GE MDS *PRODUCT RELEASE NOTES Rev E*

RELEASE NOTE For: MDS ORBIT MCR Firmware Version 1.4.9+
RELEASE DATE: February 12, 2014

FIRMWARE

Phone +1 (585) 242-9600, FAX +1 (585) 242-9620
http://www.gedigitalenergy.com/communications/wireless.htm

MDS ™ORBIT MCR

COVERING FIRMWARE – REV149 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: 1.4.9
Release Date: 07-Feb-2014

Key Features

1. Verizon 4G LTE / 3G Cell connectivity
2. 3G GSM Cell connectivity (AT&T USA, Europe, etc.)
3. 900MHz Private Unlicensed connectivity
4. IEEE 802.11 b/g/n Access Point or Station
5. 10/100 Base-T Ethernet, with Auto-MDIX
6. 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
7. IPSec/VPN
8. Firewall with Stateful Packet Inspection and NAT
9. Secure Boot
10. Secure Firmware Reprogramming
11. Tamper Detection (Magnetometer)
12. Management via Serial Console, USB Console, SSH Console, HTTP/HTTPS, SNMP, and NETCONF over SSH

Changes to Existing Features

1. Added cellular connection profiles.
2. Added WebUI wizard for port forwarding.
3. Updated organization *of interface operational data* to reflect evolving industry standards.
   - Command syntax has changed from "show interfaces interface" to "show interfaces-state interface".
4. Updated *password change verification* to prevent username from being present in the password.
5. Added recovery log event to 4G support.

Defect Resolution

1. Resolved issue that caused WebUI lock-up if a validation error occurs during a commit.
2. Resolved issue with export of configuration files so that they can be properly re-imported at a later time.
3. Updated the WebUI to better support IE8.
4. Resolved cell issues with 4G IMEI handling, status monitoring when a SIM card is not present, and on-disconnect logging.
5. Changed to handle the deletion of network interfaces more gracefully, to prevent logging of errors.
6. Updated TFTP support to resolve timeout issues.
7. Resolved issue with NETCONF client connections not being released when the client disconnects, that would prevent new connections.
8. Allow RADIUS users with admin group privileges to change the local admin password.
9. Allow RADIUS users with tech group privileges to change the local tech password.
10. Added support to recover the cellular modem if the module becomes unresponsive.
11. Prevent reboot when committing VLAN settings on a device that has a Wi-Fi station configured and enabled.
12. Support recovery login with OTP on a disabled console when RADIUS user authentication is enabled.
13. Resolved FTP firmware reprogramming error where download reached 99% and failed to complete
14. Changed firewall to clear out existing connection information when changing the firewall from disabled to enabled, to make sure the firewall will break the data streams if it is configured to block them.
15. Resolved an issue in 4G cellular modem that could cause it to be stuck in idle mode.
16. Prevent reboot when attempting to delete the Cellular and Bridge interfaces from the factory default configuration.
17. Resolved issue that prevented Wi-Fi station bridging from being able to transmit traffic through the firewall when the Wi-Fi access point is in a VLAN.

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 unit to reboot upon commit.
8. Monitoring a disconnected interface may cause a netmgr failure. (See #22 under Operational Notes and Limitations)
9. Changing a WiFi device from an enabled station with an IP address and filters to a disabled, bridged, AP 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 in not available.

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

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. Wi-Fi configuration of the Station-Max parameter 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 Wi-Fi 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. When the ORBIT MCR is configured as IPSec Responder the current VPN status will show disconnected.
16. 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.
17. A Wi-Fi client will not age out in the event that its corresponding Wi-Fi AP is no longer present.
18. Date/Time settings on ORBIT MCR are expressed in GMT format.
19. VLAN limitation: ORBIT MCR does not support tagged traffic on the Wi-Fi interface.
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 in the Wi-Fi 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. The terminal server may log internal software errors when deleting the terminal server configuration.
30. Not all certificate upload or download actions create proper events in the event log.
31. Disabling the MCR-900 (NX915) Interface may cause the unit to reboot. If this occurs unit should recover without issue.
32. HTTPS currently support only the SSL 3 and TLS 1.0 protocols.