6   CONFIGURING AP AND SM FOR CENTRALIZED AP AND SM USER NAME AND PASSWORD MANAGEMENT

5.6.1   AP – Technician/Installer/Administrator Authentication

To control technician, installer, and administrator access to the AP from a centralized RADIUS server:

1. Set **Authentication Mode** on the AP's Configuration > Security tab to **RADIUS AAA** as shown in Figure 5: AP's Account > User Authentication tab.

2. Set **User Authentication Mode** on the AP's Account > User Authentication tab (the tab only appears after the AP is set to RADIUS authentication) to **Remote** or **Remote then Local**.

   - **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed.

   - **Remote**: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **RADIUS AAA Authentication Mode** selected. For up to 2 minutes a test pattern will be displayed until the server responds or times out.

   - **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.

Either the same RADIUS server used for SM authentication and authorization can be used for user authentication and accounting (access control), or a separate RADIUS accounting server can be used. Indicate your network design under **User Authentication Server**.

If separate accounting server(s) are used, configure the IP address(es) and **Shared Secret**(s) in the **Accounting Server** fields. The default **Shared Secret** is "CanopyAcctSecret". Up to 3 servers can be used for redundancy. Servers 2 and 3 are meant for backup and reliability, not splitting the database. If Server 1 doesn't respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, Server 2 is not tried.

Accounts → User Authentication

5.7GHz - Access Point - 0a-00-3e-fc-56-40

(Save Changes)

User Authentication	⊟
User Authentication Mode :	Remote ▲▼
User Authentication Server :	◉ Use RADIUS Authentication Servers ○ Use RADIUS Accounting Servers Defined Below
Accounting Server 1 :	0.0.0.0 Shared Secret
Accounting Server 2 :	0.0.0.0 Shared Secret
Accounting Server 3 :	0.0.0.0 Shared Secret
Auth Method :	EAP−MD5 ⬍
Device Access Tracking :	○ Enabled ◉ Disabled
Allow Local Login after Reject from AAA :	○ Enabled ◉ Disabled

Figure 5: AP's Account > User Authentication tab

5.6.2   SM – Technician/Installer/Administrator Authentication

To control technician, installer, and administrator access to the SM from a centralized RADIUS server:

1. Set **Authentication Mode** on the AP's Configuration > Security tab to **AAA** (RADIUS)

2. Set **User Authentication Mode** on the AP's Account > User Authentication and Accounting tab (the tab only appears after the AP is set to AAA authentication) to **Remote** or **Remote then Local**.

3. Set **User Authentication Mode** on the SM's Account > User Authentication and Accounting tab to **Remote** or **Remote then Local** as shown in Figure 6: SM's Account > User Authentication tab.

   ▪ **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed.

   ▪ **Remote**: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **AAA** (RADIUS) **Authentication Mode** selected. For up to 2 minutes a test pattern will be displayed until the server responds or times out.

   ▪ **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the SM's menu.

Note, remote access control is enabled only after the SM registers to an AP that has **Authentication Mode** set to **RADIUS AAA**. Local access control will always be used before registration and will be used after registration if the AP is not configured for RADIUS.

Accounts → User Authentication

5.7GHz - Subscriber Module - 0a-00-3e-fe-ed-df

(Save Changes)

User Authentication   ⊟

Remote Login is enabled only when SM is Registered with an AP and the system is operating with a back-end AAA server. The SM will only do Local Login until these preconditions are met regardless of configuration settings on this page.
Current State: SM Not Operating with AAA.

User Authentication Mode :	Local ▼
Device Access Tracking :	○ Enabled ⦿ Disabled
Allow Local Login after Reject from AAA :	○ Enabled ⦿ Disabled

Figure 6: SM's Account > User Authentication tab

5.6.3 Access Tracking

To track logon and logoff times on individual radios by technicians, installers, and administrators, on the AP or SM's Account > User Authentication and Accounting tab under **Accounting** (Access Tracking) choose **Enabled.**

Device Access Tracking is enabled separately from **User Authentication Mode**. A given AP or SM can be configured for both, either, or neither.

Device Access Tracking does not track and report specific configuration actions performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as the Motorola One Point Wireless Manager.

5.7   CONFIGURING YOUR RADIUS SERVER FOR DEVICE ACCESS TRACKING

The VSA needed for device access tracking and the associated values are shown in

5.8   PROCEDURES

5.8.1 Configuring a basic system

For a basic system:

On the SM's Configuration -->Security tab:

- o Lock AAA: Disabled
- o Phase 1: EAPTTLS (can't be changed)

- o Phase 2: PAP
- o Disable Realm
- o User Name (MAC address is the default) (The RADIUS server has to use the same username)
- o Password: password (The RADIUS server has to use the same password)
- o Default Certificate file

On the SM's Accounts > User Authentication tab:

- o User Authentication Mode: Local
- o Device Access Tracking: disabled

On the AP's Configuration > Security tab:

- o Authentication Mode: RADIUS AAA
- o Authentication Server1: IP address of the RADIUS server
- o Shared Secret: CanopySharedSecret (The RADIUS server has to use this same Shared Secret for the NAS)
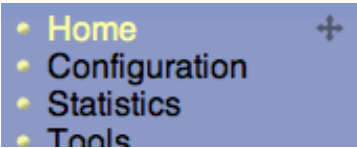
On the AP's Accounts > User Authentication tab:

- o User Authentication Mode: Local
- o User Authentication Server: Use RADIUS Authentication Servers
- o Device Access Tracking: Disabled

6   Resolved Issues

Issues resolved in Release 11.0 are listed in Table 3.

Table 3: Improvements and issues resolved in Release 11.0

Products Affected	Issue	Discussion
All	The main menu can be repositioned and float over the page. (14295)	The main menu can float and be repositioned by dragging it using the repositioning icon that appears in the upper right corner when the cursor hovers on the menu:
SM	Under certain conditions, some SMs were not acquiring a DHCP lease when they booted. (15935)	SMs configured with VLAN enabled, MVID ≠ 1, and obtaining their management IP address using DHCP would not acquire a DHCP lease when rebooted. The issues are now resolved and DHCP leases work as desired. (DHCP is enabled on the Configuration > IP tab if not using NAT, or on the Configuration > NAT tab if NAT is enabled. VLAN parameters are set on the Configuration > VLAN tab.)

7   Known Open Issues

Known open issues for Release 11.0 are listed in Table 4.

Table 4: Release 11.0 known open issues

Products affected Release reported	Description	Discussion and Recommendations
All R11.0	Only first 16 characters of User Name used. (15912)	On the Accounts > Add User tab, a User Name of more than 16 characters can be entered, but only the first 16 characters are actually used to create the user name. Workaround: Restrict user names to 16 characters or less.

8 Notes and Reference

8.1   NOTES

Notes and tips for best operation are listed in Table 5, Table 6, and Table 7, and Table 8.

Table 5: Notes first discussed with Release 11.0

Products Affected	Description	Discussion and Recommendations
All	Use only "one level" certificates	Root certificates of more than one level (a certificate from somebody who got their CA from Verisign, for example) will fail. Certificates must be either root or self-signed.
All	Watch timestamp on certificates	If an SM's certificate has a "Valid From" date and time that is after the current system time, the SM will not authenticate onto the system. Either create certificates with a "Valid From" date and time that is before any possible system time, or ensure the AP is configured to use a Network Time Protocol (NTP) server, such as the one in the CMMmicro or CMM4, and the certificates have a "Valid From" date and time before the current time. The initial system time on Canopy, with no NTP or GPS source, is 01/01/2001 00:00:00.

