GE MDS *PRODUCT RELEASE NOTES Rev T*

RELEASE NOTE For: MDS ORBIT MCR/ECR Firmware Version 4.6.8
RELEASE DATE: July 7, 2016

FIRMWARE

©2016 GE MDS LLC, 175 Science Parkway, Rochester, NY 14620 USA
Phone +1 (585) 242-9600, FAX +1 (585) 242-9620
http://www.gegridsolutions.com/Communications/

MDS™ Orbit MCR/ECR

COVERING FIRMWARE – REV 4.6.8

Overview

This section describes Software/Firmware updates for the MDS Orbit MCR/ECR platform, noting changes since REV 4.1.7.

Products: MDS Orbit MCR/ECR
Firmware Version: 4.6.8

Orbit™ MCR Learning and Development YouTube Channel

New Features

1. Support for Orbit LN9, 900MHz (896-960MHz) Licensed Radio Module
2. Dynamic Multipoint VPN (DMVPN)
   - DMVPN combines multipoint GRE (mGRE) Tunnel, IPsec encryption and NHRP (Next Hop Resolution Protocol) technology to enable simplified configuration of hub-to-spoke VPN deployments. It enables new spokes to be added to the VPN without requiring any changes on the HUB. In addition, it enables formation of on-demand dynamic tunnels between spokes for a full meshed VPN network.
3. Dynamic Routing
   - Added support for BGPv4. This is the recommended protocol for use on large scale hub-n-spoke DMVPN networks.
4. Port based authentication on Ethernet ports
   - 802.1x based authentication – The Orbit device acts as EAP authenticator that enables data traffic to flow through the port only after the device connected to the port (called client/supplicant) has authenticated itself with the EAP Authentication server. A RADIUS server with EAP extensions is the only supported Authentication server. The Orbit device acts as RADIUS client and facilitates EAP authentication exchange between the connected device and the RADIUS server.
   - MAC authentication bypass (MAB) based authentication – The Orbit device authenticates the device connected to the port (called client) based on its MAC address using Password Authentication Protocol (PAP) with the Authentication server. A RADIUS server with PAP support is the only supported Authentication server. The Orbit device acts as RADIUS client and includes the connected device's MAC address in username, password and calling-station-id attributes in the RADIUS PAP authentication request

sent to the server. This mode is useful to provide security to legacy devices that do not have EAP client/supplicant functionality.

5. Ingress rate limiting on Ethernet ports
   - The ingress rate and burst can be configured on per-port basis to limit the rate of traffic ingressing the Orbit device.
6. Virtual Router Redundancy Protocol (VRRP)
   - VRRP enables redundant default routing path for local LAN devices by creating a virtual router using two physical routers in master and backup roles. Orbit device can be configured in master or backup VRRP role and VRRP operation can be enabled on Ethernet, Bridge, and VLAN interfaces. In addition, custom functionality has been added to enable master to backup router failover if upstream/WAN connectivity is down via master router (as verified by NETMON ICMP echo probes configured on backup router).
7. IP pass-through service
   - This service enables an outside interface's (e.g. Cell) IP address to be passed through to a device connected to inside interface (Bridge) of Orbit, making Orbit acts as a dumb modem (like a cable modem). The pass through service also enables user to configure certain traffic to be terminated at Orbit (for example, management) instead getting passed through.
8. QoS
   - Added modify policy- This policy enables setting of TOS/DSCP fields of the IP packet based on layer-3/4 headers. Among other use cases, this can be used to enable QoS on traffic that is tunneled through GRE and IPsec tunnels over Cellular.
9. Configuration snapshots
   - OEM snapshots - This enables an OEM to replace the MDS factory snapshot with OEM snapshot.
   - User snapshots – This enables a user to create up to two snapshots of Orbit configuration that are stored on the device. This can be helpful if the user needs to reset unit's configuration to a working configuration that was saved previously as user snapshot.
10. VLAN
    - VLANs are now supported over GRE tunnels (in ethernet-over-gre mode).
11. Web UI
    - The VPN wizard has been completely redesigned to be more use-case based and includes network diagrams for common VPN setups.

