



GE MDS *PRODUCT RELEASE NOTES Rev H*

RELEASE NOTE For: MDS ORBIT MCR Firmware Version 1.7.4+

RELEASE DATE: Aug 22, 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 1.7.4 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: 1.7.4

Release Date: 22-Aug-2014

Orbit™ MCR Learning and Development YouTube Channel



New Features

- 1. Serial Hardware Flow Control: User can configure the serial port to operate in DCE mode, CTSKey mode, or CTSKey Plus mode. ([See Appendix for steps Serial Hardware Flow Control](#))**
 - DCE mode configures the device serial port's CTS line to follow the RTS line from the DTE. A user can configure a delay to be applied. A straight through cable would be required.
 - CTSKey mode configures the DCE to emulate a DTE port. New parameters for CTS delay and hold times allow customization to the characteristics of the attached DCE. A crossover/null modem cable would be required.
 - CTSKey Plus mode behaves the same as the CTS Key mode, except that the port will stop transmitting in response to the attached DCE lowering its CTS line. A crossover/null modem cable would be required.
 1. When operating in CTSKEY mode, it is recommended that all respective serial ports be set at the same baud rate, and that VMIN and VTIME remain at the defaults for serial data packets less than or equal to 255 bytes. For serial packets over 255 bytes it is recommended that a cts-delay time of at least 90ms be used to account for the VTIME delay of the over-the-air sending unit.
- 2. UDP Multicast Terminal Server Support. ([See Appendix for steps: UDP Multicast](#))**
 - When using UDP Multipoint Terminal Server Mode, you must create a static route in the Orbit to direct how the Orbit handles the IP packets in the Multicast subnet. This static route must match the subnet for the Multicast IP address configured for your UDP Multipoint Terminal Server, and must also contain the outgoing interface of the Orbit that the packets must exit to reach the other Multipoint Terminal Server units.
3. Static NAT (1:1 NAT): To allow network to network NAT or single IP to IP NAT. A static rule-set can be applied to VPN connections and regular interfaces.
4. Enabled Windows 7/8 clients to setup IKEv2 with the device VPN server.
5. Enabled support for creating aliases in the Command Line Interface (CLI).

Changes to Existing Features

1. Enabled NAT for local tunnel subnets. Now the local tunnel subnet can be NATed to local LAN subnet. This provides a solution for cases where overlapping LAN subnets need to be connected via IPsec.
2. Enhanced VPN Connection firewall filter configuration. Now one can apply filters to a VPN connection similar to how they are applied to regular interfaces. This obviates the need to configure rules with "match ipsec" in filters with redundant configuration already specified in VPN setup.

Defect Resolution

1. Corrected issue that prevented static routes to multicast addresses from being applied to the system.
2. Corrected issue with requiring four plus characters ('++++') to break out of terminal server mode on a fresh boot.
3. Corrected issue with losing HTTPS access after restoring a unit to factory defaults. Note: HTTPS certificates will be recreated on first boot to new firmware.

Known Errata

1. 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.
2. Changing the Wi-Fi configuration may cause station-bridge clients to stop passing data. A reboot is required to recover.
3. Changes made to an IPv4 interface (i.e., IP Address) may result in an Internal Software Alarm.
4. 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.
5. Rebooting a Station Bridge may cause a service outage to other Wi-Fi connected devices.
6. When using Dual SSIDs, changes to ap-config parameters may cause the device to reboot upon commit.
7. Monitoring a disconnected interface may cause a *netmgr* failure. (See #22 under Operational Notes and Limitations)
8. 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
9. When a Wi-Fi Station is in the bridge, the STP status information for the Wi-Fi device is not available.
10. Attempting to perform a rollback to the factory snapshot in the WebUI will generate an application error. Perform the rollback from a CLI interface.
11. 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.
12. Attempting to import a device certificate via the WebUI will cause an "Invalid params element name" error. Perform the request from a CLI interface.
13. The DHCP Server may display that it is in an Error state if the DHCP serving interface is configured to multiple static IP addresses. In this state, the DHCP Server will not function.