Table 6: Notes first discussed with Release 10.5

Products Affected	Description	Discussion and Recommendations
All	Browser-specific GUI behavior (Firefox) (15713)	The scenario is you are using a browser to view a web page on a radio and then use SNMP to make configuration changes to parameters shown on the page. With some browsers, the SNMP-made changes are shown after a manual or automatic page *refresh*. With Firefox, a manual page *change* (go to another tab and come back) is required.

Table 7: Notes first discussed with Release 10.3.1
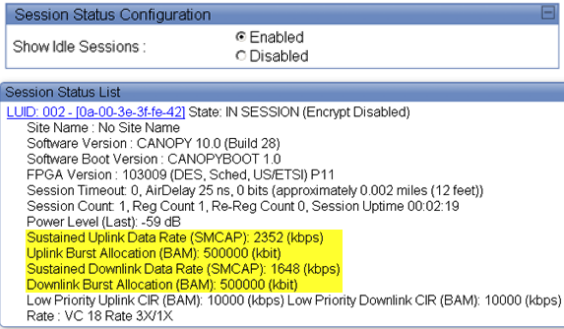
Products Affected	Description	Discussion and Recommendations
PMP 430 used with Prizm or BAM	PMP 430 SM MIR configured by Prizm to greater than max sustained MIR data rate (12257)	If the **Configuration Source** on a PMP 430 AP's Configuration > General tab is set to **Authentication Server** or **Authentication Server + SM**, SMs will receive their MIR settings from Prizm (or BAM). The resulting SM MIR may be greater than the keyed throughput of the SM. For context, the PMP 430 SM is available keyed to have a maximum throughput of 4, 10, 20 or 40 Mbps. If the SM receives a MIR setting from Prizm that is greater than the keyed bandwidth, the SM will cap the MIR using this formula: (desired uplink MIR * SM aggregate capped rate) / desired aggregate rate (desired downlink MIR * SM aggregate capped rate) / desired aggregate rate Note: Desired aggregate rate is the sum of the desired uplink rate and desired downlink rate For example, if a PMP 430 4 Mbps SM with a max MIR cap of 4000 receives a MIR setting from Prizm that is greater than 4000 kbps, it will cap the downlink MIR and the uplink MIR to equal a max of 4000 kbps. Below is an example with Prizm settings of 10000 kbps uplink MIR and 7000 downlink MIR sent to a 4 Mbps SM that is capped at 4000 kbps max MIR: Uplink calculation: (10000 * 4000) / (7000 + 10000) = 2352 kbps Downlink calculation: (7000 *4000) / (7000 + 10000) = 1648 kbps Thus the Uplink MIR of 2352 + Downlink MIR of 1648 = 4000 kbps In this example, the PMP 430 AP sessions page will display a SM uplink and downlink MIR SMCAP as shown below. For reference, the max SM MIR in kbps for each SM type is: 4 Mbps SM = 4000 10 Mbps SM = 10000 20 Mbps SM = 20000 40 Mbps SM = 65535 (displays Unlimited in the Home > General Status tab)

Table 8: Notes first discussed with Release 9.5

Products Affected	Description	Discussion and Recommendations
All	SM – DNS below a NATed SM when DNS Server Proxy is enabled	Microsoft Vista and Windows 7 will not route a 169.254/16 subnet used as the default Canopy subnet since these operating systems use 169.254/16 subnet to talk between local machines. This is not an issue if: - the PC is connected directly to the NATed SM. - the NAT/routing CPE underneath the NATed SM provides DNS services. However; if a NAT/routing CPE that is not providing DNS services (e.g. some home routers) is placed between the SM and the user's PC, a Microsoft Vista or Windows 7 machine will not route to the default 169.254/16 SM IP address space to access DNS services. **Workaround:** Reconfigure the SMs NAT LAN address to a private IP address such as 192.168/16, 172.16/12, or 10/8 or leave DNS Server Proxy disabled.
All	Updating Community Strings on the Web GUI (11699)	To flip-flop the read/write and read-only community string names, it is necessary to change one community string to a temp name first before switching community string names.
Remote AP	Remote AP Sync Input (7427)	Remote AP receives sync from SM by setting SYNC Input to Timing Port. However, if this is incorrectly configured as SYNC input to Power port the Remote AP will still correctly receive SYNC.
AP	Disable TCP ACK prioritizing in broadcast video applications (10263)	When optimizing a system for broadcast video, on the AP's Configuration => General page configure **Prioritized TCP ACK** to **Disabled**. In a system being used for internet access or similar applications prioritizing TCP ACKs improves downloading of FTP files and other activities making significant use of TCP ACKs under heavy load. However, in a system being used for broadcast video or video surveillance, prioritizing TCP ACKs can cause sporadic choppy video in the uplink.
AP or SM	Procedures for saving an XML file of a spectrum graph (8484)	When the **SpectrumAnalysis.xml** button is clicked on the SM's Tools > Spectrum Analyzer tab or the AP's Tools > Remote Spectrum Analyzer tab, the spectrum graph is redisplayed using XML and XSL if the browser supports XSL. To save the underlying XML file, right click and select "Save Target As" on a Windows PC, or equivalent action for other operating systems.
SM	SM scan frequencies not "cancelled" by SNMP actions (8172)	If you make frequency changes on the SM GUI, and then back them out using SNMP, the Reboot Required message remains on the GUI. Workaround: If it says Reboot Required, go ahead and reboot, just to clear the message.

Products Affected	Description	Discussion and Recommendations
All	Managing module accounts and passwords (none)	The best security practice is to be aware a factory unit comes with `root` and `admin` accounts, to plan your approach to accounts, and set passwords for all accounts.
		A module that either is fresh from the factory or has been operator-reset to factory defaults has two user accounts: `root` and `admin`, both with ADMINISTRATOR level permissions.
		To secure a module, access the Account => Change Users Password tab and add a password to each of these accounts. Adding a password to only one account still leaves the other open. Furthermore, an account without a password will accept any password potentially giving the impression the unit is protected when it isn't.
		Alternatively, an operator's practices may be to delete the `admin` account or delete the `root` account and replace them with their own account(s). By default, Prizm, One Point Wireless Manager and CNUT use the `root` account to manage the module, so if you delete `root` accounts on modules you will need to make coordinated changes to Prizm, Wireless Manager, and CNUT to access them with your own accounts.
All	Use 16 or fewer alphanumeric characters in user account names, passwords, and Community Strings (7808)	SNMP doesn't do data-entry checking, so more than 16 characters may be entered, but only 16 characters will be saved and displayed.
AP and SM	Timed Spectrum Analyzer settings anomaly (7442)	Values of **Timed Spectrum Analyzer** duration and **Spectrum Analysis on Boot** get saved by clicking any button on the page, not just when clicking **Save Changes** or **Start Time Spectrum Analysis** (which is typical operation for other pages).
AP and SM	Best Practice is to set SM to same **Region Code** as AP (none)	When an SM registers to an AP, it assumes the Region Code and associated parameters of the AP, disregarding any Region code set in the SM by you. However, the best practice is still for you to set a Region Code in the SM so that displayed options are consistent with the region.
All	Details on pinging Canopy modules (4831)	A ping size larger than 1494 bytes to a radio will time out and fail. However, a ping of greater than 1494 bytes to a system that is behind a radio typically succeeds. To gain an accurate view of latency, ping through the radio to a system beyond. Canopy transports ping traffic with the same priority as all transport traffic, but may handle a direct ping with lower priority when running under load.
SM	AP may be listed twice in SM's AP Evaluation tab (5298)	To help during aiming, the SM's Tools > AP Evaluation tab maintains AP entries for 15 minutes. If the frequency of an AP is changed, for 15 minutes the AP is listed twice in the AP Evaluation tab, once with the former frequency, and once with the new one.
AP and SM	When using **Link Test with MIR**, need to set both ends (4844, 2756)	To see the effects of MIR capping, you can run a link test with MIR enabled. To get meaningful results, set **Link Test with MIR** to **Enabled** on the Tools => Link Capacity Test tab *in both* the SM and the AP. When it is enabled on only one end, results are misleading.
		After you run perform a link test with MIR capping enabled, consider immediately changing **Link Test with MIR** to **Disabled** *in both* the SM and the AP, to avoid mistakenly capping only one end of the link test.

