DIGI INTERNATIONAL
9350 Excelsior Blvd, Suite 700
Hopkins, MN 55343, USA
+1 (952) 912-3444 | +1 (877) 912-3444
www.digi.com

SAROS Release Notes
WR11, WR21, WR31, WR44R, WR44RR
Version 8.3.0.1

INTRODUCTION

These are the release notes for the SAROS, the firmware used on the WR11XT, WR21, WR31, WR44R, and WR44RR routers.

SUPPORTED PRODUCTS

- Digi WR11XT, WR21, WR31, WR44R, WR44RR

KNOWN ISSUES

1. MC7354 (L5) Routers with GPS capability may report 0 satellites in view after several hours of operation. The only known workaround is to reset the module. [SAROS-2579]

UPDATE CONSIDERATIONS

It is recommended that you perform a backup of your device's settings prior to upgrading your firmware. If you should need to revert back to a previous version of firmware, this will ensure that you will be able to restore your device to its previous settings in the event that some settings are not restored properly after downgrading the firmware.

To back up your device settings, follow this simple procedure:
Open the web user interface and navigate to the "Administration" section and select "Backup/Restore".
Select the parts of the devices' settings that you wish to backup.
Click the "Backup" button and select the location to where you want to save your backup file.

To restore:
Navigate to the same section within the web UI.
Click the "Browse" button to select the backup file you saved in the previous steps.
Click the "Restore" button to upload the configuration settings contained in your backup file.

DEFAULT USER ACCOUNTS

Previous firmware releases for the WR11, WR21, WR31, and WR44 devices included a default user account with the credentials **username/password**. With firmware release 8.0.0.3, new routers will no longer include the default **username/password** account. Instead, routers manufactured with firmware release 8.0.0.3 will now have a default **admin** account and a pre-programmed unique password that is displayed on the device label.

Special consideration must be given when upgrading or downgrading devices that cross this functional boundary. The following special cases apply:

1. Upgrading routers that were manufactured prior to 8.0.0.3 (for example, 7.1.2.2):
    a. If you upgrade the firmware to 8.0.0.3 using the Web UI **Update Firmware**[1] , the router retains the existing default user accounts. For example, after the upgrade, the router will have a default **username/password** account running 8.0.0.3.
    b. If you upgrade the firmware to 8.0.0.3 using Flashwriter, the default account will be **admin** and the password will be **default**.
2. Downgrading routers originally manufactured with 8.0.0.3, that include an **admin** account with a pre-programmed unique password:
    a. If your router is running 8.0.0.3 and has the **admin** account with a pre-programmed unique password, and you use the Web UI **Update Firmware** to downgrade to a release prior to 8.0.0.3, the downgraded router will no longer recognize the pre-programmed unique **admin** account password. Instead, the **admin** account password will be **default**.
    b. If your router is running 8.0.0.3 and has the **admin** account with a pre-programmed unique password, and you use Flashwriter to downgrade to a release prior to 8.0.0.3, the **admin** account will no longer be present. Instead, the default account will be **username/password**.
        i. After downgrading with Flashwriter, if you then upgrade to 8.0.0.3 or greater using the Web UI **Update Firmware**, the router will retain the **username/password** account and not include an **admin** account.
            1. If you then factory default the router, the **admin** account with the pre-programmed unique password will return.
        ii. After downgrading with Flashwriter and losing the **admin** account, if you then upgrade to 8.0.0.3 or greater using Flashwriter, the **admin** account with the pre-programmed unique password will again be present and the **username/password** account will be removed.

[1] Any Web UI Update Firmware operation can be substituted with a Remote Manager Update Firmware operation, instead.

UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you update production devices.
2. Unless otherwise noted, apply updates in the following order:
    a. Device firmware
    b. Modem firmware
    c. Configuration
    d. Application

Digi recommends Digi Remote Manager for automated device updates. For more information, go to https://www.digi.com/products/iot-platform/digi-remote-manager.

TECHNICAL SUPPORT

Get the help you need via our Technical Support team and online resources. Digi offers multiple support levels and professional services to meet your needs. All Digi customers have access to product documentation, firmware, drivers, knowledge base and peer-to-peer support forums.