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. When using an Orbit on both sides of an IPsec tunnel there is an IKEv1 issue. IKEv2 is recommended regardless of this IKEv1 limitation.
2. In the CLI, deleting a single entry in a leaf-list will delete the entire list. Do not use brackets in the command when deleting an element in the list.
3. Internal software alarms cannot be cleared unless the ORBIT MCR is rebooted. (The Alarm *will* be in Event Log after reboot for record).
4. Configuring multiple Terminal Servers on the *same* TCP port does generate a warning, but operation will not work correctly.
5. DHCP Client operation can only be configured on one interface. Configuring it on multiple interfaces will cause unpredictable behavior.
6. 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.
7. When deleting an IPv4 address use the following sequence:
 % delete interfaces interface *myInterface* IPv4
8. The ORBIT MCR NTP service may not accept time from Windows W32Time Time service (SNTP).
9. Wi-Fi Station Bridging is not interoperable with other vendor's Wi-Fi devices.
10. When the Wi-Fi interface is enabled with Dual SSIDs, Station Bridging operation is restricted to the first alphanumeric SSID.
11. When using Dual SSIDs maximum throughput is achieved only on the first SSID; the second SSID will have reduced capacity (details are system dependent)
12. SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided.
13. On a Microsoft CA server, the SCEP template used should not include Extended Key Usage.
14. In WebUI, there are no preconfigured file servers. This facility is only accessible from the CLI.
15. In WebUI, when enabling a nested feature selection, the page must be refreshed.
16. 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.
17. 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.
18. A Wi-Fi Station will not age out in the event that its corresponding Wi-Fi Access Point is no longer present.
19. Date/Time settings on ORBIT MCR are expressed in GMT format.
20. SNMP: V3 is not currently supported; V2 requires special configuration as described below.
21. If the Cell interface is enabled through a configuration change, the ORBIT MCR must be rebooted.
22. 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.
23. In rare conditions DHCP may fail to provide IP addresses; in this case a manual reboot is required.
24. 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 "\\ ".
25. Changes to the Wi-Fi interface mode may result in loss of data for several minutes.
26. STP is not functional over interfaces belonging to a VLAN.
27. Configuration files cannot be imported while there are any active WebUI sessions.
28. 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.
29. Not all certificate upload or download actions create proper events in the event log.
30. HTTPS currently support only the SSL 3 and TLS 1.0 protocols.
31. Displaying the active routes will not show all configured routes, when connectivity to an affected subnet cannot be established.
32. An internal software error may be logged while polling an active terminal server, even if the terminal server is

working ok.

33. When changing a Wi-Fi Station to put it into a VLAN, you must reboot the device.
34. 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.
35. 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.
36. The NxRadio connected-remotes database will not show an IP address if the Remote is configured to participate in VLANs.
37. 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.
38. The configuration parameter to enable a specific Wi-Fi Access Point, overrides the higher level configuration to enable the Wi-Fi interface.
39. Long association times for Remotes may occur when an NxRadio Access Point interface is flooded with traffic.
40. 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.
41. 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.
42. A bridged link between a Wi-Fi Access Point and a Station will only pass <1492 byte frames.

UDP Multicast:

When using UDP Multipoint Terminal Server Mode, you must create a static route in the Orbit to direct how the Orbit handles the IP packets in the Multicast subnet. This static route must match the subnet for the Multicast IP address configured for your UDP Multipoint Terminal Server, and must also contain the outgoing interface of the Orbit that the packets must exit to reach the other Multipoint Terminal Server units.

Outlined Configuration:

Orbit MCR: UDP Multipoint Terminal Server Mode

1. Configure an IPv4 Static-Route for the Multicast Subnet.
 - a. Configure Destination Prefix (dest-prefix)
 - b. Configure Outgoing Interface (outgoing-interface)
2. Configure Orbit Serial Terminal Server
 - a. Configure which Serial Port to use as Terminal Server
 - b. Configure UDP as Protocol
 - c. Configure UDP Mode to use, Point-to-Multipoint, Multipoint-to-Point, Multipoint-to-Multipoint
 - d. Configure remaining Terminal Server parameters, i.e. Local listening port, Remote port, Remote IP, Multicast port, Multicast IP
3. Save/Commit Configuration

Step by step walkthrough:

Web Based Configuration:

1. On the left hand side of your Web GUI, click Routing.
2. Click Static Routes -> ipv4 -> +Add ...
3. Type an ID, used to identify this route.
4. Enter the following: This destination prefix will cover the entire Multicast Subnet, and send all Multicast data out of your Bridge interface.