Products Affected	Description	Discussion and Recommendations
AP and SM	Click Spectrum Analyzer **Enable** button twice (5284)	After you click the **Enable** button in the Tools => Spectrum Analyzer tab, the resulting display may omit bars for some frequencies, especially in frequency bands that have a large number of center channels, such as the 5.4-GHz band. If you clicking **Enable** again, the display includes the entire spectrum bar graph. *TIP:* In the Configuration => General tab, set the **Webpage Auto Update** parameter to a few seconds, to have the Spectrum Analyzer automatically fully displayed and refreshed. You can later reset the **Webpage Auto Update** time back to `0`, to disable refresh.
AP and SM	Blank screen after logging in to SM through AP Session Status tab (4706)	In some instances, depending on network activity and network design, the interface presents a blank screen to a user who logs in to an SM through the Home => Session Status tab in the AP. If you observe this, refresh your browser window.
SM	When connecting to a hub, use only half duplex Ethernet settings (7557)	Ethernet connections set to **10 Base T Full Duplex** or **100 Base T Full Duplex** will not connect to an SM through a hub, due to the way a hub works. Use half duplex settings when using a hub.

8.2   US REGION CODE OPERATION

A 5-GHz PMP 100/400/430 Series AP or a PTP 100/200 Series BH with a **Region Code** set to **United States** is not configurable to another **Region Code** by installers or end users. This is in response to FCC KDB 594280 and ensures that end users and professional installers do have access to settings which could allow a radio to be configured to operate in a manner other than that which was specified in the FCC equipment authorization grant.

Radios sold in the United States and its territories come with the **Region Code** on the Configuration > General tab pre-configured to United States and not selectable, as shown in Figure 7. Radios sold in regions outside of the United States and its territories are required to be set by the operator to the Region Code of the region in which they are used.
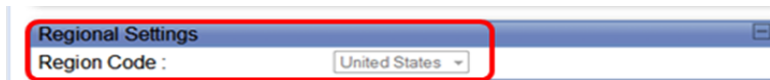
Figure 7: PMP AP and PTP BH Region Code Set to United States

Refer to Table 9 and Table 10 for lists of 5-GHz U.S. model numbers and center channels.

Table 9: 5-GHz OFDM PMP & PTP U.S. Region Code operation

OFDM Radio	U.S. Model Number	Channel Size	Center Channels
PMP 400 Series AP, 5.4-GHz	5440APUS (DES) 5441APUS (AES)	10MHz	5480 – 5595 and 5655 – 5710 (configurable on 5MHz center channels)
PMP 430 5.8-GHz Series AP, 5.8-GHz	5780APUS (DES) 5781APUS (AES)	5MHz	5727.5 – 5845 (configurable on 2.5MHz center channels)
		10MHz	5730 – 5845 (configurable on 5MHz center channels)
		20MHz	5735 – 5840 (configurable on 5MHz center channels)
PTP 200 Series BH, 5.4-GHz	5440BHUS (DES) 5441BHUS (AES)		5480 – 5595 and 5655 – 5710 (configurable on 5MHz center channels)
Note: New APs and BHs for use in the US have a model number ending in "US". For older modules, regulatory compliance mandates that the operator select the correct region code. Note: The PMP 430 5.4-GHz AP/SM is pending regulatory approval for the U.S. and Canada.			

Table 10: 5-GHz FSK PMP & PTP U.S. Region Code operation

FSK Radio	Description	U.S. Model Number	Encryption Type	Center Channels
PMP 120 (7Mpbs) 20MHz Channel Size	5.2-GHz AP	5200APUSG	DES	5275 – 5325
		5201APUSG	AES	
	5.4-GHz AP	5400APUSG	DES	5495 – 5585 and 5665 – 5705
		5401APUSG	AES	
	5.7-GHz AP	5700APUSG	DES	5735 – 5840
		5701APUSG	AES	
PMP 130 (14Mpbs) 20MHz Channel Size	5.2-GHz AP	5250APUSG	DES	5275 – 5325
		5251APUSG	AES	
	5.4-GHz AP	5450APUSG	DES	5495 – 5585 and 5665 – 5705
		5451APUSG	AES	
	5.7-GHz AP	5750APUSG	DES	5735 – 5840
		5751APUSG	AES	
PTP 120 (7Mbps) 20MHz Channel Size	5.2-GHz BH	5200BHUSG	DES	5275 – 5325
		5201BHUSG	AES	
	5.4-GHz BH	5400BHUSG	DES	5495 – 5585 and 5665 – 5705
		5401BHUSG	AES	
	5.7-GHz BH	5700BHUSG	DES	5735 – 5840
		5701BHUSG	AES	
PTP 130 (14Mpbs) 20MHz Channel Size	5.2-GHz BH	5200BH20USG	DES	5275 – 5325
		5201BH20USG	AES	
	5.4-GHz BH	5400BH20USG	DES	5495 – 5585 and 5665 – 5705
		5401BH20USG	AES	
	5.7-GHz BH	5700BH20USG	DES	5735 – 5840
		5701BH20USG	AES	
Note: New APs and BHs for use in the US have a model number ending in "US". For older modules, regulatory compliance mandates that the operator select the correct region code.				

8.3   PMP 430 CENTER CHANNELS

When the PMP 430 AP is using 5-MHz channels, the center channels can be configured every 2.5 MHz. When it is using 10- or 20-MHz channels, the center channels can be configured every 5 MHz. Available center channels as a function of channel size and regioin are shown in Table 11.

Table 11: PMP 430 center channels by channel bandwidth and region code

OFDM Radio Model	Channel Size	Region Code(s)	Range of Center Frequencies Available (MHz)	Center Channel Spacing	# of Center Channels
PMP 430 Series AP, 5.4-GHz	5 MHz	United States, Canada & Australia	5475 – 5597.5 5652.5 – 5715	2.5 MHz	76
		Europe & Spain	5472.5 – 5597.5 5652.5 – 5717.5	2.5 MHz	78
		Brazil, India, Russia & Other	5475 – 5715	2.5 MHz	97
	10 MHz	United States, Canada & Australia	5480 – 5595 5655 – 5710	5 MHz	36
		Europe & Spain	5475 – 5595 5655 – 5715	5 MHz	38
		Brazil, India, Russia & Other	5480 – 5710	5 MHz	47
	20 MHz	United States, Canada & Australia	5480 – 5590 5660 – 5710	5 MHz	34
		Europe & Spain	5475 – 5590 5660 – 5715	5 MHz	36
		Brazil, India, Russia & Other	5480 – 5710	5 MHz	47
PMP 430 Series AP, 5.8-GHz	5 MHz	United States, Canada, Australia, Brazil & Russia	5727.5 – 5845	2.5 MHz	48
		Europe & Other	5727.5 – 5872.5	2.5 MHz	59
		Spain	5727.5 – 5792.5 5817.5 – 5852.5	2.5 MHz	42
		India	5827.5 – 5872.5	2.5 MHz	19
	10 MHz	United States, Canada, Australia, Brazil & Russia	5730 – 5845	5 MHz	24
		Europe & Other	5730 – 5870	5 MHz	29
		Spain	5730 – 5790 5820 – 5850	5 MHz	20
		India	5830 – 5870	5 MHz	9
	20 MHz	United States, Canada, Australia, Brazil & Russia	5735 – 5840	5 MHz	22
		Europe & Other	5735 – 5865	5 MHz	27
		Spain	5735 – 5785 5825 – 5845	5 MHz	16
		India	5835 – 5865	5 MHz	7

8.4   PMP 100 SERIES DFS OPERATION BASED ON REGION CODE

For reference, Table 12 shows operating based on Region Code, by frequency band and module type. Note: 900MHz and 2.4-GHz are not shown as DFS operation does not apply to these frequencies.

