GE MDS *PRODUCT RELEASE NOTES Rev G*

**RELEASE NOTE For: MDS ORBIT MCR Firmware Version 1.6.2+**
**RELEASE DATE: July 02, 2014**

*FIRMWARE*

©2014 GE MDS LLC, 175 Science Parkway, Rochester, NY 14620 USA
Phone +1 (585) 242-9600, FAX +1 (585) 242-9620
http://www.gedigitalenergy.com/communications/wireless.htm

# *MDS™ORBIT MCR*

# *COVERING FIRMWARE – REV 1.6.2 AND GREATER*

## Overview

This section describes Software/Firmware updates for the MDS Orbit MCR platform.

Products: MDS Orbit MCR (including: MCR-4G, MCR-3G, MCR-900)
Firmware Version: 1.6.2
Release Date: 02-July-2014

## New Features

1. Priority based Quality of Service (QoS).
2. tcpdump diagnostic monitor tool (available to admin users at the CLI).
3. Initial setup web wizard.
4. MIB support for interface management.
5. Support for the RADIUS NAS Address and NAS Identifier attributes.
6. Check for expired certificates on startup to catch expirations that occur while the radio is not powered.

## Changes to Existing Features

1. DHCP server and interface IP dependency: Entering an IP address outside the range of the DHCP subnet will produce a warning and disable DHCP. Previously this operation resulted in failure.
2. Improved association of large NxRadio networks, such as on a reboot of the Access Point, by limiting the number of simultaneous connection requests being serviced at the same time.
3. Removed "Heartbleed" vulnerability (CVE-2014-016).
4. Improved single channel SAF performance.
5. LED behavior: when equipped with a 900MHz ISM module the corresponding NIC LED will behave as follows:
   - blink red while the radio module is initializing
   - display solid green on an Access Point when at least one Remote is connected
   - display solid red on an Access Point with no connected Remotes
   - blink red on a Remote with no link
6. Prevent disconnect of idle remotes.
7. TFTP blocksize defaults changed from 512 to 1024 bytes.
8. Requesting rollback to factory default: the new command line syntax is "request system recovery rollback snapshot Factory". Previously it was "request system recovery snapshots rollback identifier Factory".

## Defect Resolution

1. Removed the ability for users to configure RS485 mode on the COM2 or USB port, as it is only valid on COM1.
2. Orbit now gracefully handles a condition where an NxRadio Access Point tries to interact with a misconfigured EAP/PSK setup. To ensure proper operation in this scenario, firmware version 1.6.2 or higher should be installed on the Access Point and all Remotes.
3. Orbit now prevents a Wi-Fi Access Point and a Wi-Fi station referenced as members of the same bridge at the same time. This invalid configuration would prevent the device from properly booting up.
4. SNMP walk of Wi-Fi AP and client tables now behaves correctly
5. Creation of multiple IPSec tunnels w/ pre-shared-keys now behaves correctly.
6. IPSec configuration of DN and FQDN now behave correctly.
7. Operate properly as an IPSec responder.
8. The NxRadio connected-remotes database now properly displays remote IP addresses
9. Terminal Server configuration changes or session shutdown no longer generate an internal software error.
10. Fixed a failure to re-establish an NxRadio link after changing the security mode parameter.
11. Bridge priority is now properly applied on boot-up.
12. Fixed errors with the handling of the firewall address-range parameter.

## Known Errata

1. Serial Hardware Flow Control is not implemented. The ORBIT MCR (acting as the DCE) will not send data back to the PC (or DTE), unless the DTE continuously asserts the RTS line.
2. Wi-Fi interface interruptions may occur in the presence of high RF interference. If a service interruption occurs, the ORBIT MCR will detect and reset the Wi-Fi interface to restore service.
3. Changing the Wi-Fi configuration may cause station-bridge clients to stop passing data. A reboot is required to recover.
4. Changes made to an IPv4 interface (i.e., IP Address) may result in an Internal Software Alarm.
5. When a Commit is aborted by the ORBIT MCR, the device may misrepresent the current configuration. It is recommended to confirm the configuration is correct and re-commit.
6. Rebooting a Station Bridge may cause a service outage to other Wi-Fi connected devices.
7. When using Dual SSIDs, changes to ap-config parameters may cause the device to reboot upon commit.
8. Monitoring a disconnected interface may cause a *netmgr* failure. (See #20 under Operational Notes and Limitations)
9. Changing a Wi-Fi interface from an enabled Station with an IP address and filters to a disabled, bridged, Access Point without an IP address and filter may cause a *netmgr* failure
10. When a Wi-Fi Station is in the bridge, the STP status information for the Wi-Fi device is not available.
11. Attempting to perform a rollback to the factory snapshot in the WebUI will generate an application error. Perform the rollback from a CLI interface.
12. Using a NAS Identifier attribute in the RADIUS configuration selected to use with EAP device authentication on an NxRadio, will cause authentication failures due to the creation of a bad RADIUS packet.
13. Attempting to import a device certificate via the WebUI will cause an “Invalid params element name” error. Perform the request from a CLI interface.
14. Performing a restore to factory defaults in 1.6.2 will disallow connection via the HTTPS interface. Work-around is to use HTTP or avoid restore to factory defaults.