Visit us at https://www.digi.com/support to find out more.

SUPPORED CELLULAR MODULES

Within the SarOS family, Digi continues to work with cellular module vendors and stays up to date with all their latest feature improvements and bug fixes. These are the current shipping modules today and the latest module firmware we are testing with:

Sierra Wireless

MC7354 (L5)			
	AT&T	05.05.58.00	005.026_000
	Verizon	05.05.58.01	005.029_001
	Sprint	05.05.63.01	005.037_000
	Generic	05.05.58.00	005.025_002
	Telus	05.05.58.00	005.023_000
	Rogers	05.05.58.00	005.022_000
	Bell	05.05.58.00	005.024_000
MC7430 (L9)			
	Generic	02.30.03.00	002.046_001
	Telstra	02.30.03.00	002.044_000
MC7455 (M8)			
	AT&T	02.32.11.00	002.070_000
	Verizon	02.33.03.00	002.079_001
	Generic	02.32.11.00	002.064_000
	Telus	02.32.11.00	001.040_000
	Rogers	02.32.11.00	001.040_000
	Bell	02.24.05.06	001.005_000

Telit

HE910-D (U9)		12.00.028
LE910-NAG (L6)		17.00.503
LE910-EUG (L7)		17.00.523
LE910-SVG (L8)		17.00.573
LE910-NA1 (M6)		
	AT&T/Generic	20.00.527
	Verizon	20.00.017
LE910-NAV2(M5)		
	AT&T/Generic	20.00.507
	Verizon	20.00.007
LE910-EU1 (M3)		20.00.416
LE910-EUV2 (M7)		20.00.406
LE910C1-AP (M9)		25.26.255
LE910C1-NS (M4)		25.00.246

Cellient

MPN200	MO200SWE q6695-SWE-3134

Triorail

TRM-5	v03.001

CHANGE LOG

VERSION 8.3.0.1 (Bootloader 7.67) 4 January 2021

This is a recommended release.

ENHANCEMENTS

1. Optimizes the determination and handling of expired stateful firewall entries. [SAROS-3175]
2. Extends the imsi.txt auto APN list to include tnf.m2m for ICCID 893108/IMSI 20408081. [SAROS-3177]
3. Adds missing AT&T ICCIDs 8901030, 8901150, 8901170, 8901560, and 8901680, as well as 893320 to the default pdn.txt file. [SAROS-3162, SAROS-3150]
4. Changes the default Temperature logging behavior to not write to Flash. Instead a new `templog 0 save_to_flash` parameter has been created, which defaults to `off`. This can be changed to `on` to revert the behavior. [SAROS-3174]

BUG FIXES

1. Corrects a defect during DRM Firmware Repository Downloads, when the router falls behind and queues data, corruption could occur. This behavior was intermittent and never observed when using the file browser on Digi Remote Manager. The behavior was only observed when selecting firmware directly from the Remote Manager Firmware Repository. [SAROS-3157]
2. APN cleared after MC7430 upgrade. [SAROS-3176]
3. Corrects the authentication setup for Cellient MPN200 modems that prevented Radius based SIMs from establishing a cellular connection. [SAROS-3183]
4. Corrects a Getting Started Wizard defect that incorrectly disabled the `ppp 1 nocfg` <x> parameter. [SAROS-3169]
5. Corrects ARP handling that caused incorrect packet routing when VRF interfaces were configured with overlapping IP address spaces. [SAROS-3172]
6. Corrects Digi Remote Manager set settings defect when the `modbus n async_mode` parameter was set to 1 (RS-422/485). [SAROS-3173]
7. Corrects the MC7455 (M8)/MC7430 (L9) Auto Carrier selection mechanism. Also corrects the behavior of the `modemstat ?` command to clear information after a modem reset and to correct the criteria for declaring a “Got modem status OK” Outcome. [SAROS-3158]
8. Corrects a defect related to flash writes after changing the Hub and Port Isolate (`ethhub/ethvlan`) behavior. It was discovered that any flash write that occurs after issuing this command would prevent the setting from taking effect. [SAROS-3170]

VERSION 8.2.0.2 (Bootloader 7.67) 4 September 2020

This is a recommended release.