Table 12: PMP 100 AP/SM DFS operation based on region code

Region Code[1]	5.1 GHz	5.2 GHz		5.4 GHz		5.7 GHz	
	AP/SM	AP	SM	AP	SM	AP	SM
United States	NA	≥P10: FCC/IC DFS ≤ P9: no DFS	No effect	FCC/IC DFS No 5590-5660 MHz[2]	No effect	No effect	No effect
Canada	NA	≥ P10: FCC/IC DFS ≤ P9: no DFS	No effect	FCC/IC DFS No 5590-5660 MHz[2]	No effect	No effect	No effect
Europe & Spain	NA	NA	NA	ETSI EN 301 893 v1.3.1 DFS >July 1, 2008[3]: No 5590-5660 MHz[2]	ETSI EN 301 893 v1.3.1 DFS >July 1, 2008[3]: No 5585-5665 MHz[2]	ETSI EN 302 502 v1.2.1 DFS	ETSI EN 302 502 v1.2.1 DFS
Brazil	NA	NA	NA	P11: ETSI v1.4.1 DFS ≤ P10: ETSI v1.3.1 DFS	No effect	No effect	No effect
Australia	NA	NA	NA	FCC/IC DFS No 5590-5660 MHz[2]	No effect	No effect	No effect
Russia	Display Community options	No effect	No effect	NA	NA	No effect	No effect
India or Other	No effect	No effect	No effect	No effect	No effect	No effect	No effect

1. In all cases, set the **Region Code** to the region you are in, and the software will determine the correct use of DFS.
2. Terminal Doppler Weather Radar (TDWR) operates on frequencies 5600 through 5650 MHz. In some countries a "weather notch" is required to avoid impinging on these frequencies.
3. Radios placed on market in Europe after July 1, 2008, can't impinge on weather radar frequencies. To meet this requirement, the software checks the date code of the module and implements the weather notch accordingly. You can tell if a 5.4-GHz module is "newer" or "older" by setting the Region Code to Europe – if the notch frequencies *are not* shown on the Configuration => Radio page, then the module is "newer", if the notch frequencies *are* shown, the module is "older".

8.5   PTP 100 SERIES DFS OPERATION BASED ON REGION CODE

For reference, Table 13 shows operating based on Region Code, by frequency band and module type.

Table 13: PTP 100 backhaul operation based on region code

Region Code[1]	2.4 GHz	5.1 GHz	5.2 GHz		5.4 GHz		5.7 GHz	
	BH	BH	BHM	BHS	BHM	BHS	BHM	BHS
United States	No effect	NA	≥P10: FCC/IC DFS ≤ P9: no DFS	No effect	FCC/IC DFS No 5590-5660 MHz in FSK[2]	No effect	No effect	No effect
Canada	No effect	NA	≥ P10: FCC/IC DFS ≤ P9: no DFS	No effect	FCC/IC DFS No 5590-5660 MHz in FSK[2]	No effect	No effect	No effect
Europe	No effect	NA	NA	NA	ETSI EN 301 893 v1.3.1 DFS >July 1, 08[3]: No 5590-5660 MHz in FSK[2]	ETSI EN 301 893 v1.3.1 DFS >July 1, 08[3]: No 5585-5665 MHz in FSK[2]	ETSI EN 302 502 v1.2.1 DFS	ETSI EN 302 502 v1.2.1 DFS
Brazil	NA	NA	NA	NA	P11: ETSI v1.4.1 DFS ≤ P10: ETSI v1.3.1 DFS	No effect	No effect	No effect
Australia	No effect	NA	NA	NA	FCC/IC DFS No 5590-5660 MHz in FSK[2]	No effect	No effect	No effect
Russia	NA	Display Community options	No effect	No effect	NA	NA	No effect	No effect
India or Other	No effect	No effect	No effect	No effect	No effect	No effect	No effect	No effect

1. In all cases, set the **Region Code** to the region you are in, and the software will determine the correct use of DFS.

2. Terminal Doppler Weather Radar (TDWR) operates on frequencies 5600 through 5650 MHz. In some countries a "weather notch" is required to avoid impinging on these frequencies.

3. Radios placed on market in Europe after July 1, 2008, can't impinge on weather radar frequencies. To meet this requirement, the software checks the date code of the module and implements the weather notch accordingly. You can tell if a 5.4-GHz module is "newer" or "older" by setting the Region Code to Europe – if the notch frequencies *are not* shown on the Configuration => Radio page, then the module is "newer", if the notch frequencies *are* shown, the module is "older".

8.6   PMP 400/430 AND PTP 200 DFS OPERATION BASED ON REGION CODE

For reference, Table 14 shows operation based on Region Code, by frequency band and radio platform. PMP 400 and PTP 200 are available in the 5.4-GHz frequency band. PMP 430 is available in both the 5.4 and 5.8-GHz frequency band.

Note: The 4.9-GHz PMP 400 and PTP 200 are not shown as DFS operation does not apply to these frequencies.

Table 14: PMP 400/430 and PTP 200 DFS operation based on region code

Region Code[1]	Frequency	Radio Platform	AP	SM
United States	5.4-GHz	PMP 400 & PTP 200	FCC/IC DFS[3]	No effect
	5.8-GHz	PMP 430	No effect	No effect
Canada	5.4-GHz	PMP 400 & PTP 200	FCC/IC DFS[3]	No effect
	5.8-GHz	PMP 430	No effect	No effect
Europe & Spain	5.4-GHz	PMP 400/430 & PTP 200	ETSI DFS[4]	ETSI DFS[4]
	5.8-GHz	PMP 430	ETSI DFS[5]	ETSI DFS[5]
Brazil	5.4-GHz	PMP 400/430 & PTP 200	ETSI DFS[4]	No effect
	5.8-GHz	PMP 430	No effect	No effect
Australia	5.4-GHz	PMP 400/430 & PTP 200	FCC/IC DFS[3]	No effect
	5.8-GHz	PMP 430	No effect	No effect
Russia	5.4-GHz	PMP 400/430 & PTP 200	No effect	No effect
	5.8-GHz	PMP 430	No effect	No effect
India	5.4-GHz	PMP 400/430 & PTP 200	No effect	No effect
	5.8-GHz	PMP 430	No effect	No effect
Other	5.4-GHz	PMP 400/430 & PTP 200	No effect	No effect
	5.8-GHz	PMP 430	No effect	No effect

4. In all cases set the **Region Code** to the region you are in and the equipment will provide DFS consistent with that region's regulations. For countries or regions not listed, use a Region Code that provides DFS functionality and channels consistent with your country's regulatory requirements.
5. In some countries and regions, 5600 MHz to 5650 MHz is "notched" out to meet requirements to not transmit in weather radar frequencies.
6. Complies with FCC Report and Order 03-287 and Industry Canada requirements.
7. Complies with ETSI EN 301 893 v1.3.1.
8. Complies with ETSI EN 302 502 v1.2.1.

