GE MDS *BETA PRODUCT RELEASE NOTES - v6.1.6*

RELEASE NOTE For: MDS ORBIT MCR/ECR Firmware Version 6.1.6
RELEASE DATE: November 9, 2017

FIRMWARE

MDS™ Orbit MCR/ECR

COVERING BETA FIRMWARE – REV 6.1.6

Overview

This section describes Beta Software/Firmware updates for the MDS Orbit MCR/ECR platform, noting changes since REV 6.1.5.

Products: MDS Orbit MCR/ECR

Firmware Version: 6.1.6

Orbit™ Learning and Development YouTube Channel

Beta Software

GE offers Beta firmware to our customers as a convenience to allow early testing and deployment of new features and issue resolutions prior to standard Production Release. Beta firmware is selectively distributed on request to customers who acknowledge that the firmware has not yet been fully tested to Production Release standards.

Please contact Technical Services during business hours (8:30 AM to 6:00 PM Eastern Time) if you would like access to Beta firmware. Contact us using any of the methods below:

Telephone: (800) 474-0964 Option #3

E-mail: gemds.techsupport@ge.com

Web: www.gemds.com

FAX: (585) 242-8369

Important Notes

1. The configuration exported from a unit running 6.x.x release should not be imported into a unit running any prior release
2. CAUTION: Do not load this code into an Orbit AP NxRadio running Security Protocol 1.0. (See information below, under Changes to Existing Features)

Resolved Issues (Fixed)

1. Unlicensed 900MHz (NxRadio): Inability to set Avoided Frequencies.
   - This was broken in 6.1.2. It is restored in 6.1.5.
   - This fix only requires the AP to be updated. Remotes will follow the AP's settings.
2. Security: KRACK vulnerability
   - Resolved
3. VPN Wizard defects
   - Using the wizard to delete an Ethernet/GRE VPN connection, now works properly
   - DMVPN NBMA – now properly supports Domain Name
   - Bridge/Bond interface is now properly displayed for L2 GRE
4. Cell Operation: "IP passthrough" not working with firewall enabled
   - Resolved in 6.1.6
5. Cell Operation: Point-to-Multipoint over IP/GRE over DMVPN was not working
   - Resolved in 6.1.6

New Features

1. N/A

Changes to Existing Features

1. Unlicensed 900MHz (NxRadio) – incompatibility with some AP units
   - Code version 6.1.6 is incompatible with very early Orbit AP radios running Security Protocol 1.0. Orbit NxRadio AP's using Security Protocol 2.0 are unaffected. Use of Security Protocol 1.0 with AES encryption in 6.1.6 will prevent data from passing and may cause the unit to experience a kernel panic" error. If this code is accidentally loaded, effect recovery by restoring the code and database snapshot. Please Contact Technical Services for assistance.

The remainder of this note includes the material from Production Release 6.1.2 and Beta Release 6.1.5

MDS™ Orbit MCR/ECR

COVERING BETA FIRMWARE – REV 6.1.5

Overview

This section describes Beta Software/Firmware updates for the MDS Orbit MCR/ECR platform, noting changes since REV 6.1.2.

Products: MDS Orbit MCR/ECR

Firmware Version: 6.1.5

Orbit™ Learning and Development YouTube Channel

Resolved Issues (Fixed)

1. Start-up condition on firewall & network address translation
   - Fixed an issue with a specific setup where source address translation worked on initial configuration but did not work after unit was rebooted.
   - All traffic reaching Orbit is now processed after the unit has booted completely.
2. Spectrum Analyzer for unlicensed 900MHz
   - Spectrum Analyzer functionality was broken in 6.1.2. It is restored in 6.1.5
3. VPN connectivity robustness
   - Fixed an issue where VPN connectivity was not restored following an internal system fault.
4. "show log" facility
   - "show log" functionality was broken in 6.1.2. It is restored in 6.1.5
5. WiFi AP reboot on attempted connection to 6th station bridge client
   - AP now properly handles connection to >5 station bridge clients
6. Remote Management Reboot – undesirable behavior
   - "Remote Reboot" now properly ONLY reboots remotes and not the AP.