Changes to Existing Features

1. Terminal Server
   - Reduced default value of VTIME from 100ms to 10ms to enable faster polling.
2. WebUI
   - Change password & OTP warnings to be post-login instead of pre-login. Also, web UI displays a post-login warning to the user if the admin password has not been changed.
3. VPN
   - The VPN service status has been updated to include detailed information about the IKE and IPSEC security associations.
4. Cell
   - Removed the restriction of fixed MTU size from Cell interface. The MTU can be configured from the range of 68 to 1500 bytes, with default MTU of 1428.
   - Added additional status parameters to cellular status (TAC, global cell id, physical cell id, band, bandwidth etc) for 4Gn/E42/E4S cellular models.
   - Fixed an issue with event log getting full when 3G cell (model=3G1) is enabled without SIM.
5. DHCP
   - DHCP client "RENEW" event is not logged anymore to reduce unnecessary event logging.
6. CLI

- The “show log”, “monitor” and “tcpdump” commands are removed from standard access, as they are only intended to be used in conjunction with GE personnel.
- Added admin level command “clear log” to clear internal debug log files.

7. Miscellaneous
    - The boot time has been reduced by ~50% (as compared to 4.1.7 release) when the unit running this version is rebooted to the same or higher version (i.e. when it is not the first time boot to this version).
    - The *tech* and *oper* logins are now disabled if their passwords have not been changed from the default.

Resolved Issues (Fixed)

1. Cell
    - Fixed the issue where if there is no SIM in slot-A, profile does not switch correctly to SIM-B. This applies only to Orbits with the 2G/3G GSM World cellular modem in a dual-SIM configuration.
2. NX (Unlicensed 900Mhz) /LN (Licensed Narrowband) Radios:
    - Fixed multiple issues with OTA broadcast firmware reprogramming for NX/LN networks and made it significantly more robust. Also, enhanced reprogramming status information.
    - Added NX/LN network admission control to prevent exhaustion of resources (and subsequent AP reboot) when RoHC is enabled. The AP now limits the maximum number of remotes that can connect based on resource usage
3. WebUI
    - Fixed the issue of Chrome v50 not working with HTTPS.
    - Fixed an issue with update of “avoided frequencies” parameter (under advanced configuration) for NxRadio interfaces.
    - Fixed an issue with use of custom certificates for HTTPS.
    - Fixed an issue where selection of VLAN mode for Ethernet interface unchecks the “Enable” checkbox.
    - Fixed an issue with security mode setting for NxRadio in interface setup wizard.

Known Errata

1. Upon the first boot to this firmware version, a Licensed Narrowband Orbit may erroneously display a “Failed to reprogram the NIC” alarm. If this occurs, rebooting the Orbit will clear the alarms.
2. The logging manager can restart when a large number of VLAN interfaces are created at the same time.
3. Under some circumstances, the RIP, OSPF, or BGP protocol may need to be disabled and then enabled to resume normal operation.
4. When using hex as a custom ethertype in a QoS classifier it is incorrectly labeled as “T #”.
5. Wizards which require a ‘Ruleset’ name cannot include spaces or other special characters.
6. Reprogramming using a local file may fail and get into a bad state. Reboot the device to regain local file reprogramming functionality.
7. If multicast terminal server operation fails, disabling the Wi-Fi interface may restore functionality.
8. The DHCP server does not support IPv6.
9. When using multiple Orbits as WiFi Access Points, they must be located on separate broadcast domains.
10. 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.
11. 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.
12. Changing the Wi-Fi configuration may cause station-bridge clients to stop passing data. A reboot is required to recover.
13. Wi-Fi -When the AP’s psk is set to 64 Hex characters, WiFi clients are unable to join the AP. Setting the AP’s psk to 63 characters will allow clients to join.
14. 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.

15. Rebooting a Station Bridge may cause a service outage to other Wi-Fi connected devices.
16. When using Dual SSIDs, changes to ap-config parameters may cause the device to reboot upon commit.
17. Monitoring a disconnected interface may cause a *netmgr* failure. (See #22 under Operational Notes and Limitations).
18. 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.
19. When a Wi-Fi Station is in the bridge, the STP status information for the Wi-Fi device is not available.
20. The "Local IPs" configuration parameter for Terminal Servers is not currently functional.
21. WebUI -Using Firefox 47, the Rollback Recovery Snapshot field does not have a drop down box.
22. The unit does not support reporting the number of lost carrier events that have occurred on each wired LAN interface.
23. NxRadio Connected Remotes TX Statistics do not update if using encryption.
24. A Configuration File will not export the serial port baud rate if the file was created when the parameter was at the default.
25. When the Cell interface is disabled, the LED may not reflect this.
26. In rare cases, when making parameter changes or when going in and out of "Data Mode" the terminal server service may begin to repeatedly restart. If this occurs reboot the Orbit.
27. The Firewall wizard may appear blank, if this occurs, leave the wizard and re-enter it.
28. Unsupported web proxy functions may momentarily display error notices.