9   Canopy MIB

The Canopy Enterprise MIB (Management Information Base) consists of 5 MIB definition files and supports SNMP access to Canopy modules. The MIB files are available for download from the Canopy tab of http://motorola.wirelessbroadbandsupport.com/software.

Detailed information on the Canopy MIBs is available at http://motorola.wirelessbroadbandsupport.com/support/online_tools.

MIB files are used by Network Management Systems and Element Management Systems, such as the Motorola Prizm and One Point Wireless Manager systems, to support a host of surveillance, monitoring, control, and operational tasks.

Information on the Motorola Prizm element management system is available at http://www.motorolasolutions.com/Business/US-EN/Business+Product+and+Services/Wireless+Broadband+Networks/Point-to-Multipoint+Networks/Unlicensed+Point-to-Multipoint+Solutions/Element_Management_PTMP_US-EN

Information on the Motorola One Point Wireless Manager management system is available at http://www.onepointwireless.com/wirelessmanager/

Prizm and One Point Wireless Manager documentation and installers are available for download from the Canopy tab of http://motorola.wirelessbroadbandsupport.com/software.

If you are using Prizm: Prizm 3.3.10 includes the MIB information. You do not need to load MIB files.

If you are using One Point Wireless Manager 2.2 or an SNMP network management system (NMS) or element management system (EMS) other than Prizm: Load the MIBs per the instructions for One Point Wireless Manager 2.2 or your NMS or EMS.

> *Important!*   When loading the Canopy MIB files
>
> 1. First load the standard MIB files.
> 2. Then load the Canopy MIB files.

Some NMSs are not sensitive to order, but some require a specific loading order to build a MIB tree. Loading in the recommended order avoids any problems arising from loading sequence.

10 Performance Benchmarking Process

This section describes the performance benchmarking process.

10.1   DEFINITIONS

The following terms are used where these release notes discuss packet processing:

Aggregate Throughput Sum of uplink plus downlink traffic.

Offered Load Test equipment generates a specified load to the Ethernet interface of a module (SM or the AP). The specifications of the load include both packet size and packet rate.

Carried Load Test equipment measures the load delivered at the Ethernet interface of a module. The load is calculated from packet size and number of packets. As resources are exhausted at any point in the system, packets may be dropped. The Carried Load equals the Offered Load minus Dropped Packets.

Downlink/Uplink Load Ratio The ratio of downlink Carried Load to uplink Carried Load.

NOTE: Do not confuse the Downlink/Uplink Load Ratio with the **Downlink Data** configuration parameter. The Downlink/Uplink Load Ratio is determined from the Carried Loads. The **Downlink Data** is set by the operator and determines the split of downlink and uplink slots in the air frame.

10.2   SYSTEM PERFORMANCE AND SYSTEM CONSTRAINTS

Different combinations of system inputs will result in different constraints limiting system performance.

Larger Packets

With larger packets (the system handles packets up to 1522 Bytes), the system constraint is *airtime*, which can also be stated as *slots*, or maximum bits per second.

This can be calculated as follows:

PMP 100 and PTP 100 Backhauls with 20MHz Channels:

64 Bytes/fragment x 2 fragments/slot x 34 slots/frame x 400 frames/sec x 8 bits/byte = 14 Mbps

This is an aggregate (uplink plus downlink) limit, as the Canopy system is a Time Division Duplex (TDD) system.

14 Mbps is a typical maximum aggregate throughput for larger packet sizes for an FSK system. Longer range settings can reduce the number of slots in a frame and packet size (breakage on 64-byte boundaries) can affect packing efficiency (the percentage of fragments fully packed with 64 bytes).

PMP 430 (5.4 and 5.8-GHz OFDM) with 5MHz Channels:

For 1/4 Cyclic Prefix the calculation is

64 Bytes/fragment x **3** fragments/slot x **15** slots/frame x 400 frames/sec x 8 bits/byte = **9.2** Mbps

For 1/8 Cyclic Prefix the calculation is

64 Bytes/fragment x **3** fragments/slot x **17** slots/frame x 400 frames/sec x 8 bits/byte = **10.4** Mbps

For 1/16 Cyclic Prefix the calculation is

64 Bytes/fragment x **3** fragments/slot x **18** slots/frame x 400 frames/sec x 8 bits/byte = **11.0** Mbps

With 5MHz channels, 9.2 Mbps is a typical maximum aggregate (uplink plus downlink) throughput for larger packet sizes in a system configured with 1/4 cyclic prefix. For 1/8 cyclic prefix systems 10.4 Mbps is a typical maximum aggregate throughput and for 1/16 cyclic prefix 11.0 Mbps is a typical maximum aggregate throughput. Longer range settings can reduce the number of slots in a frame and packet size (breakage on 64-byte boundaries) can affect packing efficiency (the percentage of fragments fully packed with 64 bytes).

PMP 430 (5.4 and 5.8-GHz OFDM) with 10MHz Channels:
For 1/4 Cyclic Prefix the calculation is

64 Bytes/fragment x **3** fragments/slot x **33** slots/frame x 400 frames/sec x 8 bits/byte = **20.2** Mbps

For 1/8 Cyclic Prefix the calculation is

64 Bytes/fragment x **3** fragments/slot x **37** slots/frame x 400 frames/sec x 8 bits/byte = **22.7** Mbps

For 1/16 Cyclic Prefix the calculation is

64 Bytes/fragment x **3** fragments/slot x **42** slots/frame x 400 frames/sec x 8 bits/byte = **25.8** Mbps

With 10MHz channels, 20.2 Mbps is a typical maximum aggregate (uplink plus downlink) throughput for larger packet sizes in a system configured with 1/4 cyclic prefix. For 1/8 cyclic prefix systems 22.7 Mbps is a typical maximum aggregate throughput and for 1/16 cyclic prefix 25.8 Mbps is a typical maximum aggregate throughput. Longer range settings can reduce the number of slots in a frame and packet size (breakage on 64-byte boundaries) can affect packing efficiency (the percentage of fragments fully packed with 64 bytes).

PMP 430 (5.4 and 5.8-GHz OFDM) with 20MHz Channels:
For 1/4 Cyclic Prefix the calculation is

64 Bytes/fragment x **3** fragments/slot x **73** slots/frame x 400 frames/sec x 8 bits/byte = **44.8** Mbps

For 1/8 Cyclic Prefix the calculation is

64 Bytes/fragment x **3** fragments/slot x **81** slots/frame x 400 frames/sec x 8 bits/byte = **49.7** Mbps

For 1/16 Cyclic Prefix the calculation is

64 Bytes/fragment x **3** fragments/slot x **86** slots/frame x 400 frames/sec x 8 bits/byte = **52.8** Mbps

With 20MHz channels, 44.8 Mbps is a typical maximum aggregate (uplink plus downlink) throughput for larger packet sizes in a system configured with 1/4 cyclic prefix. For 1/8 cyclic prefix systems 49.7 Mbps is a typical maximum aggregate throughput and for 1/16 cyclic prefix 52.8 Mbps is a typical maximum aggregate throughput. Longer range settings can reduce the number of slots in a frame and packet size (breakage on 64-byte boundaries) can affect packing efficiency (the percentage of fragments fully packed with 64 bytes).

Smaller Packets
With smaller packets, the system constraint is *processing power* in any module handling the traffic stream. Even though there may be airtime or slots available, the overall throughput is limited by packet handling ability.

10.3   BENCHMARK DEFINITION

In a complex system, any measurement depends on system configuration, traffic mix, various settings, and measurement techniques, and so to have reproducible results a "benchmark" is defined.

