Digital Energy
MDS

PRODUCT RELEASE NOTE

RELEASE NOTE for: Mercury Firmware Version 3.6.3
RELEASE DATE: June 19, 2015

FIRMWARE

Phone +1 (585) 242-9600, FAX +1 (585) 242-9620, Web: www.gemds.com

MDS Mercury Firmware – Version 3.6.3

This document describes the software package for the Mercury Indoor Base Station, Indoor Subscriber, and Outdoor Subscriber.

Introduction

This next-generation of Mercury uses 802.16-2009 (802.16E) WiMAX technology which represents significant improvements in wireless networking by employing Scalable OFDM, MIMO, Hybrid ARQ, and Quality of Service.

The Mercury is a flexible, industrial wireless communication solution that is fully interoperable with the WiMAX and 802.16-2009 standards. It creates point-to-point and point-to-multipoint high-capacity wireless networks. The product is available as an Indoor Base Station, Indoor Subscriber (IDU), and Outdoor Subscriber (ODU). The products will provide user-experience throughput up to 30Mbps with data rate scaling automatically in order to trade off throughput versus distance, terrain, and interference.

Features

The Mercury family is designed to meet the demanding needs of today's wireless networks for SCADA, automation, and monitoring in industrial environments. It offers an array of features including:

- IEEE 802.16-2009 WiMAX interoperability
- Scalable OFDM with QPSK to 64QAM modulation
- Software configurable bandwidths 3.5MHz to 10MHz
- FCC/IC 3650MHz and IC 1800MHz band operation
- Web-based Device Manager, SNMPv3, and SSH
- Advanced security including EAP-TLS authentication and AES-CCM encryption: PKMv2 & PSK
- Quality of Service with support for WiMAX services types UGS, Best Effort , rtPS, ertPS, & nrtPS
- 2x2 MIMO operation employing Space Time Coding and Spatial Multiplexing on all units
- Dual SSID Wi-Fi with independent security and IP configuration, including VLANs
- Multiple-CA (tiered) PKI supported with manual or SCEP certificate management

Resolved Issues

The following issues are addressed in this release of software.

- Updated build to resolve the GHOST vulnerability.
- Modem upgraded to support pre-shared key (PSK) Device Auth Mode. As with any modem change, first power on will take up to three minutes to initialize.
- Stricter modem checking for PKM version and authorization policy during capabilities negotiation. This prevents association to rogue units claiming PKMv2 with no authorization policy.
- Increased the maximum frame length to 1800 bytes + 4 for the CRC.
- Modem initialization changed so the uplink modulation selected in SISO mode remains comparable to downlink.

- PIC changed continuous energy duration required to trigger an LBT event from 20 uS to 50 uS.
- Switch init/deinit modified so that we properly pass untagged frames OTA in VLAN native mode.
- Switch init/deinit modified so that toggling VLAN mode in trunk mode doesn't require a reboot.
- Kernel modified to properly handle being in VLAN access port mode.
- Generate new PSK key when Encryption Phrase is changed. If generation fails, log system error 'Max PSK Generate Attempts' in the event log.
- Only use TX/RX1 antenna port when in SISO mode on a Subscriber. **NOTE:** SISO subscribers connected to TX/RX2 antenna port may go off network once rebooted to 3.6.3. Ensure the proper connections or select a different MIMO Type before rebooting.
- Add cell ID & subchannel parameters to Base Station Radio Configuration, Frequency Control UIs.
- Add TDD Sync Mode "Prefer GPS" to allow operation when the GPS PPS signal is missing. For TDD Sync Modes Free Run and Prefer GPS, track out PPS offset frequency errors slowly to prevent losing Subscribers as they try to correct.
- Differentiate the uplink and downlink SNR/CINR on Base Stations.
- Changed event log processing to avoid a resource limit if the login times out with the log open.
- Increase the resource limit to provide enough room for full-log support bundles.
- Increase internal fragmentation threshold to allow larger RADIUS packets.
- Add SNMP support for read and clear of COM1 serial statistics to mercury_comm.mib.
- Remove trailing '.1' element from SNMP trap OID to match mercury_comm.mib.
- Append missing modulations to the rdbPerf*Modulation SNMP OIDs in mercury_ap.mib.
- SNMP queries of modemEthAddr now return the unit's MAC address.
- Change console menu and web UIs to require confirmation for password entries.
- Log the 'Obtained DHCP Address' event for Wi-Fi SSIDs, including the assigned address. All 'Obtained DHCP Address' event log entries should now include the assigned address.
- Update the route to the RADIUS server after a DHCP address is assigned.
- Poll RADIUS server when Subscriber associates. Log Parameter Changed event when RADIUS server changes.
- Changing a RADIUS server setting reverts to Server 1 and re-verifies the active server.
- RADIUS User Auth now has a 5-minute guard time at power on. When DHCP client is enabled and the unit has the default address, five minutes must elapse before the local fallback is used.
- Wi-Fi watchdog added. If triggered, log "Internal Error Wi-Fi restarted: unresponsive".
- Wi-Fi MAC addresses are now auto-generated if they have not been provisioned at the factory.
- Wi-Fi station 802.11 Status, Time Connected field is now populated regardless of Log 802.11 Events setting.
- Add WiMAX Frequency to Subscriber WiMAX Network Status UIs.
- Add Transmit Power and Connection Time to the console menu in order to match the web.
- Change Connection Date and Connection Time to display local time rather than UTC.
- Increase Support Bundle Filename length to 80 characters & include modem logs in the bundle.
- Correct web Performance, GPS Status panel form so JSON requests occur.
- Allow letter keys in multipage views like event log: (U)p, (D)own, Pg-U(p), Pg-D(n), (H)ome, (E)nd.
- Correct Frequency & 802.11 web panels so selective display functions work for 'operator' logins.