ENHANCEMENTS

1. Adds a default pdn.txt file. This includes ICCIDs for devices that required connecting from PDN 1. This file will be present with routers that ship from the factory, or get reprogrammed with Flashwriter. [SAROS-3126]

BUG FIXES

1. Corrects the MC7455 (M8) and MC7430 (L9) setup of Radius (Username/Password) parameters, required prior to the establishment (and activation) of a connection. Prior to this change, the initial Radius authentication could easily fail and prevent an initial LTE connection. Often observed was an initial WCDMA/UMTS connection, which would then migrate later to LTE. [SAROS-3138, SAROS-3133]
2. Corrects the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) setup of Radius (Username/Password) parameters, similar to the above. In addition, also removes errant short AT command timeouts related to connection establishment (#NCM) and activation (+CGACT), and will automatically attempt a connection on PDN slot 1 if a failure occurs on slot 3. Lastly, will also clear out

the APN written to PDN 1 when no ICCID pdn.txt match found. [SAROS-3143]
3. Corrects defects in the MC7455 (M8), MC7430 (L9), and MC7354 (L5)-based power up/down process that could leave a modem stuck in the Low Power State (Airplane Mode). [SAROS-3139, SAROS-3142]
4. Corrects several NAT defects including a defect related to NAT response packet routing for packets that originate on an IP address matching an interface address on the router and the routing of IMCP packets. [SAROS-3118, SAROS-3140]
5. Corrects several DRM defects, including a defect that prevented the display or configuration of serial settings, a missing parameter for the ovpn x sslcli_add y setting, and the ability to set NAT settings. [SAROS-3135, SAROS-3145, SAROS-3122]
6. Changes the maximum size of the pdn.txt file from 5 to 1024 entries. [SAROS-3144]
7. Adds several missing modem disconnect reasons to the logcodes.txt file. [SAROS-3131]

VERSION 8.1.0.1 (Bootloader 7.67) 23 April 2020

This is a mandatory release.

ENHANCEMENTS

1. Adds support to auto sense cellular MTU on all QMI and LE910-NAV2 (M5) and LE910-NA1 (M6) based routers. Routers that use QMI modems will query the modem and set the MTU based on the carrier response. For LE910-NAV2 (M5) and LE910-NA1 (M6) routers, if `ppp 1 l_mru` and `r_mru` remain unchanged at a default setting of 1500, the router will automatically set the MTU to 1428 when the Firmware Carrier used is Verizon; and 1430 for all other carriers. [SAROS-3106, SAROS-3100, SAROS-3096]
2. Adds support for a new configuration parameter (`services 0 ip_in_ip ON|OFF`) to control IPv4 encapsulated IPv4 packet handling. This new parameter, which defaults to OFF, drops all IPv4 encapsulated IPv4 packets. If required and you're on a private network, you can set this parameter ON to receive these packets. [SAROS-3102]
3. Adds support to display the SIM slot to the `modemstat` command and the subnet mask to the `ppp 1 status` command. [SAROS-3077, SAROS-3082]

SECURITY FIXES

1. A reflective DoS vulnerability was reported by Yannay Livneh to Digi's security team. Digi measureed this vulnerability as a CVSSv3.0 score as a 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). This reflective attack can occur on the cellular network interfaces if no firewall is configured. Digi recommends either turning on the default firewall configuration, or upgrading to this release to mitigate the vulnerability. Details on this vulnerability will be shared around May 15th, 2020. Please see https://kb.cert.org/vuls/id/636397/ for details at that time. Digi International will also be coordinating the release of details at https://www.digi.com/security. Many thanks to Yannay Livneh for finding this vulnerability, as well as Vijay Sarvepalli, CERT Coordination Center, Carnegie Mellon University for coordinating the details of the release. [SEC-1411]