The screenshot shows a configuration form with the following fields and values:

- Description: [Empty] [Create]
- Outgoing Interface: Bridge [Dropdown arrow] [X]
- Dest Prefix *: 224.0.0.0/4
- Next Hop: [Empty] [Create]

5. Save your configuration.
6. Navigate back to the Routing page and verify your route is present:

Dest Prefix	Next Hop	Outgoing Interface	Source
0.0.0.0/0		Cell	kernel
10.15.64.0/26		Bridge	kernel
169.254.254.0/24		Bridge	kernel
224.0.0.0/4		Bridge	static
fe80::/64			kernel
fe80::/64			kernel

7. Step #7 & #8 are ONLY if the user has a Terminal Server already configured in their system. Otherwise proceed to Step #9
8. Then disable and re-enable your Terminal Server. This is done in Services/Serial/Terminal Server ... Click your Serial Port, uncheck the Enabled box and then Save.
9. Re-check the Enabled box and then Save.
10. Repeat this on each Multipoint unit.
11. Navigate to Services -> Serial -> Terminal Server -> Add ... then select the COM port to use as a Terminal Server, OK, then Create.

12. Click Mode -> Choices -> Udp -> Create -> Udp
13. Configure the UDP Mode that best fits your system, configure any local ports, remote ports/IPs, and Multicast ports/IPs.

The screenshot shows a configuration page for a UDP mode. At the top, the 'Mode' is set to 'Point To Multipoint'. Below this, there is a section for 'Local Ips' with two buttons: 'Add an entry ...' for 'Ipv 4 Ips' and 'Add an entry ...' for 'Ipv 6 Ips'. The 'Port' field is set to '30015', with a default of '30011' and a note that valid values are '0-65535'. The 'Multicast' section has three fields: 'Address' set to '224.100.0.5', 'Port' set to '30016' (default '30011'), and 'Ttl' set to '1'.

14. Save the Configuration

Command Line Interface (CLI) Configuration commands:

Note: Change **BOLDITALICS** to fit your system

1. Configure the following:
 - a. % set routing static-routes ipv4 route **1** dest-prefix 224.0.0.0/4 outgoing-interface **Bridge**
 - b. % set services serial terminal-server server **YOURPORT** mode udp mode **point-to-multipoint** port **30015** multicast port **30016** address **224.100.0.5**
 - i. This is an example.
 - c. % commit

Serial Hardware Flow Control

Hardware Flow Control: When operating in CTSKEY mode, it is recommended that all respective serial ports be set at the same baud rate, and that VMIN and VTIME remain at the defaults for serial data packets less than or equal to 255 bytes. For serial packets over 255 bytes it is recommended that a cts-delay time of at least 90ms be used to account for the VTIME delay of the over-the-air sending unit.

Hardware Flow Control Modes:

1. DCE
 - a. CTS follows RTS after a programmable “**CTS delay**”.
 - b. If the unit’s input buffer approaches a full condition it can deassert CTS regardless of state of RTS.
2. CTSKEY
 - a. Based on legacy MDS devices including TransNET, the device will act similar to a DTE but will provide signaling on the CTS line instead of the RTS line.
 - b. When the first character of a transmission is ready to be sent to the serial port, the unit shall assert CTS and delay for “**CTS delay**” time expiration before outputting the first character.
 - c. After the last character of a transmission is output from the serial port, the unit shall keep CTS asserted until the expiration of “**CTS hold**” time.
3. CTSKEYPLUS
 - a. The unit shall support flow control (Throttling) on the RTS pin. The device is expected to be wired via null modem to an external DCE device. The CTS line of the external DCE device drives the RTS line of the unit.

