GE MDS

PRODUCT RELEASE NOTES Rev AP

V9.6.4

RELEASE NOTE For: MDS Master Station Firmware Version 9.6.4
RELEASE DATE: October 31, 2023

FIRMWARE

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

MDS™ Master Station

COVERING FIRMWARE – REV 9.6.4

Overview

This section describes Software/Firmware updates for the MDS Master Station, noting changes since REV 9.5.1

Products: MDS Master Station
Including: MPRS, MPRL, MPRU, MDPL
Firmware Version: 9.6.4

Consult Orbit MCR/ECR Release Notes for additional information on Orbit features that may apply to Master Station (MPR) operation.

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) 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 https://www.gegridsolutions.com/Communications/MDS/software.asp?directory=Master_Station/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.

IMPORTANT NOTES:

- This firmware applies to all MPR (MPRS/MPRL/MPRU/MDPL) except as described below
  - This firmware does NOT support Evolution/Migration Master station (serial-router).
- Once running 4.x or later system firmware, 3.x system firmware ***cannot*** be downloaded into the Master Station. To preserve the ability to boot back to 3.x firmware, ***do not*** overwrite your inactive 3.x firmware image.
  - See the section labeled “Special Instructions: Booting to 3.x firmware in the inactive image (MPRS Only)” later in the release notes for detailed instructions.
- Both active and inactive Radio Modules have their own firmware that the MPR upgrades together and keeps in sync. The Radio modules use different versioning than the Master Station system firmware. See the firmware version list in the Overview section for the expected radio module firmware versions.
- When the Firewall experiences an error, all traffic is dropped with the exception of the HTTPS and SSH protocols. These protocols can be used to recover the device to a functional state.

Supported Radio Modules

- **MDS Master Station with LN Radio Modules (MPRL)**
  - LN1B
  - LN1C
  - LN2X
  - LN4A
  - LN4C
  - LN4E
  - LN7A
  - LN9A
  - LN9C
- **MDS Master Station with LW Radio Modules (MPRL)**
  - LW7
- **MDS Master Station with SD Radio Modules (MPRS):**
  - SDM4A
  - SDM4B
  - SDM4C
  - SDM4D
  - SDM9C *(including new modules shipping in Q3 2023)*
  - SDM9K *(including new modules shipping in Q3 2023)*
- **MDS Master Station with Unlicensed 900MHz Radio Modules (MPRU)**
  - NX
- **MDS Dual Protected Master Station with LN Radio Modules (MDPL)**
  - LN1C

New Features

1. NX Profiles (U91 NIC module)
   - Functionality analogous to LN Profiles capabilities
   - Multiple configuration attributes are available for secondary profiles
   - One key use case is pre-configuring Unlicensed 900MHz remotes to be able to connect to alternate APs.

2. SNMP access now available to retrieve "system geographical-location"
   - Provides a way for NMS system to query units for fixed location without GPS
   - New OIBs: mSysLocLatitude, mSysLocLongitude, mSysLocAltitude

Changes to Existing Features

1. Added support for RADIUS Message-Authenticator attribute
2. Added ability for RADIUS Servers list to include multiple entries to the same IP/Port
3. The MultiHop feature (available in select configurations only) now supports 20 static routes.
4. Multiple Updates for CVE resolution (improved security)

Resolved Issues (Fixed)

MDS Master Station since v9.5.1:

- LN Flash Robustness protection was added. This protects against rare cases of LN Flash Corruption seen in some low voltage brown-out conditions [n0020]
- Radius Authentication was not working on a point-to-point link [n0057]
- Orbit LN operating in FSK modes, now prevents use of invalid unit address (which caused DLINK operations to be ignored) [6086] [6087]
- For serial operation when Vmin was set to 0 on a physical COM port (e.g., COM1), the Vtime setting was being treated like 0. Vtime is now properly handled. [6091]

Preserving ability to run previous configuration

New versions of Master Station code use updated configuration data models that are not backwards compatible with older releases. When a unit running a *previous* release is upgraded to this release, a snapshot of its configuration is made and stored on the unit called "Auto". The unit's configuration is automatically migrated to newer data model. The user can downgrade back to the *previous* firmware version only by choosing to revert to the legacy configuration snapshot as described here. Any firmware can be loaded that is greater than or equal to the Factory snapshot version, but may require a different firmware cert be loaded (See SPECIAL NOTICE FOR CUSTOMERS UPGRADING TO THIS VERSION section above).

To maintain ability to run previous firmware follow the procedure below.