BUG FIXES

1. Corrects several defects that prevented configuration via Remote Manager on the WR11 and WR44RR platforms. [SAROS-3090, SAROS-3080, SAROS-3116]
2. Corrects a defect that prevented SMS from correctly sending on the LE910-EU1 (M3) or LE910-EUV2 (M7) platforms, when operating on some Orange networks. For these carriers, and others that require the 3GPP TS 23.038 SMS Data Coding scheme or the Cell Broadcast Data Coding Scheme, setting the `modemcc 0 send_csmp ON` enables this behavior. The behavior will default to `OFF`. [SAROS-3093]
3. Corrects the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) platforms to auto detect network deactivations (i.e., due to PRL updates) and to gracefully reestablish connections that were mistakenly thought to be active. [SAROS-3095]
4. Corrects a defect that prevented the disabling USB devices when using the Web UI or the CLI command `usb dislist usb-1-.` [SAROS-3067]
5. Corrects a defect that prevented the backup APN (`modemcc 0 buapn XXX`) from working correctly. [SAROS-3072]

6. Corrects VRRP defects that leaked packets containing the hardware MAC address, instead of the IETF assigned address, on single Ethernet WR21's; corrected a defect that caused memory corruption during each VRRP transition when SNMP Traps were enabled. [SAROS-3073, SAROS-3086]
7. Corrects a potential WR44R/WR44RR illegal exception crash in the Wi-Fi AP. [SAROS-3104]
8. Corrects a defect in the MultiTX Match String support that left the Matched string in the datagram when the Strip match string was enabled. [SAROS-3070]
9. Availability of the latest LE910-NAv2 (M5) and LE910-NA1 (M6) 20.00.xx7 firmware addresses a defect in the modem that resulted in duplicate DNS servers observed. [SAROS-2839]

VERSION 8.0.0.3 (Bootloader 7.67) 30 November 2019

This is a recommended release.

ENHANCEMENTS

1. Adds support for unique device passwords. Starting with SarOS 8.0, routers will no longer include a default username/password account. Instead, routers will have an admin account and use the manufactured password that is printed on the product label. [SAROS-2938]
2. Adds Digi SureLink by default to the Getting Started Wizard, which protects against devices that disconnect from the cellular network. Changes the default link_retries setting for all routers to 50 (which is roughly 50*10 seconds), which allows two full link_retry recovery cycles, before a default rebootfails cycle occurs (which defaults to 125). [SAROS-2982, SAROS-3021]
3. Adds `wififilt` command wildcard matching, similar to the wildcard support in the `macfilt` command. [SAROS-2987]
4. Adds support (`modemcc 0 GSMenc 0`) to enable GSM SMS encryption for the LE910-EU1 (M3) and LE910-EUV2 (M7) routers. This allows interoperability for those carriers that require GSM encryption, even though the encryption is considered weak. The setting defaults to off. [SAROS-2989]
5. Updates the DHCP server to prevent the assignment of IP addresses that are defined as static lease reservations using the `mac2ip` command. [SAROS-2991]
6. Adds the ability to set an `eroute n locmsk 255.255.255.255`, allowing the IKE negotiation to use an IP address instead of a subnet. [SAROS-3002]
7. Raises the IKEv2 limit from 5 to 10 tunnels. [SAROS-3032]
8. Adds autocmd support for quotes (“). [SAROS-3044]

BUG FIXES

1. Removes the event log entry showed stated the random number entropy was too low. [SAROS-2939]
2. Corrects a defect that prevented the router from booting from an alternate image1 file, when an image1.cwe file was present. [SAROS-2990]
3. Corrects a LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) defect that was incorrectly reporting latency health metrics to the 3G data stream when the router was connected to LTE. [SAROS-2995]
4. Corrects the dial out rate for the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) routers, which caused a 70 sec rate versus 10 sec. This errantly slowed the ability of Digi SureLink recovery activities for these routers. [SAROS-3003]
5. Eliminates a potential Digi SureLink rebootfails corrective action when performing a module carrier update cycle. [SAROS-3004]
6. Removes errant event log line feeds when displaying Context 3 AT#CEERNETEXT responses and removes redundant “2964 triggered” messages. [SAROS-3006. SAROS-3007]
7. Corrects a WR11-M9 defect caused when configuring the APN using a clean 7.1.1.2 or 7.1.0.4 Flashwriter image. If no APN was written prior, an “Unable to modify profile” event log entry will occur. [SAROS-3013]
8. Corrects an OpenVPN defect that caused packet corruption when receiving out of order packets over an OpenVPN connection. [SAROS-3016]
9. Corrects a defect that resulted in a grossly incorrect ppp 1 txbytes statistic. [SAROS-3018]
10. Corrects a Web UI defect that caused various non-password fields (for example, SIM PIN and PUK) to be auto-filled in with the device password. [SAROS-3027]

