GE MDS *PRODUCT RELEASE NOTES Rev K*

RELEASE NOTE For: MDS ORBIT MCR Firmware Version 2.0.9+
RELEASE DATE: November 19, 2014

FIRMWARE

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

MDS™ Orbit MCR

COVERING FIRMWARE – REV 2.0.9 AND GREATER

NOTE: BEFORE UPGRADING MCR 3G UNITS, CONTACT TECH SERVICES AT 1-800-474-0964 (OPTION 3) AND/OR REVIEW SPECIAL NOTES SECTION BELOW.

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: 2.0.9
Release Date: 19-Nov-2014

Orbit™ MCR Learning and Development YouTube Channel

New Features

1. **Enhanced SNMP support**
   - SNMP V3 support
     - User Security Model (USM) - Ability to configure user authentication (md5 or sha1) and encryption (DES or AES).
     - View based Access Control (VACM) – Ability to configure VACM groups and views.
     - V3 Traps and Informs
   - New MIBs added (to enable PulseNET support)
     - MDS-SYSTEM-MIB.mib - GE MDS MIB for ORBIT system status.
     - MDS-SERVICES-MIB.mib – GE MDS MIB for ORBIT services status.
     - MDS-SERIAL-MIB.mib - GE MDS MIB for ORBIT terminal server status.
     - MDS-IF-NX-MIB.mib – GE MDS MIB for ORBIT NX915 interface status.

   NOTE: SNMP functionality allows only monitoring (and not configuration) of Orbit MCR.

2. **WebUI Configuration Wizards**

   The configuration wizards enable easier configuration of commonly used and/or advanced functionality of Orbit MCR. Following wizards have been added/updated:

   - **Initial Setup Wizard** – Walks the user through configuration of initial system settings – System Information, Password Configuration, Time and DNS setup.
   - **Basic Interface Setup Wizard** - Walks the user through configuration of basic settings for Bridge, Ethernet, Cell, Wi-Fi and NX Radio settings.
   - **VPN Setup** - Walks the user through configuration of IPsec VPN tunnels.
   - **Access Control List Setup (Filter)** - Walks the user through configuration of firewall filters and applying them to filter incoming and outgoing traffic on various interfaces.
   - **Port Forwarding (Destination NAT)** - Walks the user through configuration of destination NAT (a.k.a port forwarding) rule-sets to allow hosts on public network (e.g. Cell) to access services running on hosts in the private network (e.g. LAN).
   - **IP Masquerading (Source NAT**) – Walks the user through configuration of source NAT (a.k.a IP masquerading) rule-sets to enable multiple hosts on the private network (e.g. LAN) to communicate with a host on the public network (e.g. Cell).
   - **One-to-One (static) NAT** – Walks the user through configuration of one-to-one (a.k.a static NAT) rule-sets to enable a single host or an entire private network to be mapped into a publicly accessible address or a network respectively.

3. **Network Link Failover/Failback**

   The network link failover and failback functionality is provided by following features:

   - Route (Layer-3) Failover - The unit supports this feature by enabling configuration of multiple routes to same destination network with different preference (metric) values, enabling traffic to be sent using the route with high preference in normal scenario and failing back to the route with lower preference when the destination network is not reachable through the higher preference route.

   - Link (Layer-2) Failover - The unit supports this feature by creation of a bond interface in an active-backup mode that can aggregate a primary and secondary layer-2 link. When primary link is down, the secondary link is used to send layer-2 traffic etc.

   These features can be used to support NX Radio to Cell failover/failback to create high reliability network.

4. **IPsec VPN**

   Added following additional parameters to IKE peer configuration: initiator-mode (= 'on-demand' or 'always-on' (default)) and inactivity-timeout (applicable only if mode is on-demand). The ‘always-on’ mode implies the unit always attempts to keep the tunnel connected to the peer. The ‘on-demand’ mode implies that tunnel is setup only when traffic matching the IPsec local and remote network is sent and the tunnel is torn down in case no traffic flows for ‘inactivity-timeout’ interval. The ‘on-demand’ mode is useful when using NX Radio to Cell failover/failback setup, since IPsec tunnel is then established only when traffic fails over to Cell.

