# GE MDS *PRODUCT RELEASE NOTE Rev D*

**RELEASE NOTE For: MDS ORBIT MCR-4G Firmware Version 1.1.7**
**RELEASE DATE: August 23, 2013**

*FIRMWARE*


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

# *GEMDS ORBIT MCR-4G FIRMWARE – FIRMWARE VERSION 1.1.7*

## Overview

This section describes Software/Firmware updates for the MDS Orbit MCR-4G product.

Products: GEMDS Orbit MCR-4G
Firmware Version: 1.1.7
Release Date: 23-AUG-2013

## Key Features

1. Verizon 4G LTE & 3G Cell connectivity
2. IEEE 802.11 b/g/n Access Point or Station
3. 10/100 BaseT Ethernet, with Auto-MDIX.
4. RS-232 and RS-485 (2-wire and 4-wire) Serial Terminal Server, with support for TCP Server, TCP Client, UDP unicast, and TCP/MODBUS conversion modes.
5. IPSec/VPN.
6. Firewall with Stateful Packet Inspection and NAT.
7. Secure Boot.
8. Secure Firmware Reprogramming
9. Management via Serial Console, USB Console, SSH Console, HTTP/HTTPS, SNMP, and NETCONF over SSH.

## Changes to Existing Features

1. Added Spanning Tree support.

## Defect Fixes

1. N/A.

**Known Errata**

1. Serial Hardware Flow Control is not implemented. The MCR-4G (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 MCR-4G 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. NIC LED behavior as described in the manual in Table 4 is incorrect. LEDs indicate connected status only.
5. Changes made to an IPv4 interface (i.e., IP Address) may result in an Internal Software Alarm.
6. In the event a Commit is aborted by the MCR-4G, the device may misrepresent the current configuration. It is recommended to confirm the configuration is correct and re-commit.
7. Rebooting a Station Bridge may cause a service outage to other Wi-Fi connected devices.
8. When using Dual SSIDs, changes to ap-config parameters may cause the unit to reboot upon commit.
9. Monitoring a disconnected interface may cause a netmgr failure. (See #25 under Operational Notes and Limitations)

**Operational Notes and Limitations**

1. Internal software alarms cannot be cleared unless the MCR-4G is rebooted. (Alarm will be in Event Log after reboot).
2. Configuring multiple Terminal Servers on the same TCP port does not 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. Wi-Fi configuration of the Station-Max parameter is not limited to 7 Stations, even though the MCR-4G currently supports 7 Stations.
5. When deleting an ipv4 address use the following sequence:

   % delete interfaces interface *myInterface* ipv4
6. The MCR-4G NTP service may not accept time from Windows W32Time Time service (SNTP).
7. TFTP transfers will not timeout if the connection to the TFTP server is lost. Since this is more likely on wireless interface, FTP or SFTP are recommended instead of TFTP when performing the operations over the Cell or Wi-Fi.
8. Wi-Fi Station Bridging is not interoperable with other vendor's Wi-Fi devices.
9. When Wi-Fi is enabled with Dual SSIDs, Station Bridging operation is restricted to the first alphanumeric SSID.
10. When using Dual SSIDs maximum throughput is achieved only on the first SSID; the second SSID will have reduced capacity (details are system dependent)
11. SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided.
12. The SCEP template used should not include Extended Key Usage.
13. In WebUI, there are no preconfigured file servers. This facility is only accessible from the CLI.
14. In WebUI, when enabling a nested feature selection, the page must be refreshed.
15. The USB port is currently intended for console access only
    - Note: If the USB port is in use as a Terminal Server and the MCR-4G is rebooted (or connection interrupted) the USB cable must be disconnected and reconnected and the Terminal Session on the connected device must be restarted.
16. When the MCR-4G is configured as IPSec Responder the current VPN status will show disconnected.
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 client will not age out in the event that its corresponding Wi-Fi AP is no longer present.

19. Cell may drop connection in the event packets are received on the Wi-Fi or LAN interfaces with source addresses outside their respective subnets. Proper Firewall Rule configuration of the MCR-4G is required to prevent this.
20. Date/Time settings on MCR-4G are expressed in GMT format.
21. VLAN limitation: MCR-4G does not support tagged traffic on the Wi-Fi interface.
22. SNMP: V3 is not supported in the initial release; V2 requires special configuration described below.
23. If the Cell interface is enabled through a configuration change, the MCR-4G must be rebooted.
24. Disabling and re-enabling a VLAN interface with an included Wi-Fi interface will cause station bridge units to stop passing data. A reboot is required to recover.
25. Some CLI command sequences, particularly those involving device configuration, 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.
26. In rare conditions DHCP may fail to provide IP addresses; in this case a manual reboot is required.

## 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 unit:

1. Obtain the engine id generated by the unit 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

### Firewall Rule for Cell Configuration

MCR-4G units shipped from the factory should include the following default firewall configuration:

```
% set services firewall address-set LOCAL-NETS addresses [ 192.168.1.0/24 ]
% set services firewall filter OUT_UNTRUSTED rule 1 match src-address address-set LOCAL-NETS
% set services firewall filter OUT_UNTRUSTED rule 1 match src-address add-interface-address true
% set services firewall filter OUT_UNTRUSTED rule 1 actions action accept
% set interfaces interface Cell filter output OUT_UNTRUSTED
```

These items ensure that only traffic originating on the local subnet is routed outward to the 4G cell interface.

NOTE: Earlier MCR-4G units may lack this configuration. If these rules are not included they should be manually added prior to using the cell interface.

**Firewall Rule for DNS Configuration**

MCR-4G units shipped from the factory should include the following default firewall configuration:

```
% set services firewall filter IN_UNTRUSTED rule 2 match protocol udp
% set services firewall filter IN_UNTRUSTED rule 2 match src-port services dns
% set services firewall filter IN_UNTRUSTED rule 2 actions action accept
```

IMPORTANT: Pings to the internet (using DNS names) will not function properly without this configuration.

NOTE: Earlier MCR-4G units may lack this configuration. If these rules are not included they should be manually added.