11. Corrects an LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) defect that prevented DNS servers from getting configured. Intermittently, the cellular module would not get a DNS address assigned. This fix resets the modem when it detects no non-0.0.0.0 DNS address assigned. For those service plans that do not include DNS, this mechanism must be disabled. Failure to do so will result in repeatedly recycling power on the modem with an Event Log entry stating PPP 1 is down due to No DNS IP address. This fix can be disabled by setting `modemcc 0 needs_dns OFF`. [SAROS-3031]
12. Corrects the autoAPN setting for ICCID 302220* from isp.telus.iot to isp.telus.com. [SAROS-3034]
13. Corrects problems with carriers that required APNs to be written to PDN 1, which was changed to avoid problems with other carriers support for IMS. [SAROS-3039, SAROS-3042]
14. Corrects a DNS Server update defect that prevented updates when default routes were changing. [SAROS-3046]
15. Corrects a defect that prevented the all the at\mibs=gprs data fields from getting displayed. [SAROS-2900, SAROS-3047]

VERSION 7.1.2.2 (Bootloader 7.66) 15 November 2019

This is a mandatory release.

BUG FIXES

1. Corrects a defect that caused a Data Abort crash when a router receives a burst of TCP/IP connection requests. [SAROS-3058]

VERSION 7.1.2.1 (Bootloader 7.66) 20 September 2019

This is a mandatory release.

BUG FIXES

1. Corrects Cellular UL throughput on QMI-based devices (L5/MC7354, L6/LE910-NAG, L7/LE910-EUG, L8/LE910-SVG, L9/MC7430, M4/LE910C1-NS, M8/MC7455, M9/LE910C1-AP products. [SAROS-3026]

VERSION 7.1.1.2 (Bootloader 7.66) 12 July 2019

This release has a critical defect (SAROS-3026) and should not be used.

ENHANCEMENTS

1. Improves the cellular uplink speed for LE910-EU1(M3)/LE910-NA1(M6) CAT1 routers. [SAROS-2949]

BUG FIXES

1. Corrects an LE910-NAV2(M5)/LE910-NA1(M6) Verizon connectivity problem when incorrect APNs are programmed and power is lost attempting to connect to the carrier. [SAROS-2964]
2. Corrects defects in the ftp client code that incorrectly terminated FTP sessions when updating module firmware using the carrier XXX –ftp update command. [SAROS-2965]
3. Corrects invalid long code used to receive Remote Manager SMS, which prevented delivery outside North America. [SAROS-2655]
4. Corrects a defect that could prevent a command processor instance from freeing up, which eventually could block access to serial, telnet, or SSH. [SAROS-2961]
5. Corrects a defect that filtered special characters (i.e., “_”) from SMS commands, preventing commands that contained these characters (i.e., “ppp 1 deact_rq”) from remotely executing. [SAROS-2956]
6. Corrects a defect that caused the WR44 to go into a reboot cycle when greater than 200 Access Points are present. [SAROS-2679]
7. Adds a workaround that prevented completion of an OpenVPN tunnels in the case of a faulty server that drops a PUSH_REQUSET during negotiation. [SAROS-2986]
8. Corrects a defect that prevented several fields from getting rendered (e..g, Radio Technology, Signal Quality, Radio Band, Channel, Cell ID, Network, and Service Domain) during a modemstat ? command.

[SAROS-2953, SAROS-2662, SAROS-2992]
9. Corrects a defect in the SNMP 1.3.6.1.4.1.16378.10000.2.8.0 OID kept the value stuck at 0. [SAROS-2673]
10. Removes references to Transport from the UI. [SAROS-2968]

VERSION 7.1.0.5 (Bootloader 7.66) 10 May 2019

This is a mandatory release.

