RELEASE NOTE For: MDS ORBIT MCR/ECR Firmware Version 8.0.7 RELEASE DATE: July 31, 2020	*FIRMWARE*

MDS™ Orbit MCR/ECR

COVERING FIRMWARE – REV 8.0.7

Overview

This section describes Software/Firmware updates for the MDS Orbit MCR/ECR platform, noting changes since REV 7.6.5.

Products: MDS Orbit MCR/ECR

Firmware Version: 8.0.7

Starting with this version, the Orbit MCR/ECR Release Notes will begin including some items associated with Master Station (MPR) operation. Separate MPR notes will be maintained for now.

SPECIAL NOTICE FOR CUSTOMERS UPGRADING TO THIS VERSION (from pre-7.0)

As part of an enhanced security posture this release uses a SHA256 firmware certificate. When upgrading from earlier firmware versions (before 7.0.0) it is necessary to overwrite the previous GE MDS firmware certificate with this new one. Related information:

- The new certificate can be found at the GE Industrial Communications website at
  http://www.gegridsolutions.com/Communications/MDS/software.asp?directory=Orbit_MCR/Support_Items
- Certificates can be loaded individually (see Certificate Management, at the bottom of the navigation pane)
- Certificates can be broadcast to a network using remote management.

New Features

1. LN Profiles
   - Similar to "Cell Profiles" but applicable to the Orbit Licensed Narrowband family
   - Provides ability to automatically switch from one pre-programmed LN radio configuration to another based on connectivity timeouts
   - Programmed configurations can be as simple as new sets of RX/TX frequency (e.g., to provide a set of APs to hunt for) or more complex (e.g., changing the operating mode of the radio at remotes to accommodate future mode changes at the AP)

2. Redundant AP support
   - A collection of advanced features to support highly reliable operation with redundant APs.
   - Facility operates by extending existing Orbit features such as VRRP (Virtual Router Redundancy Protocol) and Netmon to work with GE MDS Proprietary radios (LN/NX/LW). Feature support works across MCR/ECR/MPRL
   - A new redundant AP Wizard provides step-by-step configuration of all key related components.
   - Configuration has provisions to ensure backhaul integrity to distinguish a broken link from a broken radio and prevent two units from both becoming active APs.

3. Support for L1C Licensed Narrowband hardware
   - L1C (135-156MHz), 12.5, 25.0, 50.0KHz channels
   - ETSI RED compliant / CE Marked

4. Support for L9A Licensed Narrowband hardware
   - L9A (800-870MHz), 12.5, 25.0, 50.0KHz channels
   - FCC and AUSTEST approved
   - For applications in the USA, this covers the 318 new ''interstitial'' 12.5KHz channels created in the 800MHz Mid-Band supporting public safety and other Private Land Mobile Radio (PLMR) users.

5. Support for 4GD Cell Module
   - 4G/3G/2G support (Target regions: Europe and Latin America)
     - LTE Bands: B1,B2,B3,B4,B5,B7,B8,B12,B13,B18,B19,B20,B25,B26,B28,B38,B39,B40,B41
     - WCDMA (3G) Bands: B1,B2,B4,B5,B6,B8,B19
     - 2G Bands: GSM 850, EGSM 900, DCS 1800, DCS 1900
   - GCF certified

6. NETMON enhancements
   - Added new "logic-monitor" operation, which allows user to create a logical expression composed of other NETMON operations using following operators: AND, and, OR, or, NOT, not, &&, ||, !.
   - Added new "radio-monitor" operation, which monitors/tests the health of an LN/NX/LW radio interface.

7. TACACS+
   - Cisco protocol for User Authentication and Authorization.

8. DHCP Server enhancements
   - Static DHCP client address assignments are now supported. List entries are specified by "client ID"/MAC address bound to IP address.