New Features

1. N/A

Changes to Existing Features

1. Firewall IN_UNTRUSTED factory default
   - The Factory default for the IN_UNTRUSTED firewall filter now allows connection by ssh, https, and Netconf. In the event of a revert to factory default, this change facilitates basic connection to an Orbit equipped with cell, without mandating a site visit. The Web UI start-up screen has been modified to alert users to change the default to create a more secure configuration.

MDS™ Orbit MCR/ECR

COVERING FIRMWARE – REV 6.1.2

Overview

This section describes Software/Firmware updates for the MDS Orbit MCR/ECR platform, noting changes since REV 4.6.8.

Products: MDS Orbit MCR/ECR

Firmware Version: 6.1.2

Orbit™ MCR Learning and Development YouTube Channel

New Features

1. Support for Orbit LN7, LN1, and LN2, Licensed Radio modules.
2. *New LN radio modes supporting over-the-air interoperability with SD and x710 A radios.*

   - "transparent-serial" supports substitution of LN radios for X710s and SDs (in transparent mode) running MODEM 9600

   - "packet-with-mac" mode supports substitution of LN radios for SD remotes or SAF units running MODEM 9600 in packet-with-MAC mode.

   Consult MDS Orbit MCR/ECR Technical Manual (Rev. G) for additional details and limitations.

Changes to Existing Features

1. NX interface

   - Enhanced UI to support frequency avoidance; Orbit now allows user to enter a single frequency instead of requiring a range.
2. DHCP

   - Added DHCP relay functionality.
3. Miscellaneous

   - Added domain names as an option in the SCEP URI

Resolved Issues (Fixed)

1. Cell
   - Fixed an issue where the cell modem erroneously reported being in idle state.
2. NX (Unlicensed 900Mhz) /LN (Licensed Narrowband) Radios:
   - When used as a VLAN trunk, all VLAN IPv4 addresses are now shown at the remote for the AP, and at the AP for every remote in the connected remotes table
3. Wi-Fi
   - Fixed an issue where multiple station bridged access points on the same subnet failed to work.
4. SCEP
   - Resolved an issue where AES encryption not working with Microsoft server 2012 and 2016
2. Serial
   - Fixed an issue where 485-2 wire did not work correctly
3. WebUI
   - Fixed the issue of Chrome v56 and newer not working with HTTPS.

Known Errata

1. The logging manager can restart when a large number of VLAN interfaces are created at the same time.
2. Under some circumstances, the RIP, OSPF, or BGP protocol may need to be disabled and then enabled to resume normal operation.
3. When using hex as a custom ethertype in a QoS classifier it is incorrectly labeled as "T #".
4. Reprogramming using a local file may fail and get into a bad state. Reboot the device to regain local file reprogramming functionality.
5. If multicast terminal server operation fails, disabling the Wi-Fi interface may restore functionality.
6. On NxRadio interface status tab, refresh of NxRadio panel at the rate of 1 sec can cause the loader to be always running, thereby preventing the user from clicking 'stop' to stop the automatic refresh. It is recommended that nx-status be refreshed no more than every 5 secs. In the event, the user gets in this state, normal operation can be restored by clicking browser's reload/refresh button.
7. 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.
8. When a Commit is aborted the device may misrepresent the current configuration. It is recommended to confirm the configuration is correct and re-commit.
9. Rebooting a Station Bridge may cause a service outage to other Wi-Fi connected devices.
10. When using Dual SSIDs, changes to ap-config parameters may cause the device to reboot upon commit.
11. Monitoring a disconnected interface may cause a *netmgr* failure. (See #19 under Operational Notes and Limitations).
12. 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.
13. When a Wi-Fi Station is in the bridge, the STP status information for the Wi-Fi device is not available.
14. The "Local IPs" configuration parameter for Terminal Servers is not currently functional.
15. The unit does not support reporting the number of lost carrier events that have occurred on each wired LAN interface.
16. Unsupported web proxy functions may momentarily display error notices.
17. When using COM2 in passthrough only, the radio does not apply the vmin and vtime settings
18. Attempting to send invalid firmware over broadcast reprogramming may cause services manage to crash
19. Ethernet-GRE tunnel must be removed from any bridged interface before the VPN wizard can delete it.
20. In some cases, changes to the GRE interface configuration will require a reboot to take effect.
21. IKE using AES and gcm/16 is not functional