ENHANCEMENTS

1. Adds support for latest LE910C1-NS (M4) Sprint firmware, 25.00.246, which replaces the prior 25.00.244 firmware and includes fixes for OMA status functions, like Hands Free Activation. [SAROS-2891, NPIX-939]
2. Adds additional Digi Remote Manager Health Metrics for carrier, network, Signal strength, Signal Quality, and Signal Percent. [SAROS-2913]

SECURITY FIXES

1. Corrects the HTTPS key on the router from a fixed static key (which is the same on all routers) to a randomly generated key. Note the certificate is still a self-signed certificate, so true authentication is still questionable; however, your privacy is assured. [SAROS-2936]

BUG FIXES

1. Corrects all QMI based module handling of PDP contexts. The change will now leave the first PDP context unchanged, which some carriers use as their default bearer, and use QMI tags to access unused PDP contexts. A QMI tag will be created for any of these modemcc APN parameters (i.e., apn, apn_2, buapn or buapn_2) that are configured and used. This corrects difficulties connecting on some private networks and allows the default bearer to remain connected as needed or required by the carrier. [SAROS-2911, SAROS-2942]
2. Corrects reboot loop for WR44 routers L5 that have no Wi-Fi (e.g., WR44-L5A3-CE1-RF) support. [SAROS-2937]
3. Corrects an intermittent issue causing a command session to get locked up and lost, preventing SSH or telnet access to the router after a carrier firmware update. [SAROS-2931]
4. Corrects a defect that prevented L5/MC7354 routers from changing carrier firmware reliably. [SAROS-2954, SAROS-3037]
5. Removes unnecessary “Certificate Code Error” entries from the Event log when accessing the router over HTTPS, with Chrome version 73.0.3683.86. [SAROS-2933]
   Corrected two defects for HE910-D (U9) based routers were invalid “SIM PIN ERROR” strings were inserted on connection failures and Network Technology changes were showing LTE connectivity. [SAROS-2935, SAROS-2945]

VERSION 7.0.3.5 (Bootloader 7.66) March 2019

ENHANCEMENTS

1. Adds support for latest MC7455 (M8) firmware, 02.30.01.01, which replaces the prior 02.24.05.06 firmware for Telus and Rogers. [SAROS-2891]
2. Adds support for latest LE910-EU1 (M3) firmware, 20.00.414, which replaces the prior 20.00.413 firmware.
3. Adds support for latest LE910-EU V2 (M7) firmware, 20.00.404, which replaces the prior 20.00.403 firmware.

BUG FIXES

1. Corrects the HTTPS key on the router from a fixed static key (which is the same on all routers) to a randomly generated key. Note the certificate is still a self-signed certificate, so true authentication is

still questionable; however, your privacy is assured. [SAROS-2936]
2. Adds support for latest 20.00.005/20.00.505 LE910-NA V2 (M5) firmware, which includes a correction for future Verizon LTE Band 4 upgrades. [NPIX-954]
3. Corrects LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) handling of carriers that use IMS auto attach bearer connections, which resulted in failure to connect to private networks or the inability to obtain the expected IP address from the carrier. [SAROS-2839]
4. Corrects the LE910-EUG (L7) SMS handling, which prevented the router from receiving SMS from some carriers (like Telia and Telenor). [SAROS-2835]
5. Corrects the WR21/WR31 handling of Ethernet packets greater than 455 bytes that should have travelled between the ETH0 and ETH1 interfaces, when in HUB mode. [SAROS-2912]
6. Corrects a defect that prevented modified configuration data from being uploaded to Device Cloud. [SAROS-2822]
7. Corrects LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) handling of the carrier subnet route, which intermittently prevented packets from getting sent. [SAROS-2908]
8. Corrects a defect that prevented the at\mibs=gprs data fields from getting loaded. [SAROS-2900]
9. Corrects a defect that caused the router to reset when uploading a file from Remote Manager [SAROS-2910]
10. Corrected intermittent behaviour when updating the MC7455 (M8) module with the carrier update command. [SAROS-2903]

VERSION 7.0.2.1 (Bootloader 7.66) January 2019

BUG FIXES

1. Corrects a WR11/WR21/WR31 Ethernet lock up problem when Ethernet Buffers were almost exhausted or the RX FIFO was almost full. [SAROS-2883]