Changes to Existing Features

1. Multiple Web GUI enhancements have been implemented to improve user experience.

2. In 7.6.5 and later releases (except 7.7.0, 7.8.0), the clear-apn parameter under /interfaces/interface{Cell}/cell-config/connection-profile{PROFILE-1}/bearer-config has no effect. If the bearer-config/apn is not set, then the APN is cleared from the modem (only when running non-verizon carrier image) and the device will send LTE attach to the network with no APN included, which allows the network to activate default bearer on the APN associated with the SIM profile in the EPC. When the bearer-config/apn is set, then the device will send LTE

attach to the network with the configured APN included. Also, bearer-config/ip protocol parameter is now always configured in the modem. In prior releases, one either needs to set bearer-config/clear-apn to true or set bearer-config/apn in order for bearer-config/ip parameter to take effect.

3. In 7.6.5 and later releases, when IPv4 MTU is NOT configured explicitly by the user, the IPv4 MTU provided by the cellular network (during LTE attach) is configured on the cellular interface. This is the expected behavior for cellular devices and ensures that traffic sent to the network from the device conforms to the MTU value expected by the network.

4. In 7.6.5 and later releases, when GPS is enabled or disabled the Cell modem is restarted. This will cause the Cell link to be disconnected for few minutes.

Resolved Issues (Fixed)

1. Resolved issue with wrong options displayed on Advanced Config tab after changing device from Basic Config.
2. Passthrough configuration can now be removed in Basic web mode
3. Over-the-air reprogramming properly shows 100% complete through LN SAF units. This previously never showed 100% completion.
4. SNMP could previously use up all available login sessions. SNMP, WebUI, CLI and Netconf are now all properly limited to 5 sessions each.
5. Fixed an issue with DMVPN where IPsec transport mode SA went down and, in a rare event, was not detected and re-established by NHRP service.
6. Fixed an issue with BGP Neighbor netmon signal that was non-functional since 7.5.6

Special Notes

1. IMPORTANT COMPATIBILITY NOTICES
   - For legacy systems running Orbit LN in backward compatible packet-with-mac mode, running with ethernet data and using DLINK diagnostics (i.e., with PulseNET), version 8.0.7 is not recommended. A scenario is possible where data remains stalled at the remote for up to 10 seconds. This will result in degraded performance. This problem can be alleviated by eliminating or highly reducing DLINK traffic. The problem does not manifest in serial-only systems.
   - For systems running in Advanced-Polling mode, it is critical to update the AP to version 8.0.7 or higher, prior to running any remotes with version 8.0.7.

2. Reverting to earlier configurations
   - Orbit software releases include updated configuration data models that are not backwards compatible with older releases. When a unit running an older release is upgraded to this release, a snapshot of its configuration is made and stored on the unit. The unit's configuration is automatically migrated to newer data model. The user can downgrade back to the older firmware version only by choosing to revert to the legacy configuration snapshot.

3. Firewall Robustness
   - The Orbit Firewall is a powerful tool for restricting unintended traffic. As a protective measure, if the Orbit Firewall ever experiences an unexpected error, all traffic is dropped with the exception of HTTPS and SSH protocols. These protocols can be used to recover the device to a functional state.