22. In some cases, IPSec configurations will require a reboot to take effect.
23. Setting peer-endpoint to any in DMVPN will cause all traffic on all interfaces attempt to use the VPN.
24. Using "!" in SNMP community string gives error.
25. Using the rollback command on the CLI may not restore the vlan-id to the interface.
26. When doing 802.1x port authentication, If the radius server is not reachable when the Ethernet is inserted, then it may need to be reinserted
27. Firefox versions 47-50 have a known issue preventing using the initial setup wizard
28. VLAN priority is not preserved if passed from one VLAN trunk to another
29. 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.
30. Changing settings of the RADIUS server under system, may not propagate to the Wi-Fi interface for device authentication. Disabling and re-enabling the Wi-Fi interface will resolve the issue.
31. There may be occasions where alerts are erroneously displayed on the web interface.
32. When using RADIUS user authentication with multiple servers, incorrect routes will cause authentication to fail.
33. 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.
34. Reordering lists (such as the RADIUS servers and Cell connections) is not possible in the web interface and must be done on a CLI if needed.
35. When using the remote web proxy feature, you are not able to manage the system firmware. You must connect over ssh.
36. In the web there is an issue deleting the OSPF configuration; recommendation is to do this via the CLI.
37. In there are more than 50 routes in the radio's routing table, there is an issue when displaying them via the CLI.
38. There are some known issues with the firewall configuration when editing in IE 11. Review the changes before saving in that browser.
39. Carefully review the summary of changes at the end of the firewall wizard to ensure all the changes are expected.
40. There is a known issue in some versions of Firefox where the rollback to snapshot page is not rendered correctly. You must double click the snapshot field to have the options appear.
41. Known bug in the initial setup wizard where the radius server authentication type may attempt to reset to CHAP. Review the summary and ensure the authentication type is correct.
42. In the web view of the event log, the previous button goes to the first page of the event log instead of the previous page.
43. In the web VPN Wizard, when specifying the DMVPN NBMA, you cannot use a domain name. You must use the standard web interface commands or the CLI.
44. When using the remote management service to reboot your network to a particular version, it will also reboot the unit issuing the request.
45. Changes to a QoS modify policy, may require a reboot to take effect.
46. Hitting control-C during ping will not always display the overall ping statistics.

Special Notes

1. **Configuration compatibility**
   - This release features updated configuration data models that are not backwards compatible with older releases. When a unit running an older release (e.g., 3.x.x or 4.1.x) 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.
2. Feature Availability
   - Features in this release correspond to the MDS Orbit MCR/ECR Technical Manual (Rev. G). Undocumented features if applicable should not be used without prior consultation with GE MDS.