VERSION 7.0.1.3 (Bootloader 7.66) December 2018

ENHANCEMENTS

1. Adds support for latest LE910C1-AP (M9) firmware, 25.26.255, which replaces the prior Generic (25.00.251) and Telstra (25.00.252) images. Note that this firmware is incompatible to the older firmware. Under no circumstance should you try to overwrite the newer 25.26.255 firmware over the 25.00 firmware. [SAROS-2887, SAROS-2889]
2. Adds support for latest MC7455 (M8) firmware, 02.30.01.01, which replaces the prior 02.24.05.06 firmware for Verizon, Generic, and AT&T. [SAROS-2891]
3. Adds support for latest MC7430 (L9) firmware 02.30.01.01, which replaces the prior 02.24.05.06 Telstra and 02.27.01.00 Generic firmware images.

BUG FIXES

1. Corrects a RealPort defect that prevented it from remaining connected and reconnecting in the case it got disconnected. [SAROS-2886]
2. Corrects a defect that caused cloud watchdog events from disconnecting and reconnecting a router to the cloud, even though it never actually disconnected. [SAROS-2895]

VERSION 7.0.0.6 (Bootloader 7.66) November 2018

ENHANCEMENTS

1. Adds support for a Device Cloud Install Code and changes the default Device Cloud connection behavior (cloud 0 clientconn ?) for routers that have a valid install code. Routers manufactured heretofore will include a unique Install Code and require this install code to be entered when adding a router to a

Device Cloud account. The install code will be visible on the product label. Note, routers that do not have a valid install code, will not connect to Device Cloud by default. [SAROS-2847, SAROS-2799, SAROS-2850]

2. Adds the ability to automatically assign an APN for Telus IoT SIMs when no APN is configured for the LE910-NAV2 (M5), LE910-NA1 (M6), and MC7455 (M8) platforms. The algorithm will scan a list and locate matching ICCID and IMSI prefixes. When a match is found, the APN will be written to the cellular module. The following table shows the ICCID and IMSI prefixes, and the associated APN that will be assigned:

ICCID	IMSI	Assigned APN
891223	3022205370	m2mjde.telus.com
891223	3022205370	m2mjde.telus.com
891223	3022205371	m2m-east.telus.iot
891223	3022205372	m2m-east.telus.iot
891223	3022205373	m2mjde.telus.com
891223	3022205374	m2m-east.telus.iot
891223	3022205375	m2m-east.telus.iot
891223	302760000	m2m-east.telus.iot
891223	302760001	m2m-east.telus.iot
891223	3027600020	m2m-east.telus.iot
891223	3027600021	m2m-east.telus.iot
891223	3027600022	m2m-east.telus.iot
891223	3027600023	m2m-east.telus.iot
891223	3027600024	m2m-east.telus.iot
891223	302220	isp.telus.iot

   For example, if you install SIM card 89122300000000000001 with IMSI 302760002400001, if you're APN is set to none (the default setting), then m2m-east.telus.iot will be used. [SAROS-2685, SAROS-2702-SAROS-2708, SAROS-2837]

3. Adds support for WR44R Wi-Fi station DFS channels. Allows an 802.11ac Wi-Fi station to connect on DFS channels. Note this capability is only available when running as a Wi-Fi station only and will not be available when running an Access Point and station, simultaneously. [SAROS-2663]
4. Changes the Remote Manager Cloud connector watchdog to reboot the router if no default route is UP after it's watchdog timeout expires, which protects against the case when a cellular connection is down. The prior functionality only restarted the Cloud connector client. [SAROS-2816]
5. Adds support in the bootloader to ignore serial input at power up, which in some cases prevents the router from booting. [SAROS-2057]
6. Adds support for the Telit Trace Tool for the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) platforms. [SAROS-2345]
7. Changed the Factory Default state to enable HTTPS and will now always redirect traffic from HTTP to HTTPS. [SAROS-2811, SAROS-2812]
8. Adds the ability to use %m in the PPTP or L2TP Description string, which pulls in the router's MAC address. [SAROS-2026]
9. Changes the default "Allow anonymous FTP login" checkbox setting from enabled to disabled on the Configuration – System > General Web UI page. [SAROS-2806]
10. Changes the SMS International Long Code for Device Cloud from 447786201216 to 447537431797. [SAROS-2858]
11. Expands the Wi-Fi module "reset, Hardware" event Log messages to include finer granularity (e.g., Syncing Rx, Popping AMSDU, Popping Frame, Extracting AMSDU, and Restarting Core), of which none are catastrophic. [SAROS-2826]