1. Should it be determined that reverting to the previous firmware is necessary, perform the following command on the CLI to reboot to the old firmware, and restore the system using a configuration snapshot. The Auto or a user snapshot can be used if available, but the factory snapshot will always be available.

```
> request system recovery rollback which-image { inactive } snapshot Auto
```

2. You will be prompted to confirm this action:
   The current system configuration will be erased and replaced with the snapshot. Proceed? [no,yes]
3. Type 'yes' and press enter, and the system will restart to the *previous* configuration
4. Note that the recovery operation *may* include restoration of a previous SHA1 FW certificate. If so, then it will be necessary to reinstall the new SHA256 FW certificate before newer software can be downloaded again.

Special Instructions: Booting to 3.x firmware in the inactive image (MPRS Only)

To switch between 3.x firmware and 4.x system firmware on an MPRS follow the procedure below.

1. IMPORTANT: Once you are running 4.x firmware or greater, be sure to not overwrite the 3.x firmware in the inactive firmware location, or you will not be able to revert back to that version. E.g. copying active firmware to inactive location, or installing a new version to the inactive firmware location.
2. Should it be determined that reverting to the old 3.x firmware is necessary, perform the steps from the "Preserving ability to run previous configuration" section above to load the inactive image with a previous snapshot.

Known Errata

- **MDS Master Station Platform (including MPRS/MPRL/MPRU/MDPL):**
  - It is recommended to not delete certificates or keys that are configured for use. If they are deleted there can be many errors including display issues on the web interface. [6241]
  - For MPRS, when updating Firmware a reboot may sometimes be required. [5853]
  - When using OpenVPN, if data is not able to pass over the VPN or the status page indicates that the service is in error, then the unit must be rebooted to recover. [5857]
  - When using MPRS to broadcast reprogram SD radios, if remote detection is enabled, then we recommend increasing the reprogram repeat value from 3 to 6. [5643]
  - Avoid binding a service to a radio interface. This may cause erratic behavior. [5422]
  - Firewall filters that have a layer 2 rule can only be applied to a bridge or VLAN interface. They will not be displayed in the tab complete or pulldown menus for other types of interfaces. [5644]
  - Binding the SSH, SNMP, or NETCONF service to an IPv4 or IPv6 address can cause boot errors if that address's interface is not up at the time of boot. This can happen if the unit is rebooted with the interface disabled or in the case of WiFi, if a connection is not made shortly after boot. To mitigate this issue, firewall can be set to control what traffic passes on each interface. [5289]
  - When using OpenVPN, verify that the clients are connecting properly. An errant client it can prevent a valid client from connecting correctly. [5295]
  - When using OpenVPN server, if multiple clients connect with the same client certificate, the assigned IP address will be in conflict. Ensure unique certificates are used among all clients and restart the OpenVPN server. [5043]

- VRF interface packet statistics may not match the member interfaces. Use the member interface statistics instead. [5034]
- The Orbit MCR 6 Ethernet port offering does not include physical serial ports. Serial over USB is provided and is configured as COM1 in the Orbit user interface. [3613]
- For a system with LW radios, if degraded performance is observed immediately following a radio configuration change, effect recovery by disabling then re-enabling the LwRadio interface. [4712]
- Exports of large serial captures might fail. Retry the operation capturing data for a smaller interval of time. [4198]
- If TACACS+ user authentication is used, and the server is routable, but not reachable, the system may lock up and reboot while attempting to authenticate a user. [4611]
- If broadcast reprogramming does not complete, restart the transfer to continue reprogramming. [4283]
- On a Web-based file transfer (From Local File) through remote proxy, if the WebUI gets stuck in the file transfer state, performing the operation via CLI can restore operation. The CLI file transfer request need not be successful. [4395]
- When performing bulk changes to the SNMP service if the commit operations fails, it may be necessary to break the changes up into a set of smaller commits. You must discard current changes (or reboot) and enter the changes in smaller sets. [4520]
- In a very large LN network with multiple polling threads, it may be necessary to reduce the traffic entering the LN AP prior to initiating broadcast reprogramming. [4180]
- Do not use MPRS to broadcast an update to the DLINK encryption phrase. [4259]
- Destination NAT is not currently supported for IPv6. [4196]
- If a unit repeatedly fails to receive an over the air broadcast reprogram, connect to the unit and copy the active image over the inactive image to attempt to recover the state. Restart the broadcast reprogramming if it has stopped. [3681]
- Payload buffer delay is only applicable in x710 mode. [3972]
- 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. [2139]
- 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. [1876]
- QOS does not operate handle the DSCP field correctly. To ensure proper QOS priority use the TOS equivalent. [2304]
- A QoS modify policy is not tied to an interface and must be deleted to disable it. [1542]
- Changes may not be applied immediately when changing Data Device Mode to either DCE or CTS Key mode. They will be applied after a reboot or failover. [1267,1377]
- MPRS does not support multiple TCP connections in TCP multi-host mode. [1934]
- When using QoS, you cannot have a shaping policy as the next-policy of priority policy. [1544]
- A QoS modify policy will act like it is automatically applied to all interfaces [2023]
- Syslog is not fully compliant with RFC5424. [1028,1033]