Known Errata

The following are known issues that exist in this release of the software.

- Subscribers with VLAN enabled and the Serial VLAN Subnet configured for Dynamic IP Address Mode may not show the DHCP-assigned address while either Wi-Fi VLAN ID matches the Serial VLAN ID. This is a display issue; the address is assigned to the bridge interface containing both the serial VLAN and Wi-Fi SSID.

- Subscribers configured as a Wi-Fi Access Point with privacy mode WPA Enterprise or WPA2 Enterprise will only use the RADIUS server that was active when Wi-Fi was enabled. Wi-Fi clients that try to authenticate after a RADIUS server switch will fail unless the original server returns to service. Disable/re-enable Wi-Fi or reboot the Subscriber to apply the updated RADIUS server configuration for new client authentications.
- Systems running Wireless Security Device Auth Mode PSK may lose link briefly every 70 days.
- Units using Wireless Security Device Auth Mode PSK that downgrade below release 3.5.0 won't associate, showing "Error" for Device Auth Mode. Change to a mode supported in the downgrade release before rebooting.
- Units using TDD Sync Mode Prefer GPS that downgrade below release 3.5.2 may not associate. Select a mode supported in the downgrade release before rebooting.
- Downgrading a unit below 3.6.0 may show a blank Base Location file on first boot. Reboot the unit once more after downgrading to recover the file contents.
- Radios operating on the 5800 FCC band must not use firmware versions below 3.0.6, as it is not compatible with newer 5800 units with higher power limits.
- In larger systems, over-the-air reprogramming sessions may timeout. If this occurs, increase the timeout parameter.
- MODBUS/TCP traffic may experience CRC corruption if the radio boots in serial data mode. Should this occur, disable the COM port and re-enable it to resolve.
- High Ethernet traffic rates of >30Mbps may result in undesirable system behavior.
- The web UI may allow more than 4 login attempts before disabling logins for five minutes.
- Base Stations may refuse to allow a Subscriber to associate after multiple failed ranging attempts. If this occurs, reboot the Base Station.
- A GPS antenna must be connected to the radio's GPS port before the radio is powered on. Attaching an antenna while the radio is powered will result in the unit requiring a reboot.
- Subscribers displaying Connection Status ABORTED for an extended period must be rebooted.
- In a large system of twenty or more Subscribers per Base Station, some Subscribers may take a long period to associate to the Base Station due to Service Flows establishing.
- Configuration scripts that are uploaded on the Subscriber, and that modify WiFi parameters, may result in incorrect IP settings being applied. This may be remedied by rebooting the affected Subscriber.
- WiFi service may stop while passing continuous MODBUS traffic and require a reboot to recover.
- WiFi while in VLAN operation may drop Clients intermittently.
- WiFi service may stop when WiFi parameters are changed on a radio operating as a WiFi access point while external clients are attempting to connect. This may also occur if the unit operates in WiFi ad hoc mode while external peers attempt to connect. Should this happen, reboot the radio.
- VLAN parameters changed through SNMP clients may not respond to a set request. Perform a subsequent get request to ensure that the parameter was set properly.
- An SNMP walk may not return all parameters.
- If a QoS filter entry is preceded by a blank entry, the QoS filter will not be applied.