System configuration

The PMP benchmark system consists of 3 SMs and 1 Advantage AP, as shown in Figure 8 on page 42. Traffic generation and measurement equipment is connected to both SMs and the AP. Traffic is generated such that any one packet attempts to traverse an SM and then the AP, or the AP and then an SM. No SM-to-SM traffic is included in the benchmark. RF conditions are maintained such that all links run at max rate (2X or 3X).

Traffic mix/Packet size

All generated packets have a size of 64 Bytes. The packet format used is a valid Ethernet/IP packet. The performance of interest is performance near a 50% Downlink/Uplink Load Ratio.

PMP Settings

- Downlink Data: 50%
- Control Slots: 2
- Range: 2 miles
- Max rate (2X or 3X) Enabled
- Encryption: Enabled (DES modules)
- MIR: 20,000 kbits/sec sustained rate and 500,000 kbits burst allocation (defaults)
- CIR: 0 (default)
- NAT: Disabled (default)
- VLAN: Disabled (default)
- High Priority: Disabled (default)

PTP Settings

- Downlink Data: 50%
- Max rate (2X or 3X) Enabled
- Encryption: Enabled (DES modules)

Measurement technique

1. Send a specific number of frames at a specific rate through SMs and AP (uplinks) and AP and SM (downlink) simultaneously. This is the Offered Load. Count the frames that are received correctly at both sides. This is the Carried Load. Repeat this through the load rates of interest. Review the results, noting where the packet loss (the difference between the Offered Load and Carried Load) is essentially zero (<0.001%).

2. Confirm results by running longer tests at selected load rates.

3. Confirm results by varying Downlink/Uplink Load Ratios to ensure no significant changes around the 50% benchmark.
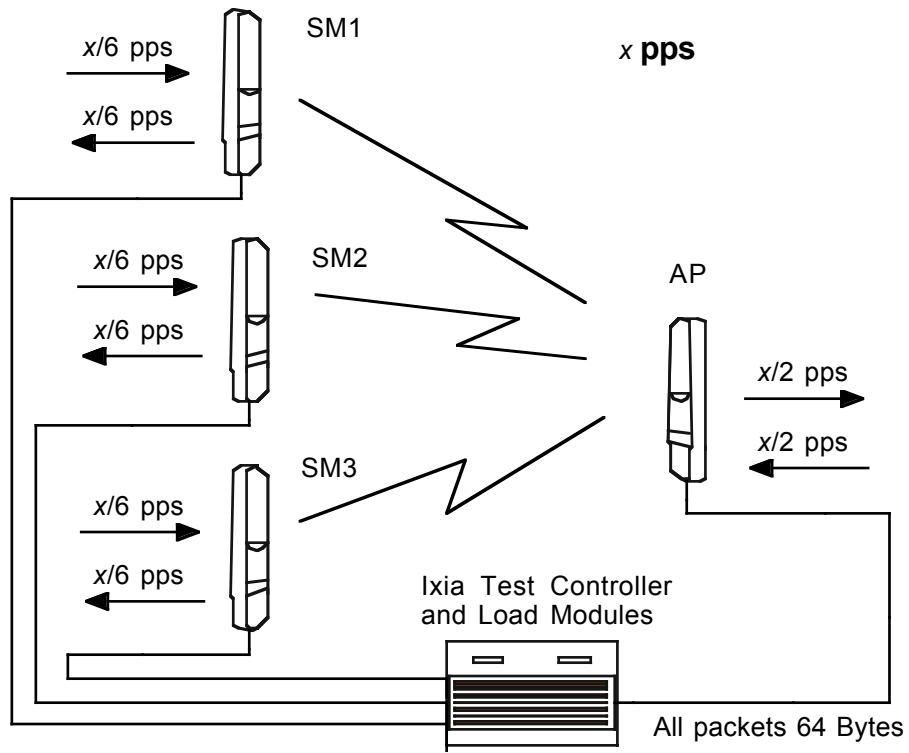
Figure 8: PPS Benchmark Test Setup

11 Regulatory and Legal Notices

11.1   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.

11.2   NATIONAL AND REGIONAL REGULATORY NOTICES

11.2.1   U.S. Federal Communication Commission (FCC) Notification

For 900MHz, 2.4, 5.2, 5.4, 5.7 and 5.8-GHz devices:

This device complies with Part 15 of the US FCC Rules and Regulations. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the US FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications.   If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

FCC IDs and the specific configurations covered are listed in Table 15.

For 4.9-GHz devices:

The 4.9-GHz band is a licensed band allocated to public safety services. State and local government entities that provide public safety services are eligible to apply for 4.9 GHz licenses. For additional information, refer to FCC regulations.

Table 15: US FCC IDs and Industry Canada Certification Numbers and covered configurations

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna	Maximum Tx Output Power
ABZ89FC5809	109W-9000	8 MHz channels, centered on 906-924 MHz in 1 MHz increments (within the 902-928 MHz ISM band)	9000 SM, AP	12 dBi integrated antenna	24 dBm (250 mW)
				17 dBi Last Mile Gear Cyclone 900-17H Yagi	18 dBm (63 mW)
				10 dBi Maxrad Model # Z1681 (MP9027XFPT or Motorola AN900A) flat panel	26 dBm (390 mW)
				10 dBi Mars Model # MA-IS91-T2, flat panel	26 dBm (390 mW)
				10 dBi MTI Model # MT-2630003/N (MT-263003/N) flat panel	26 dBm (390 mW)
ABZ89FC5808	109W-2400	20 MHz channels, centered on 2415-2457.5 MHz in 2.5 MHz increments (within the 2400-2483.5 MHz ISM band)	2400 BH, SM, AP	8 dBi internal	25 dBm (340 mW)
			2400 BH, SM	8 dBi internal + 11 dB reflector	25 dBm (340 mW)
ABZ89FC3789	109W-5200	20 MHz channels, centered on 5275-5325 MHz in 5 MHz increments (within the 5250-5350 MHz U-NII band)	5200 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5200 BH SM, AP	7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm (25 mW)
ABZ89FT7623	---	20 MHz channels, centered on 5495-5705 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band)	5400 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
				7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm (25 mW)
---	109W-5400	20 MHz channels, centered on 5495-5585 and 5665-5705 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band with 5600-5650 MHz excluded)	5400 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
				7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm (25 mW)

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna	Maximum Tx Output Power
ABZ89FC5804	109W-5700	20 MHz channels, centered on 5735-5840 MHz in 5 MHz increments (within the 5725-5850 MHz ISM band)	5700 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5700 BH, SM	7 dBi internal + 18 dB reflector	23 dBm (200 mW)
				7 dBi internal + 10 dB lens	23 dBm (200 mW)
			5700 AP	7 dBi internal + 10 dB lens	19 dBm (80 mW)
ABZ89FT7634	---	5 MHz channels, centered on 5727.5-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5780APC	17 dBi connectorized PCTEL Model 8514724E01 antenna (60° x 5° -3 dB beam width) with 1 dB connector cable loss	19 dBm
		10 MHz channels, centered on 5730-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)			19 dBm
		20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)			19 dBm
ABZ89FT7635	---	5 MHz channels, centered on 5727.5-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	10 dBi (55° x 55° -3 dB beam width)	19 dBm
		10 MHz channels, centered on 5730-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)			19 dBm
		20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)			19 dBm