Operational Notes and Limitations

- **MDS Master Station Platform (including MPRS/MPRL/MPRU/MDPL)**
  - Performing an ICMPv6 ping to a link local address requires one to specify the src-address of the outgoing interface. [1385]
  - 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. [93]
  - While MDS Orbit supports management and routing via IPv6, not all services have support for IPv6. [1672]
  - STP is not functional over interfaces belonging to a VLAN. [3324]
  - 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. [1246]
  - In the event of Web display issues, try clearing the browser cache. [3505]

- If there is an error downloading firmware from an HTTP server, the unit may require a reboot. [3580]
- For the LW radio in the MPR, the LED behavior on the card may not be as expected. [1844]
- UDP Iperf server does not return a report. Use TCP mode to see bandwidth. [3223]
- MPR VSWR support for LN 100MHz and 200MHz is not supported. [3082]
- On MPR, if SD interface returns error about unsupported mode, in some cases this is erroneous and can be ignored. There can be errors in the detection of the SD nic type that manifest this way. [2022]
- MPRS (4B) receive frequencies using exact multiples of 25MHz (400.000, 425.000, 450.000, 475.000, and 500.000MHz), result in degraded sensitivity and performance. [700]
- Due to a limitation of SD data compression when operating with certain modems, this feature has been removed. [825]
- When operating as a repeater in x710 or transparent mode, using modem 9600 and baud rate 9600-8E1, the new repeater-tolerance parameter should be set to 'custom' to reduce errors. [758]
- When operating MPRS as a DATAKEY Repeater with SDx/x710 radios as remote endpoints in 9600 modem, for proper operation we recommend that the following parameters be configured in the remotes:

  SDx/SDMS Polling Remote SCD: 8ms

  x710/SDx Remote SCD: 12ms

  SDx/SDMS Polling Remote and x710/SDx Remote PTT

  For baud 96008N1: 0ms

  For baud 96008E1: 4ms

  When operating the SDMS as a CKEY Repeater with SDx/x710 radios as remote endpoints in 9600 modem, for proper operation we recommend that the following parameters be configured in the remotes:

  SDx/SDMS Polling Remote SCD: 6ms

  x710/SDx Remote SCD: 8ms

  [762]
- When operating in RTS keying mode, full-duplex operation is not supported. For full-duplex operation, continuous keying must be used. [324]
- An MPRS in transparent mode using ip-payload may require a reduction in the transparent-rx-timeout value, if the data streams are longer than 1480 continues bytes. [1215]
- When using PulseNET or PulseNET Enterprise to monitor an MPRS in Packet w/ MAC mode, the Passive Collection Repeat Interval (in PulseNET) must be changed from the default 5000ms to a recommended value of 130000ms. This value must be changed for EACH MPRS being monitored in PulseNET. [1328]
- An SD Radio Module configured as a Dlink root will not send local Dlink messages over the air if the radio is also configured for Repeater Mode "repeater". An SD repeater that is also a Dlink root must be set to "repeater-with-local-data". [750]
- When the operational mode of a radio is changed (e.g. from transparent to packet-with-mac), all mode specific parameters will assume their default values, even if previously set to a different value (e.g. MAC AP vs. Remote). [611]
- Operating as a Repeater with local-data when using modem "none" may not work properly when using SDM9C or SDM9K Radio Modules. In this case, set the repeater mode to "repeater" instead of "repeater-with-local-data". This does not apply when using SDM4B or SDM4C Radio Modules. For these modules, "repeater-with-local-data" should be used. [542]
- With configuration change of radio parameters, an entire poll cycle may be needed in LN advanced polling mode. [1940]
- Current release of MPRL NIC module hardware does not set the TX LED correctly, if operating in simplex mode. It is constantly on even when the NIC is receiving. [1165]

- When configuring L7W (Licensed 700MHz Wide), do not set NIC-id. It is not supported in this release and will prevent link establishment. [3747]
- In a LN system, if modulation is forced to 64 QAM we recommend enabling FEC (forward error correction). [1327,1405]
- Header compression is not recommended for large serial polled system or system with only broadcast downstream messaging. [1951]
- Timeout of MODBUS transactions, can cause dropped TCP connections. Potential fixes to increase poll rate or increase transaction timeout. [1646]
- If web page display seems to render incorrectly, try refreshing the page. [1783]
- 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 "\\". [1234]
- On a Microsoft CA server, the SCEP template used should not include Extended Key Usage. [2053,2409]
- SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided. [2052,2408]
- 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. [1326]
- While the MDS Master Station supports management and routing via IPv6, not all services have support for IPv6. [1781]