Outlined Configuration:

Orbit MCR: Hardware Flow Control

1. Configure Serial Port under test for Hardware Flow Control
 - a. Configure Hw Flow Control to true
 - b. Configure Hw Device Mode: DCE, CTSKEY, CTSKEYPLUS
 - c. Configure any remaining parameters, Cts Delay, Cts Hold, VMIN, VTIME
2. Save/Commit Configuration

Step by step Walkthrough:

Web Based Configuration

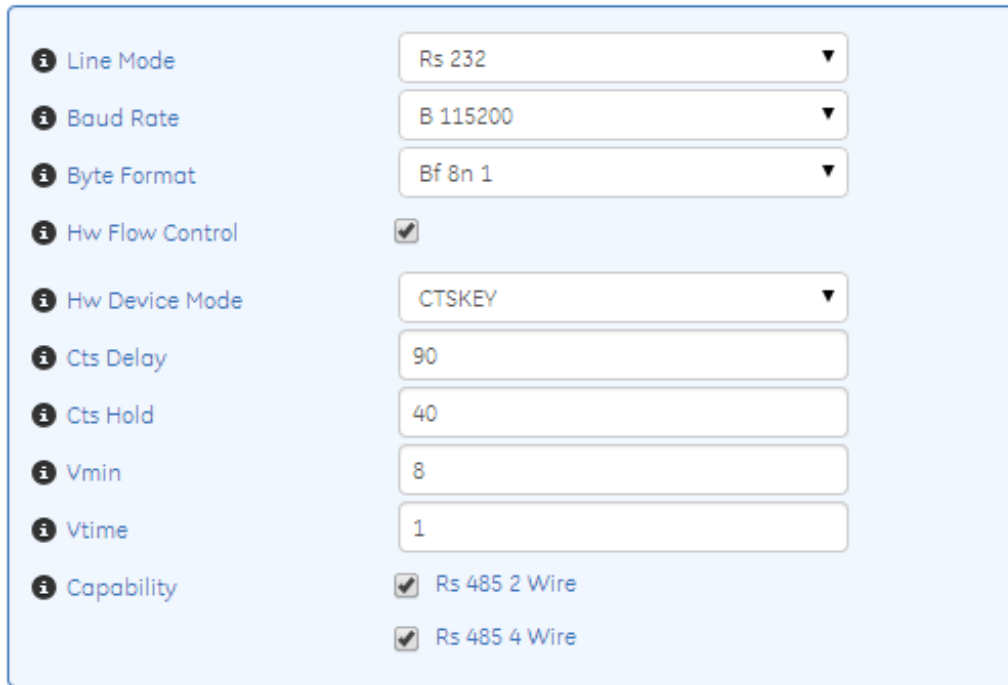
1. On the left hand side of the Web GUI, click Services.
2. Click Serial at the bottom of this page.
3. Click the Serial Port Name to configure Hardware Flow Control.

Name	Line Mode	Baud Rate	Byte Format	Hw Flow Control	Hw Device Mode	Cts Delay
COM1	rs232	b115200	bf8n1	true	CTSKEY	90
USB1	rs232	b115200	bf8n1	false	DCE	0

Showing 1 to 2 of 2

4. To enable Hardware Flow Control, click the Hw Flow Control checkbox.
5. Refresh the Web Page.

- Adjust the new parameters to fit the system, Hw Device Mode, Cts Delay, Cts Hold.



Line Mode	Rs 232
Baud Rate	B 115200
Byte Format	Bf 8n 1
Hw Flow Control	<input checked="" type="checkbox"/>
Hw Device Mode	CTSKEY
Cts Delay	90
Cts Hold	40
Vmin	8
Vtime	1
Capability	<input checked="" type="checkbox"/> Rs 485 2 Wire <input checked="" type="checkbox"/> Rs 485 4 Wire

- This is also where VMIN and VTIME can be adjusted.
- Save the Configuration.

CLI Configuration commands: Change ***BOLDITALICS*** to fit the system

- Configure the following:
 - % set services serial ports ***COM1*** hw-flow-control true hw-device-mode ***CTSKEY*** cts-delay ***90*** cts-hold ***40***
 - This is an example.
 - % commit