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna	Maximum Tx Output Power
---	109W-5780	5 MHz channels, centered on 5727.5-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5780APC	17 dBi connectorized PCTEL Model 8514724E01 antenna (60° x 5° -3 dB beam width) with 1 dB connector cable loss	19 dBm
		10 MHz channels, centered on 5730-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)			19 dBm
		20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)			19 dBm
---	109W-5790	5 MHz channels, centered on 5727.5-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	10 dBi (55° x 55° -3 dB beam width)	19 dBm
		10 MHz channels, centered on 5730-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)			19 dBm
		20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)			19 dBm
ABZ89FT7629	---	10 MHz channels, centered on 5480-5595 and 5655-5710 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band with 5600-5650 MHz excluded)	5440 AP	18 dBi connectorized PCTEL Model 8514724E01 antenna (60° x 5° -3 dB beam width) with 1 dB connector cable loss	10 dBm
			5440 SM 5440 BH	17 dBi integrated antenna (15° x 15° -3 dB beam width)	10 dBm
---	109W-5440	10 MHz channels, centered on 5480-5595 and 5655-5710 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band with 5600-5650 MHz excluded)	5440 AP	18 dBi connectorized PCTEL Model 8514724E01 antenna (60° x 5° -3 dB beam width) with 1 dB connector cable loss	10 dBm
			5440 SM 5440 BH	17 dBi integrated antenna (15° x 15° -3 dB beam width)	10 dBm

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna	Maximum Tx Output Power
ABZ89FT7631	109W-4940	10 MHz channels, centered on 4945-4985 in 5 MHz increments (within the 4940-4990 MHz public safety licensed band)	4940 AP	18 dBi connectorized PCTEL Model AP 85010066001 antenna (60° x 5° -3 dB beam width) with 1 dB cable loss	18 dBm
			4940 SM 4940 BH	17 dBi integrated antenna (15.5° x 17.5° (el x az) -3 dB beam width)	18 dBm
Note 1: To ensure regulatory compliance, including DFS compliance, the professional installer is responsible for: ◦ setting the Region Code on the Configuration => General page to the correct region ◦ setting the Transmitter Output Power on the Confiiguration => Radio page no higher than listed for a given configuration ◦ setting the External Gain on the Configuration => Radio page, if displayed, to the gain of any external device (such as a reflector or lens)					

11.2.2   Industry Canada (IC) Notification

For 900MHz, 2.4-GHz, 5.2-GHz. 5.4-GHz, 5.7-GHz and 5.8-GHz devices:

This device complies with RSS-210 of Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Users should be cautioned to take note that in Canada high power radars are allocated as primary users (meaning they have priority) of 5250 – 5350 MHz and 5650 – 5850 MHz and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to RSS-210 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications.   If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

To reduce potential radio interference to other users, the antenna type and its gain should be chosen so its Equivalent Isotropic Radiated Power (EIRP) is not more than that permitted for successful communication.

Industry Canada Certification Numbers and the specific configurations covered are listed in Table 15.

This device has been designed to operate with the antennas listed in Table 15 and having a maximum gain as shown in Table 15. Antennas not included or having a gain greater than as shown in Table 15 are strictly prohibited from use with this device. Required antenna impedance is 50 ohms.

For 4.9-GHz devices:

The 4.9-GHz band is a licensed band allocated to public safety services. Government entities that provide public safety services are eligible to apply for 4.9 GHz licenses. For additional information, refer to Industry Canada regulations.

11.2.3 Regulatory Requirement for CEPT Member States (www.cept.org)

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

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

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

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

- France – Outdoor operation at 100mW is only permitted in the frequency band 2400 to 2454 MHz;
  - Any outdoor operation in the band 2454 to 2483.5MHz shall not exceed 10mW (10dBm);
  - Indoor operation at 100mW (20dBm) is permitted across the band 2400 to 2483.5 MHz
    - 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 are categorized as "Class 2" devices

within the EU and are marked with the class identifier symbol   ⚠ , denoting that national restrictions apply (for example, France). The French restriction in the 2.4 GHz band will be removed in 2011.

This 2.4 GHz equipment is "CE" marked 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://motorola.wirelessbroadbandsupport.com/doc.php.

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

Motorola Canopy Radio equipment operating in the 5470 to 5725 MHz band are categorized as "Class 1" devices within the EU in accordance with ECC DEC(04)08 and are "CE" marked $C\epsilon$ to show compliance with the European Radio & Telecommunications Terminal Equipment (R&TTE) directive 1999/5/EC. The relevant Declaration of Conformity can be found at http://motorola.wirelessbroadbandsupport.com/doc.php.

A European Commission decision, implemented by Member States on 31 October 2005, makes the frequency band 5470-5725 MHz available in all EU Member States for wireless access systems. Under this decision, the designation of Canopy 5.4GHz products become "Class 1 devices" and these do not require notification under article 6, section 4 of the R&TTE Directive. Consequently, these 5.4GHz products are only marked with the $C\epsilon$ 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

11.2.4 European Union Notification for 5.7 and 5.8 GHz Product

The 5.7 and 5.8 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 $C\epsilon$ to show compliance with the European R&TTE directive 1999/5/EC.

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

11.2.5 Equipment Disposal

Waste (Disposal) of Electronic and Electric Equipment

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

11.2.6 EU Declaration of Conformity for RoHS Compliance

Motorola hereby, declares that these Motorola products are in compliance with the essential requirements and other relevant provisions of Directive 2002/95/EC, Restriction of the use of certain Hazardous Substances (RoHS) in electrical and electronic equipment.

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

11.2.7 UK Notification

The 5.7 and 5.8 GHz connectorized product has been notified for operation in the UK, and when operated in accordance with instructions for use it is compliant with UK Interface Requirement IR2007. For UK use, installations must conform to the requirements of IR2007 in terms of EIRP spectral density against elevation profile above the local horizon in order to protect Fixed Satellite Services. The frequency range 5795-5815 MHz is assigned to Road Transport & Traffic Telematics (RTTT) in the U.K. and shall not be used by FWA systems in order to protect RTTT devices. UK licensing specifies that radiolocation services shall be protected by a Dynamic Frequency Selection (DFS) mechanism to prevent co-channel operation in the presence of radar signals.

11.2.8 Belgium Notification

Belgium national restrictions in the 2.4 GHz band include

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

11.2.9 Luxembourg Notification

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

11.2.10 Czech Republic Notification

2.4 GHz products can be operated in accordance with the Czech General License No. GL-12/R/2000. 5.4 GHz products can be operated in accordance with the Czech General License No. GL-30/R/2000.

11.2.11 Norway Notification

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

Canopy 5.7 and 5.8 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 and 5.8 GHz connectorized products).

11.2.12 Brazil Notification

Local regulations do not allow the use of 900 MHz, 2.4 GHz, or 5.2 GHz Canopy modules in Brazil.

For compliant operation of an AP in the 5.8 GHz band, the Equivalent Isotropic Radiated Power from the built-in patch antenna and any associated reflector dish or LENS shall not exceed 36 dBm (4 W). When using the passive reflector (18 dB), transmitter output power must be configured no higher than 11 dBm. When using the LENS (10 dB at 5.8 GHz), transmitter output power must be configured no higher than 19 dBm.

For compliant operation in the 5.4 GHz band, the Equivalent Isotropic Radiated Power from the built-in patch antenna and any associated reflector dish or LENS shall not exceed 30 dBm (1 W). When using the passive reflector (18 dB), transmitter output power must be configured no higher than 5 dBm. When using the LENS (9 dB at 5.4 GHz), transmitter output power must be configured no higher than 14 dBm. When not using the passive reflector or the LENS, the transmitter output power of the radio must be configured no higher than 23 dBm.

The operator is responsible for enabling the DFS feature on any Canopy 5.4 GHz radio by setting the Region Code to "Brazil", including after the module is reset to factory defaults.