5. **GRE Tunnel Interface**

   GRE tunnel interface enables following use cases:

   - Tunneling of IP unicast/multicast (mode = ip-over-gre)
   - Tunneling of Ethernet traffic (mode = ethernet-over-gre) across an IP network (e.g. a Cellular network).
   - Provide a routed interface over IPsec to enable route failover from, say, a routed Ethernet or NX interface etc to GRE interface (over IPsec over Cell).

   Also, added a loopback interface type in order to enable GRE to work over IPsec. The loopback interface must be configured with an address from the local tunnel subnet.

6. **BOND Interface**

   A BOND interface bonds two layer-2 interfaces together and presents them as a single layer-2 interface to the rest of the system. Specifically, the BOND interface in active-backup mode enables redundancy between the

enslaved interfaces by activating the secondary member link when primary link goes down. The BOND interface enables following uses cases:

- High Reliability MCR AP to REMOTE Layer-2 network by using NX as the primary link and Cell as a secondary (backup) link.

7. Network Monitor (NETMON) service

Network monitor service allows the user to configure network monitor operations like interface-monitor or icmp-echo-monitor. These operations signal whether the operation state is up or down based on the state of the interface or periodic pinging of a remote host respectively. This signal can then be used by other applications to do interesting things. For example, routing uses the signal from interface-monitor or icmp-echo-monitor to add/remove routes that have been configured with verify-reachability check using that operation. This enables route failover/failback based on the state of the operation. Also, icmp-monitor-operation can also just be used to generate some periodic traffic towards a specific host.

8. New Cell Functionality

- A new modem option has been made available (configurator string = E4S and E42) to support LTE networks in EMEA region that supports following technologies/bands:
  - 4G LTE
    - Band 1 (2100 MHz)
    - Band 3 (1800 MHz)
    - Band 7 (2600 MHz)
    - Band 8 (900 MHz)
    - Band 20 (800 MHz)
  - 3G UMTS/HSPA+
    - Band 1 (2100 MHz)
    - Band 2 (1900 MHz)
    - Band 5 (850 MHz)
    - Band 6 (800 MHz)
    - Band 8 (900 MHz)
  - 2G GPRS/EDGE
    - GSM 850 (850 MHz)
    - EGSM 900 (900 MHz)
    - DCS 1800 (1800 MHz)
    - PCS 1900 (1900 MHz)

Changes to Existing Features

1. The VTIME resolution has been changed from "multiples of 0.1 seconds" to "milliseconds". The previous default was 1, meaning 100 ms. The default value has been changed to 100, meaning 100 ms. If the user has changed it to a specific value, then it would now be interpreted as milliseconds. This change enables faster polling of serial MODBUS devices.
2. Additional baud rate options of 300 and 230400 have been added to serial port configuration.
3. Removed the 'physical-interface' and 'virtual-type' configuration parameters for an interface and consolidated them into a single 'type' parameter. The interfaces names for physical interfaces must match pre-configured values (Cell, Wi-Fi, NxRadio, ETH1, ETH2).
4. The previously obsoleted 'station-bridge' Wi-Fi mode option has been removed. Any configuration still using this setting will be automatically migrated.
5. The use of cellular connection-profiles is now mandatory. Any old cellular configuration not using connection profile will be automatically migrated to use one.
6. Added request-dns and request-routers to dhcp client config on an interface.

   The request-dns (true|false) allows user to control whether DHCP client running on the interface requests and processes the DNS information received from the DHCP server over this interface.

   The request-routers (true|false) allows user to control whether DHCP client running on the interface requests and processes the default router information received from the DHCP server over this interface.

   These options now can be used to enable DHCP client operation (to obtain an IP address) on more than one interface. This removes one of the previous limitations. NOTE: Only one interface in the unit should have

request-dns or request-routers options set to true to ensure that system-wide DNS and default router are configured only from a single source.

7. Added configuration support to control RM-to-RM retransmission on the NxRadio interface.
8. IPsec IMA has been enhanced to be compatible with latest strongswan imv-scanner, imv-os and imv-attestation plugins by upgrading strongswan IPsec to 5.2.0. This also implies that IMA is not compatible with older version of strongswan IMVs (prior to 5.2.0).