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. F). Undocumented features if applicable should not be used without prior consultation with GE MDS.

Special Configuration for SEL Mirrored Bits™

Orbit devices equipped with NX (Unlicensed 900Mhz) Radio modules have been tested to successfully run with select SEL Mirrored Bits™ devices, provided that the modem setting is MODEM 1250, and that following configuration is added:

```
admin@(none) 17:24:43> unhide debug
admin@(none) 17:24:51> configure
Entering configuration mode private

admin@(none) 17:25:03% set watchdog resource-monitor period 67
admin@(none) 17:25:34% set watchdog polled-applications period 61
[ok][2013-03-06 17:25:49]

admin@(none) 17:25:49% commit
Commit complete.
admin@(none) 17:25:59> hide debug
```

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. 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 or Google Chrome.
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 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. While using the multicast reprogramming feature, do not interact with the sending device for the first 5 minutes.
10. 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.
11. To delete all IPv4 addresses from an interface use the following command:

    % delete interfaces interface *myInterface* ipv4
12. Wi-Fi Station Bridging is not interoperable with other vendor's Wi-Fi devices.
13. When the Wi-Fi interface is enabled with Dual SSIDs, Station Bridging operation is restricted to the first alphanumeric SSID.
14. When using Dual SSIDs maximum throughput is achieved only on the first SSID; the second SSID will have reduced capacity (details are system dependent)
15. SCEP operations require certificate information to contain a Common Name, otherwise the operation will fail. No direct indication of failure is provided.
16. On a Microsoft CA server, the SCEP template used should not include Extended Key Usage.
17. In WebUI, there are no preconfigured file servers. This facility is only accessible from the CLI.
18. 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.
19. 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.
20. A Wi-Fi Station will not age out in the event that its corresponding Wi-Fi Access Point is no longer present.
21. Date/Time settings on ORBIT MCR are expressed in GMT format.
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 to the Wi-Fi interface mode may result in loss of data for several minutes.
26. STP is not functional over interfaces belonging to a VLAN.
27. 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.
28. Not all certificate upload or download actions create proper events in the event log.
29. Displaying the active routes will not show all configured routes, when connectivity to an affected subnet cannot be established.
30. When changing a Wi-Fi Station to put it into a VLAN, you must reboot the device.

31. The NxRadio connected-remotes database will not show an IP address if the Remote is configured to participate in VLANs.
32. The configuration parameter to enable a specific Wi-Fi Access Point, overrides the higher level configuration to enable the Wi-Fi interface.
33. Long association times for Remotes may occur when an NxRadio Access Point interface is flooded with traffic.
34. 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.
35. A bridged link between a Wi-Fi Access Point and a Station will only pass <1492 byte frames.
36. When using a Public Dynamic IP Addressed SIM card, On-Demand IPsec Mode is not supported. Always-On mode must be used instead.
37. A user many not modify an already saved 'user snapshot'. Instead, delete and remake the snapshot with the necessary changes.
38. 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.
39. Unit may alarm after starting broadcast reprogramming with a slab memory warning, however operationally the unit will be functional.
40. 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.
41. The Firewall (Access Control Wizard) may get into a state where the filter screen does not display any rules. It is recommended to cancel and restart the Wizard. Verify accuracy of all changes on the summary screen before saving the configuration.
42. 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.
43. A user may not be able to proceed past the DHCP Server screen in the Interface Setup (Connectivity) Wizard. To ensure proper operation do not configure these items via the Wizard.
44. 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.
45. The routing table may not update properly after saving the configuration. To ensure proper operation a reboot is recommended.
46. 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.
47. 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.
48. An error will appear when logging into an Orbit via Web Proxy, however operationally the unit will be functional.
49. 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.
50. The NX (or LN) NIC LED when the interface is disabled, may incorrectly show its previous link status until the interface is re-enabled or the unit is rebooted.
51. 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.
52. When re-authentication occurs on a WiFi enterprise link, data is blocked until authentication completes.
53. Re-authentication is not supported on an established 802.1X Port based session.
54. Syslog is not fully compliant with RFC5424
55. At the conclusion of remote over-the-air broadcast reprogramming, the System Manager may restart.