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

11.2.13 Australia Notification

900 MHz modules must be set to transmit and receive only on center channels of 920, 922, or 923 MHz so as to stay within the ACMA approved band of 915 MHz to 928 MHz for the class license and not interfere with other approved users.

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

11.2.14 Labeling and Disclosure Table for China

The People's Republic of China requires that Motorola's products comply with China Management Methods (CMM) environmental regulations. (China Management Methods refers to the regulation *Management Methods for Controlling Pollution by Electronic Information Products*.) Two items are used to demonstrate compliance; the label and the disclosure table.

The label is placed in a customer visible position on the product.

- Logo 1 means that the product contains no substances in excess of the maximum concentration value for materials identified in the China Management Methods regulation.
- Logo 2 means that the product may contain substances in excess of the maximum concentration value for materials identified in the China Management Methods regulation, and has an Environmental Friendly Use Period (EFUP) in years, fifty years in the example shown.

Logo 1   Logo 2

The Environmental Friendly Use Period (EFUP) is the period (in years) during which the Toxic and Hazardous Substances (T&HS) contained in the Electronic Information Product (EIP) will not leak or mutate causing environmental pollution or bodily injury from the use of the EIP. The EFUP indicated by the Logo 2 label applies to a product and all its parts. Certain field-replaceable parts, such as battery modules, can have a different EFUP and are marked separately.

The Disclosure table is intended to communicate compliance with only China requirements; it is not intended to communicate compliance with EU RoHS or any other environmental requirements.

Table 16: China disclosure table

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件	✕	○	✕	✕	○	○
电路模块	✕	○	✕	✕	○	○
电缆及电缆组件	✕	○	✕	✕	○	○
塑料和聚合物部件	○	○	○	○	○	✕
○： 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T11363-2006 标准规定的限量要求以下。						

✕ ： 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T11363-2006
标准规定的限量要求。

11.3   RF EXPOSURE SEPARATION DISTANCES

To protect from overexposure to RF energy, install Canopy radios so as to provide and maintain the minimum separation distances from all persons shown in Table 17.

Table 17: Exposure separation distances

Module Type	Separation Distance from Persons
Canopy Module (FSK or OFDM)	At least 20 cm (approx 8 in)
Canopy Module with Reflector Dish	At least 1.5 m (approx 5 ft)
Canopy Module with LENS	At least 50 cm (approx 20 in)
AP Antenna of connectorized module or integrated 900 MHz module	At least 80 cm (32 in)
Indoor 900 MHz SM	At least 10 cm (4 in)

The following section and its Table 18 provide details and discussion of the associated calculations.

11.3.1 Details of Exposure Separation Distances Calculations and Power Compliance Margins

Limits and guidelines for RF exposure come from:

- US FCC limits for the general population. See the FCC web site at http://www.fcc.gov, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See the Health Canada web site at http://www.hc-sc.gc.ca/rpb and Safety Code 6.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at http://www.icnirp.de/ and *Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields*.

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

- 10 W/m^2 for RF energy in the 5.7/5.8-GHz frequency bands.

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

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

where
S = power density in W/m^2
P = RMS transmit power capability of the radio, in W
G = total Tx gain as a factor, converted from dB
d = distance from point source, in m

Rearranging terms to solve for distance yields
$$d = \sqrt{\frac{P \cdot G}{4\pi S}}$$

Table 18 shows calculated minimum separation distances d, recommended distances and resulting power compliance margins for each frequency band and antenna combination.

Table 18: Calculated exposure distances and power compliance margins

Band	Antenna	Variable			d (calcu-lated)	Recom-mended Separation Distance	Power Compliance Margin
		P	**G**	**S**			
900 MHz FSK	integrated	0.25 W (24 dBm)	15.8 (12 dB)	6 W/m^2	23 cm	80 cm (32 in)	12
	external Yagi	0.063 W (18 dBm)	50.1 (17 dB)	6 W/m^2	20 cm	80 cm (32 in)	15
	external flat panel	0.39 W (26 dBm)	10.0 (10 dB)	6 W/m^2	23 cm	80 cm (32 in)	12
	indoor, integrated	Simulation model used to estimate Specific Absorption Rate (SAR) levels				10 cm (4 in)	2
2.4 GHz FSK	integrated	0.34 W (25 dBm)	6.3 (8 dB)	10 W/m^2	13 cm	20 cm (8 in)	2.3
	integrated plus reflector	0.34 W (25 dBm)	79.4 (19 dB)	10 W/m^2	46 cm	1.5 m (5 ft)	10
5.2 GHz FSK	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m^2	9 cm	1.5 m (5 ft)	279
	integrated plus LENS	0.025 W (14 dBm)	40 (16 dB)	10 W/m^2	9 cm	50 cm (12 in)	31
5.4 GHz FSK	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m^2	9 cm	1.5 m (5 ft)	279
	integrated plus LENS	0.020 W (13 dBm)	50 (17 dB)	10 W/m^2	9 cm	50 cm (12 in)	31
5.7 GHz FSK	Integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.2 W (23 dBm)	316 (25 dB)	10 W/m^2	71 cm	1.5 m (5 ft)	4.5
	Integrated plus LENS	0.2 W (23 dBm)	50 (17 dB)	1 W/m^2	28 cm	50 cm (20 in)	3.13

5.4 GHz OFDM	Integrated, 17 dBi	0.05 W (10 dBm)	50 (17 dB)	10 W/m^2	6 cm	20 cm (8 in)	10
	Connectorized, 17 dBi	0.05 W (10 dBm)	50 (17 dB)	10 W/m^2	6 cm	20 cm (8 in)	10
5.8 GHz OFDM	Integrated SM	0.05 W (10 dBm)	50 (10 dB)	10 W/m^2	6 cm	20 cm (8 in)	10
	Connectorized AP	0.063 W (17 dBm)	40 (16 dB)	10 W/m^2	14 cm	80 cm (32 in)	10
4.9 GHz OFDM	Integrated, 17 dBi	0.063 W (18 dBm)	40 (16 dB)	10 W/m^2	14 cm	20 cm (8 in)	2
	Connectorized, 17 dBi	0.063 W (18 dBm)	40 (16 dB)	10 W/m^2	14 cm	20 cm (8 in)	2

The Recommended Separation Distance is chosen to give significant compliance margin in all cases. It is also chosen so that a given item (bare module, reflector, or LENS) always has the same distance, regardless of frequency band, to simplify remembering and following exposure distances in the field.

These are conservative distances:

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

11.4   LEGAL NOTICES

11.4.1 Software License Terms and Conditions

ONLY OPEN THE PACKAGE, OR USE THE SOFTWARE AND RELATED PRODUCT IF YOU ACCEPT THE TERMS OF THIS LICENSE. BY BREAKING THE SEAL ON THIS DISK KIT / CDROM, OR IF YOU USE THE SOFTWARE OR RELATED PRODUCT, YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SOFTWARE OR RELATED PRODUCT; INSTEAD, RETURN THE SOFTWARE TO PLACE OF PURCHASE FOR A FULL REFUND. THE FOLLOWING AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR ENTITY), AND MOTOROLA, INC. (FOR ITSELF AND ITS LICENSORS). THE RIGHT TO USE THIS PRODUCT IS LICENSED ONLY ON THE CONDITION THAT YOU AGREE TO THE FOLLOWING TERMS.

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

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

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

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

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

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

THIS LIMITED WARRANTY IS THE ONLY WARRANTY PROVIDED BY MOTOROLA, AND MOTOROLA AND ITS LICENSORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS 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.

11.4.2 Hardware Warranty in US

Motorola US offers a warranty covering a period of 1 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.

11.5   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.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com