1. Updating the firmware via web interface using a local file may fail and get into a bad state. The device will function properly, but updating firmware will fail until the device is rebooted.
2. The standard Wi-Fi (W51) may experience interruptions 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. When a Commit is aborted the device may misrepresent the current configuration. It is recommended to confirm the configuration is correct and re-commit.
4. Rebooting a device functioning as a WiFi Station Bridge may cause a service outage to other WiFi connected devices. The other WiFi devices will resume connections on their own after a short time. (approx. 30 seconds)
5. Showing status on a disconnected interface may cause a netmgr failure. This internal failure will be logged as an event and the device will recover on its own.
6. Changing a WiFi 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. This internal failure will be logged as an event and the device will recover on its own.
7. When a WiFi Station is in the bridge, the STP status information for the WiFi device is not available.
8. Attempting to send invalid firmware over broadcast reprogramming may cause a services manager failure.
9. In some cases, changes to the GRE interface configuration (VPN) will require a reboot to take effect. It is good practice to reboot the device after making changes to the VPN configuration.
10. In some cases, changes to IPSec configurations (VPN) will require a reboot to take effect. It is good practice to reboot the device after making changes to the VPN configuration.
11. Setting peer-endpoint to any in DMVPN will cause all traffic on all interfaces attempt to use the VPN.
12. When doing 802.1x port authentication, If the radius server is not reachable when the Ethernet cable is inserted, then it may need to be reinserted to reinitiate authentication.
13. VLAN priority is not preserved if passed from one VLAN trunk to another.
14. With multiple RADIUS servers configured for user authentication and none are reachable, it is possible that it will take a long time for the fallback authentication (if enabled) to be evaluated as each RADIUS server communication times out.
15. There may be occasions where alerts are erroneously displayed on the web interface.
16. When using RADIUS user authentication with multiple servers, incorrect routes will cause authentication to fail.
17. When in the IPsec Connections window and creating a new connection, the Remote Virtual Address field does not show up after selecting the host-to-net option. You must navigate away, then back for it to show up.
18. If there are more than 50 routes in a radio's routing table, the routes will not be correctly displayed via the CLI.
19. Carefully review the summary of changes at the end of the firewall wizard to ensure all the changes are expected.
20. When making changes to QOS settings, changes will not occur after committing if traffic flow is already in progress. Reset the interface (or reboot the device) to ensure that changes will be in effect.
21. Entering control-C during ping may cause the display of overall ping statistics to be suppressed.
22. For Orbit LN using 7FSK modems, operation with a repeater is not recommended.
23. In rare cases, allowing a confirmed commit to timeout (i.e. no user confirm) and rollback the configuration may cause the device to reboot. After the device reboots, it will be running the previous configuration.
24. Instead of prioritizing on the DSCP field, it is recommended to prioritize with the TOS equivalent.
25. When using the Web interface, custom table columns will only be preserved with the tables refresh button. All other page refreshes will reset the columns to the default settings. For example, Connected Remotes Table on an NX AP or LN AP web interface.
26. If using mirrored bits protocol on an NX network, it is recommended that you use a version 7.1.1 or earlier.
27. Operation as a Store-and-Forward device is not recommended in 7 level FSK modems. Operation with system ID is not recommended with 7 level FSK modems.
28. If there is an issue exporting support bundle via web interface, please cancel via the CLI, and retry.
29. When changing terminal server modes and you experience an error committing, refresh and review the settings.

30. When configuring the Static Routes Next Hop parameter, leave the Outgoing Interface blank. Otherwise, the routing table will not be properly configured and data passing may stop.
31. Broadcast reprogramming of the firmware certificate may not correctly show the status at the broadcast sender.
32. Transporting Mirrored Bits (TM) protocol is only supported on NX interfaces.
33. The remote web proxy will not function if the device disables firmware push.
34. When doing broadcast reprogramming, it is recommended that you use an external file.
35. When doing requests on the CLI with many arguments, ensure that the nested arguments (ones with {}) are provided last.
36. It is recommended that if the user is using a LN radio in packet with mac mode with both Ethernet and DLINK/SDMS remote detection traffic that the radio run 7.1.1 or earlier.
37. Alarm threshold parameters "rssi-upper-threshold" and "rssi-lower-threshold" in the ln-config, nx-config, and lw-config had inverted meaning in earlier code.

    If you upgrade to this version then return back to an earlier version, values may need to be manually adjusted.
38. In the firewall wizard in the web interface, when adding a service to the rule click 'Add New Entry' first before selecting Add/Update option for each new entry.
39. While MDS Orbit supports management and routing via IPv6, not all services have support for IPv6.
40. The LNMS Retry Percentage alarm is non-functional.
41. On cellular units with 4Gx modem type, if GPS service is enabled and modem firmware is upgraded, this could result cellular interface being inoperable. Customer is advised to disable GPS before reprogramming the modem.
42. There may be issues managing a serial pass-through configuration in basic web mode if it was initially set up in advanced web or the CLI.
43. In the case that a web file transfer fails, it is possible that the user must start a cli session and issue a cancel for the transfer. Alternately the unit can be rebooted to resolve the incorrect state.
44. In firmware version 7.6.5 and above, when GPS is enabled or disabled the Cell modem is restarted. This will cause the Cell link to be disconnected for few minutes.
45. The command line interface command "tcpdump list" is not functional. It is recommended that the user uses netdump instead of tcpdump.