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. In the Access Control List Wizard, if the Layer 2 Log Prefix field yields an error, delete this field to continue.
3. The HTTP Protocol is not supported for exporting files.
4. The Terminal Server may fail if polling with VMIN = 1. Disable then re-enable the Terminal Server to regain functionality.
5. Internet Explorer version 8 is no longer supported. Please upgrade this application to version 11, or use Mozilla Firefox, Google Chrome, or Microsoft Edge
6. When using an Orbit on both sides of an IPsec tunnel there is an IKEv1 issue. IKEv2 is recommended regardless of this IKEv1 limitation.
7. 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.
8. Configuring multiple Terminal Servers on the *same* TCP port does generate a warning, but operation will not work correctly.
9. Configuration of the station-max parameter, on the Wi-Fi interface, does not enforce 7 Station limit, even though the ORBIT MCR currently supports 7 Stations.
10. To delete all IPv4 addresses from an interface use the following command:
    % delete interfaces interface *myInterface* ipv4
11. Wi-Fi Station Bridging is not interoperable with other vendor's Wi-Fi devices.
12. When the Wi-Fi interface is enabled with Dual SSIDs, Station Bridging operation is restricted to the first alphanumeric SSID.
13. SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided.
14. On a Microsoft CA server, the SCEP template used should not include Extended Key Usage.
15. In WebUI, there are no preconfigured file servers. This facility is only accessible from the CLI.
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 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. Date/Time settings on ORBIT MCR are expressed in GMT format.
19. 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.
20. In rare conditions DHCP may fail to provide IP addresses; in this case a manual reboot is required.
21. 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 "\\".
22. Changes to the Wi-Fi interface mode may result in loss of data for a brief period of time.
23. STP is not functional over interfaces belonging to a VLAN.
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. The configuration parameter to enable a specific Wi-Fi Access Point, overrides the higher level configuration to

enable the Wi-Fi interface.

29. Long association times for Remotes may occur when an NxRadio Access Point interface is flooded with traffic.
30. 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.
31. When using a Public Dynamic IP Addressed SIM card, On-Demand IPsec Mode is not supported. Always-On mode must be used instead.
32. A user may not modify an already saved 'user snapshot'. Instead, delete and remake the snapshot with the necessary changes.
33. An Orbit may alarm when configuring the system name. A user may view and clear this alarm on the home screen of the Web GUI.
34. Unit may alarm after starting broadcast reprogramming with a slab memory warning, however operationally the unit will be functional.
35. The Firewall (Access Control Wizard) may get into a state where the summary screen displays changes that were not made by the user. It is recommended to cancel and restart the Wizard. Verify accuracy of all changes on the summary screen before saving the configuration.
36. A user may not be able to apply the configuration using the Interface Setup (Connectivity) Wizard and will be presented with a blank error. To ensure proper operation do not configure these items via the Wizard.
37. The user cannot proceed past the Wi-Fi Setup page in the Interface Setup (Connectivity) Wizard when using the Enterprise Privacy Mode for a Wi-Fi Access Point.
38. The routing table may not update properly after saving the configuration. To ensure proper operation a reboot is recommended.
39. 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.
40. 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.
41. An error will appear when logging into an Orbit via Web Proxy, however operationally the unit will be functional.
42. 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.
43. A com port configured as Console mode only supports 8N1 formatting even though the serial settings can be set otherwise, operates correctly when in data mode.
44. When re-authentication occurs on a WiFi enterprise link, data is blocked until authentication completes.
45. Re-authentication is not supported on an established 802.1X Port based session.
46. Syslog is not fully compliant with RFC5424.
47. At the conclusion of remote over-the-air broadcast reprogramming, the System Manager may restart.
48. Nx NICs may need be configured with dwell times above 30ms if running at 125kbps.
49. When NX is in store and forward mode, continuous downlink saturation may cause some nodes to be starved and not given upstream time.
50. In a LN system, if the modulation is forced to 64 QAM, it is recommended that FEC (forward error correction) is enabled.
51. When reprogramming from the browser on low bandwidth links, you must ensure the browser session does not time out before the file is transferred, or the reprogramming will be canceled.
52. Log level is not applicable for the eth-rules in firewall.
53. If running a com port at 300 baud it is recommended that the vtime be set to greater than 35 ms.
54. Preconfigured servers are not applicable to broadcast reprogramming.
55. When using QoS, you cannot have a shaping policy as the next-policy of priority policy.
56. When importing a configuration file that contains references to certificates, first ensure those certificates are loaded onto the unit.
57. In the web interface, certain configuration changes require a manual refresh of the web browser.
58. When operating Orbit LN in backward-compatible mode, degraded performance may sometimes occur in certain complex configurations that include an SDMS.