Important Notice: Frequency Limits

The following radio frequency/agency options have wider frequency ranges in release 3.2.6 than they did in release 3.0.6:

- 1800 MHz
- 3650 MHz
    - IC-only agency
    - FCC/IC combined agencies
    - **NOTE:** The 3650 MHz FCC-only agency has *not* changed.

Refer to the tables below to determine the new minimum and maximum center frequencies that may be used in a system on these radios.

Bandwidth	1800 MHz Minimum Center Frequency	Maximum Center Frequency
3.5 MHz	1801.75 MHz	1828.25 MHz
5 MHz	1802.50 MHz	1827.50 MHz
7 MHz	1803.50 MHz	1826.50 MHz
10 MHz	1805.00 MHz	1825.00 MHz

Bandwidth	3650 MHz - IC Minimum Center Frequency	Maximum Center Frequency
3.5 MHz	3651.75 MHz	3698.25 MHz
5 MHz	3652.50 MHz	3697.50 MHz
7 MHz	3653.50 MHz	3696.50 MHz
10 MHz	3655.00 MHz	3695.00 MHz

Bandwidth	3650 MHz – FCC/IC Minimum Center Frequency	Maximum Center Frequency
3.5 MHz	3651.75 MHz	3698.25 MHz
5 MHz	3652.50 MHz	3697.50 MHz
7 MHz	3653.50 MHz	3696.50 MHz
10 MHz	3655.00 MHz	3695.00 MHz

The table below summarizes all available regulatory profiles.

Supported Regulatory Profiles							
		Normal Mode		DFS/Listen Before Talk Mode			
Value	Name	Start (MHz)	End (MHz)	Start (MHz)	End (MHz)	Max Tx (dBm)	Since
0	None	0	0	0	0	0	0.1.2
1	IC 1800MHz	1800	1830			30	0.3.5
2	FCC 3650MHz	3650	3675			30	0.1.2
3	IC 3650MHz	3650	3700			30	0.1.2
4	FCC 3650MHz ODU	3650	3675			23	0.3.2
5	IC 3650MHz ODU	3650	3700			23	0.3.2
6	IC 1800MHz ODU	1800	1830			30	0.3.1
7	Test 2500MHz	2500	2700			1	0.3.5
8	FCC 5800MHz	5725	5850			17	2.0.3
9	Test 900MHz	900	930			30	1.0.4
10	FCC 5800MHz ODU	5725	5850			18	2.0.3
11	Test 3300MHz	3300	3600			30	1.1.4

12	Test 3600MHz	3600	3900			30	1.1.4
13	Test 2300MHz	2300.25	2700			30	3.1.0
14	Test 5800MHz	5850	5875	5725	5850	23	3.2.4
15	Test 5800MHz ODU	5850	5875	5725	5850	18	3.2.4
16	Test 3300MHz ODU	3300	3600			30	2.0.0
17	ETSI 5800MHz	5850	5875	5725	5875	20	3.0.2
18	ETSI 5800MHz ODU	5850	5875	5725	5875	12	3.0.2
19	FCC 5800MHz V2	5725	5850			23	2.0.5
20	ACMA 3600MHz	3575	3700			30	2.0.6
21	ACMA 3600MHz ODU	3575	3700			23	2.0.6
22	FCC/IC 3650MHz	3650	3675	3650	3700	30	3.2.1
23	FCC/IC 3650MHz ODU	3650	3675	3650	3700	23	3.2.1
24	Whitespace LP	50	950			-10	3.2.7
25	Whitespace	50	950			30	3.2.7
26	IC 3500MHz	3475	3650			30	3.3.0
27	IC 3500MHz ODU	3475	3650			23	3.3.0
28	FCC 5400MHz	5470	5850			24	3.5.5
29	FCC 5400MHz ODU	5470	5850			24	3.5.5
30	ETSI 5400MHz	5470	5725			28	3.3.0
31	ETSI 5400MHz ODU	5470	5725			28	3.3.0