Operational Notes and Limitations

1. The Web UI rejects a password change with the backslash character if repeated two times in a row example: Y1 \ \ n%*". The CLI and SSH reject a password change with a single backslash character, example: Tech\123.

2. The HTTP Protocol is not supported for exporting files.

3. The Terminal Server may fail if polling with VMIN = 1. Disable then re-enable the Terminal Server to regain functionality.

4. Internet Explorer version 8 is no longer supported. Please upgrade this application to version 11, or use Mozilla Firefox, Google Chrome, or Microsoft Edge.

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

   % delete interfaces interface myInterface ipv4

6. Wi-Fi Station Bridging is not interoperable with other vendor's Wi-Fi devices.

7. When the Wi-Fi interface is enabled with Dual SSIDs, Station Bridging operation is restricted to the first alphanumeric SSID.

8. SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided.

9. On a Microsoft CA server, the SCEP template used should not include Extended Key Usage.

10. In WebUI, there are no preconfigured file servers. This facility is only accessible from the CLI.

11. 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 is rebooted (or connection interrupted) the USB cable must be disconnected and reconnected and the Terminal Session on the connected device must be restarted.

12. 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.

13. Date/Time settings on ORBIT MCR are expressed in GMT format.

14. 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.

15. The backslash 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 "\\".

16. STP is not functional over interfaces belonging to a VLAN.

17. Displaying the active routes will not show all configured routes, when connectivity to an affected subnet cannot be established.

18. When changing a Wi-Fi Access point to put it into a VLAN, you may need to reboot the device for traffic to flow over the Wi-Fi interface.

19. The configuration parameter to enable a specific Wi-Fi Access Point, overrides the higher level configuration to enable the Wi-Fi interface.

20. 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.

21. When using a Public Dynamic IP Addressed SIM card, On-Demand IPsec Mode is not supported. Always-On mode must be used instead.

22. When configuring custom layer-2 protocol filters use 0x as a prefix when entering the value as Hex, otherwise enter the decimal value. Example for ARP: Enter 0x0806 or 2054.

23. An Orbit Wi-Fi Access Point may not pass data to an Orbit Wi-Fi Station-Bridge [after configuration changes are committed]. To ensure proper operation a reboot is recommended.

24. On the web interface, when pop up lists are used, entries cannot be deleted. To delete an entry simply highlight the text in the box and delete the text.

25. COM port attributes (data bits, parity, stop bits) are only applicable to data mode. When operating in Console COM ports will only supports 8N1.