## Special Notes

## SNMP Configuration

To enable monitoring of interfaces via SNMP v1 or v2c, the user must update the default community ('public') configuration with the SNMP engine id generated by the device:

1. Obtain the engine id generated by the device as shown in the example:
   ```
   admin@(none) 19:53:58> show SNMP-FRAMEWORK-MIB
   SNMP-FRAMEWORK-MIB snmpEngine snmpEngineID 80:00:10:22:03:00:06:3d:06:ea:96
   ```

2. Update the engine-id configuration of the default community entry ('public'):
   ```
   admin@(none) 19:56:06% set SNMP-COMMUNITY-MIB snmpCommunityTable snmpCommunityEntry public
   snmpCommunityContextEngineID 80:00:10:22:03:00:06:3d:06:ea:96
   [ok][2013-07-31 19:56:20]

   [edit]
   admin@(none) 19:56:20% commit and-quit
   ```

## Operational Notes and Limitations

1. Internal software alarms cannot be cleared unless the ORBIT MCR is rebooted. (The Alarm *will* be in Event Log after reboot for record).
2. Configuring multiple Terminal Servers on the ***same*** TCP port does generate a warning, but operation will not work correctly.
3. DHCP Client operation can only be configured on one interface. Configuring it on multiple interfaces will cause unpredictable behavior.
4. Configuration of the station-max parameter, on the Wi-Fi interface, is not limited to 7 Stations, even though the ORBIT MCR currently supports 7 Stations.
5. When deleting an IPv4 address use the following sequence:
   ```
   % delete interfaces interface myInterface IPv4
   ```
6. The ORBIT MCR NTP service may not accept time from Windows W32Time Time service (SNTP).
7. Wi-Fi Station Bridging is not interoperable with other vendor's Wi-Fi devices.
8. When the Wi-Fi interface is enabled with Dual SSIDs, Station Bridging operation is restricted to the first alphanumeric SSID.
9. When using Dual SSIDs maximum throughput is achieved only on the first SSID; the second SSID will have reduced capacity (details are system dependent)
10. SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided.
11. On a Microsoft CA server, the SCEP template used should not include Extended Key Usage.
12. In WebUI, there are no preconfigured file servers. This facility is only accessible from the CLI.
13. In WebUI, when enabling a nested feature selection, the page must be refreshed.
14. The USB port is currently intended for console access only
    - Note: If the USB port is in use as a Terminal Server and the ORBIT MCR is rebooted (or connection interrupted) the USB cable must be disconnected and reconnected and the Terminal Session on the connected device must be restarted.
15. Any member of a disabled bridge will be disabled. Members must first be removed from the bridge in order to regain access to the interface.
16. A Wi-Fi Station will not age out in the event that its corresponding Wi-Fi Access Point is no longer present.
17. Date/Time settings on ORBIT MCR are expressed in GMT format.
18. SNMP: V3 is not currently supported; V2 requires special configuration as described below.
19. If the Cell interface is enabled through a configuration change, the ORBIT MCR must be rebooted.

20. Some CLI command sequences, particularly those involving device configuration or repeat status monitoring, may rarely cause an internal error known as a *netmgr* failure. The system will effect recovery, but to ensure proper operation a reboot is recommended.
21. In rare conditions DHCP may fail to provide IP addresses; in this case a manual reboot is required.
22. The "\" character is an escape character for the CLI. If you want to enter a "\" into a text field (such as a user password), you will need to use "\\".
23. Changes to the Wi-Fi interface mode may result in loss of data for several minutes.
24. STP is not functional over interfaces belonging to a VLAN.
25. Configuration files cannot be imported while there are any active WebUI sessions.
26. Tab completion is not available on the CLI when deleting list entries. The entry name must be manually entered using the name as displayed by the show command.
27. Not all certificate upload or download actions create proper events in the event log.
28. HTTPS currently support only the SSL 3 and TLS 1.0 protocols.
29. Displaying the active routes will not show all configured routes, when connectivity to an affected subnet cannot be established.
30. An internal software error may be logged while polling an active terminal server, even if the terminal server is working ok.
31. When changing a Wi-Fi Station to put it into a VLAN, you must reboot the device.
32. Attempts to request files from an SFTP server that cannot be reached may cause an internal error known as a *certmgr* failure. The system will affect recovery.
33. Attempting to perform simultaneous reprogramming operations on more than four NxRadio remotes, via the Over-the-Air link, may result in reprogramming failures. This will be more noticeable at lower modem modes.
34. The NxRadio connected-remotes database will not show an IP address if the Remote is configured to participate in VLANs.
35. Changes to RADIUS server configuration parameters on an interface using WPA/WPA2 Enterprise or EAP device authentication require an interface restart. This can be achieved either by a reboot of the device or by disabling and re-enabling the Wi-Fi and/or NxRadio interfaces that are configured to use the RADIUS server.
36. The configuration parameter to enable a specific Wi-Fi Access Point, overrides the higher level configuration to enable the Wi-Fi interface.
37. Long association times for Remotes may occur when an NxRadio Access Point interface is flooded with traffic.
38. QoS may not affect the Ethernet interfaces or bridging of Ethernet traffic between a Wi-Fi Access Point and a Wi-Fi Station in a bridge.
39. By default, the Serial Terminal Server modes will have a minimum 100ms delay between polls. To increase polling speeds adjust the VMIN and VTIME parameters in the Serial Port settings under the Services menu.
40. A bridged link between a Wi-Fi Access Point and a Station will only pass <1492 byte frames.
41. UDP Terminal Server Mode only supports Point to Point configuration. Multicast operation for serial point-to-multipoint is not currently supported.