Resolved Issues (Fixed)

1. DHCP Client operation to allow it to be configured on multiple interfaces.
2. Attempting to import a device certificate via the WebUI will cause an "Invalid params element name" error. Perform the request from a CLI interface.
3. In WebUI, when enabling a nested feature selection, the page must be refreshed.
4. In WebUI (HTTPS), SSL 3.0 support has been dropped to address the POODLE vulnerability (CVE-2014-3566). Also, added TLS 1.1 and TLS 1.2 support.
5. An internal software error may be logged while polling an active terminal server, even if the terminal server is working ok.
6. 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.
7. 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.
8. 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.

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. 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.
4. Rebooting a Station Bridge may cause a service outage to other Wi-Fi connected devices.
5. When using Dual SSIDs, changes to ap-config parameters may cause the device to reboot upon commit.
6. Monitoring a disconnected interface may cause a *netmgr* failure. (See #18 under Operational Notes and Limitations).
7. 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.
8. When a Wi-Fi Station is in the bridge, the STP status information for the Wi-Fi device is not available.
9. The "Local IPs" configuration parameter for Terminal Servers is not currently functional.
10. The Web GUI may unexpectedly logout when configuring the 'User Authentication Order'. Using the CLI is recommended in this instance.
11. Access Control List Wizard:
    - The 'Actions->log->Prefix' field in the filter rule within the Access Control List Wizard may create errors and unexpected configuration changes. It is recommended to not configure this parameter.
    - When using Windows IE8 the order of Rules do not display correctly
12. Destination NAT Wizard: The Destination NAT Wizard requires a 'Ruleset' named without spaces.
13. Initial Setup Wizard: The Initial Setup Wizard does not allow for the configuration of a Radius Server. It is recommended to configure these changes after the Wizard is complete.

Special Notes

1. **BEFORE UPGRADING MCR 3G units (that have default factory configuration for Cell interface), please configure a connection profile using instructions below. Once the connection profile is configured or if one already exists, then the firmware can be upgraded to this release.**

Using CLI (login as admin):

admin@(none) 23:27:06> configure
admin@(none) 23:27:06% set interfaces interface Cell cell-config connection-profile PROFILE-1
admin@(none) 23:27:06% commit

2. **This release features updated configuration data models that are not backwards compatible with older releases (pre 2.0.9). When a unit running an older release is upgraded to this release, a snapshot of its configuration will be made and stored on the unit. The unit's configuration will be automatically migrated to newer data model. The user will be allowed to downgrade to older firmware version only by choosing to go back to legacy configuration snapshot.**

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. 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.
6. To delete all IPv4 addresses from an interface use the following command:

   % delete interfaces interface *myInterface* IPv4
7. The ORBIT MCR NTP service may not accept time from Windows W32Time Time service (SNTP).
8. Wi-Fi Station Bridging is not interoperable with other vendor's Wi-Fi devices.
9. When the Wi-Fi interface 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. On a Microsoft CA server, 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. 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. 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.
19. In rare conditions DHCP may fail to provide IP addresses; in this case a manual reboot is required.
20. 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 "\\".

21. Changes to the Wi-Fi interface mode may result in loss of data for several minutes.
22. STP is not functional over interfaces belonging to a VLAN.
23. Configuration files cannot be imported while there are any active WebUI sessions.
24. 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.
25. Not all certificate upload or download actions create proper events in the event log.
26. Displaying the active routes will not show all configured routes, when connectivity to an affected subnet cannot be established.
27. When changing a Wi-Fi Station to put it into a VLAN, you must reboot the device.
28. 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.
29. The NxRadio connected-remotes database will not show an IP address if the Remote is configured to participate in VLANs.
30. The configuration parameter to enable a specific Wi-Fi Access Point, overrides the higher level configuration to enable the Wi-Fi interface.
31. Long association times for Remotes may occur when an NxRadio Access Point interface is flooded with traffic.
32. 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.
33. A bridged link between a Wi-Fi Access Point and a Station will only pass <1492 byte frames.
34. When using a Public Dynamic IP Addressed SIM card, On-Demand IPsec Mode is not supported. Always-On mode must be used instead.