26. Re-authentication is not supported on an established 802.1X Port based session.

27. Syslog is not fully compliant with RFC5424.

28. At the conclusion of remote over-the-air broadcast reprogramming, the System Manager may restart.
29. Nx NICs may need be configured with dwell times above 30ms if running at 125kbps.
30. When NX is in store and forward mode, continuous downlink saturation may cause some nodes to be starved and not given upstream time.
31. In a LN system, if the modulation is forced to 64 QAM, it is recommended that FEC (forward error correction) is enabled.
32. If running a COM port at 300 baud it is recommended that vtime be set to greater than 35 ms.
33. Preconfigured servers are not applicable to broadcast reprogramming.
34. When using QoS, you cannot have a shaping policy as the next-policy of priority policy.
35. When importing a configuration file that contains references to certificates, first ensure those certificates are loaded onto the unit.
36. When operating Orbit LN in backward-compatible mode, degraded performance may sometimes occur in certain complex configurations that include MPRS.
37. If using the Orbit as a DHCPv6 server with IPv6 subnet constructed from the interface specified in constructor-interface parameter, one must specify the v6subnet prefix as ::/0.
38. Interfaces that user can name (bridges, vlans, etc.) should not have spaces in them.
39. To limit the possibility of a cell connected unit not being accessible after a factory reset, we explicitly no longer block HTTPs and SSH ports from being initiated from over the cell link. As a part of provisioning, these ports should be disabled by modifying the IN_UNTRUSTED rules if they are not required.
40. Station bridged WiFi clients behave differently from normal (i.e., non-bridged) clients. Station bridged clients can communicate directly to each other, while normal clients are isolated and IP traffic will not pass between them.
41. When configuring L7W (Licensed 700MHz Wide), do not set NIC-id. It is not supported in this release and will prevent link establishment.
42. In rare cases where an NX or LN access point does not associate new remotes, disabling and then reenabling the access point may resolve the issue.
43. A QoS modify policy is not tied to an interface and must be deleted to disable it.
44. When using an Orbit on both sides of an IPsec tunnel there is an IKEv1 issue. IKEv2 is recommended regardless of this IKEv1 issue.
45. If using terminal server in TCP polled mode, it must be configured with the serial ports vmin to be greater than the largest possible response in bytes.
46. If you are experiencing unexpected fragmentation of data on your LN virtual radio channel or transparent serial, try increasing the vmin and vtime on the virtual serial port.
47. Web proxy (if enabled) will attempt to work with older code revisions (prior to 6.6.x) using a fallback method. MCR code before 6.0.0 will not render at all. This is a best effort system and may not render the web accurately. Firmware update of the network is recommended.
48. For LN in transparent mode, if your over the air rate is greater than your serial port rate, it is recommended that you increase your SCD (soft carrier dekey) on x790 or data key hold time on your MPRS to at least 5 to eliminate potential gaps in the transmission.
49. The configured power for Wi-Fi radio may not be used, instead a lower caped value is used depending on regulatory constraints.
50. The broadcast reprogramming feature is meant to make minimal impact to the current operation of the network. As such the time for reprogramming is highly dependent on the throughput of the link and how much it is loaded.
51. Basic webui only supports units with an NX, LN, or LW radio (with an optional Wi-Fi module). Standalone Wi-Fi, Cell, and Cell with Wi-Fi are not currently supported.
52. Timeout of MODBUS transactions can cause dropped TCP connections. Workaround is to increase poll rate or increase transaction timeout.
53. When changing COM port usage from a terminal server to a passthrough it is recommended to remove a terminal server with a commit first and then create the passthrough instance on a separate commit.
54. In the CLI, deleting a single entry in a leaf-list with bracket notation will delete the entire list. Do not use brackets in the command when deleting an element in the list.

55. When running VRRP on a Bridge interface, it is recommended to disable STP (spanning tree protocol).

56. Transparent serial system using repeaters, may need to mute portions of the echo repeater response. If polling remote is MPRS use the rx-mute to at least 5. An LN polling remote use data-key-hold-timeout of at least 8.

57. When issuing a repeat command on the CLI, add the additional syntax "| nomore" (without quotes).

58. After modifying serial passthrough parameters (Simple Serial), you must wait 5 minutes for the unit to go into data mode.

59. MTU settings on the Cell interface have the following restrictions:

    -When IPv4 MTU is NOT configured explicitly by the user, the IPv4 MTU provided by the cellular network (during LTE attach) is configured on the cellular interface. This is the expected behaviour for cellular devices and ensures that traffic sent to the network from the device conforms to the MTU value expected by the network.

    - When IPv4 MTU is configured explicitly by the user AND the configured MTU is LOWER than currently active MTU value, then new IPv4 MTU value is applied to the celullar interface. NOTE: The user should never configure MTU value higher than one supported by the cellular network.

    - When IPv4 MTU is configured explicitly by the user AND the configured MTU is GREATER than currently active MTU value, then new IPv4 MTU value is NOT applied to the celullar interface. In this case, the user must disable and re-enable cellular interface.

60. In 7.6.5 and later releases (except 7.7.0, 7.8.0), the clear-apn parameter under /interfaces/interface{Cell}/cell-config/connection-profile{PROFILE-1}/bearer-config has no effect. If the bearer-config/apn is not set, then the APN is cleared from the modem (only when running non-verizon carrier image) and the device will send LTE attach to the network with no APN included, which allows the network to activate default bearer on the APN associated with the SIM profile in the EPC. When the bearer-config/apn is set, then the device will send LTE attach to the network with the configured APN included. Also, bearer-config/ip protocol parameter is now always configured in the modem. In prior releases, one either needs to set bearer-config/clear-apn to true or set bearer-config/apn in order for bearer-config/ip parameter to take effect.