BUG FIXES

1. Removes the GSM GEA/1 Ciphering Algorithm support from the LE910-EU1 (M3) and LE910-EUV2 (M7) modems, considered broken and no longer secure. [SAROS-2725, SAROS-2759]
2. Corrects a defect in the WR11, WR21, and WR31 power control that resulted in sporadic processor shut downs, which resulted in the router going dark: all LEDs go OFF and the router will not respond until power cycled. [SAROS-2846, SAROS-2859, WR11-244]
3. Corrects the Web Server session ID cookie and secure flag, which prevents Browser access to the web server through HTTP, once the server accesses HTTPS. [SAROS-2772]
4. Corrects a defect that prevents the WR11 LE910C1-AP (M9) module from utilizing SIMs that has their SIM PIN enabled. [SAROS-2640]
5. Corrects the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) WWAN/Service LED blink pattern, which was one short from the expected value. [SAROS-2678]

6. Corrects defects that prevent LE910-NAV2 (M5) and LE910-NA1 (M6) routers from sending or receiving SMS from the Verizon network. [SAROS-2695, SAROS-2696]
7. Corrects defects that prevent LE910C1-NS (M4) routers from sending or receiving SMS. [SAROS-2697]
8. Corrects a defect that prevents python scripts from auto-starting python when stored on an external USB Flash drive. [SAROS-2771]
9. Corrects an intermittent problem that cut off portions of files when using the update command to download information or modem firmware from the support site. [SAROS-2762]
10. Corrects LE910-NAV2 (M5) Getting Started Wizard failures when using Verizon SIMs. [SAROS-2805]
11. Corrects missing Device Cloud support for setting Open VPN routes. [SAROS-2734]
12. Corrects a defect that prevents QXDM connections on LE910-NAG (L6), LE910-EUG (L7), LE910-SVG (L8), LE910C1-NS (M4) and LE910C1-AP (M9) routers. [SAROS-2818]
13. Corrects the OSPF and BGP web UI to render the configuration file name only (instead of displaying the configuration file contents), and thus enables successful DRM import and export cycles. [SAROS-2832]
14. Corrects a defect that prevents the insertion of a message prefix or suffix into GPS forwarded NEMA data. [SAROS-2833]
15. Corrects defective behaviour that now prevents “Your.APN.goes.here” from getting written to the modem. This string is used as a place holder in the web UI to guide an operator where to enter data. Sometimes, this data can be left blank, and thus the invalid APN was errantly written, preventing cellular connectivity. [SAROS-2845]
16. Adds missing Telemetry configuration support to Digi Remote Manager. [SAROS-1863]
17. Corrects a defect on the LE910-NAV2 (M5) and LE910-NA1 (M6) platforms that prevented modemprofiles from working when operating on the Verizon network. [SAROS-2715, SAROS-2827]
18. Corrects a MODBUS defect that prevents the gateway from connecting to more than 2 MODBUS TCP slaves. [SAROS-2748]
19. Corrects a defect in the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) routing table that left out the local the cellular subnet route. [SAROS-2756]
20. Corrects a defect that prevents the Web UI from displaying files in the user directory. [SAROS-2797]
21. Corrects a Web UI defect that included the Configuration – Telemetry tab for the WR11 (which does not have Telemetry). [SAROS-2807]
22. Corrects a defect that prevented GPS location data from getting uploaded to Device Cloud and rendering device location. [SAROS-2764]
23. Corrects a defect in the “Clear PPP n Statistics” button on the Management – Network Status > Interfaces > Advanced > PPP > PPP 0-9 > PPPn Web UI page that prevented the statistics from getting cleared. [SAROS-2854]
24. Corrects a Firewall defect that prevented FTP server access from a cellular WAN-side client. [SAROS-2866]
25. Corrects the IKEv1 aggressive mode exchange to only encrypt the final hash packet when we are the IKE initiating party and not encrypt the final packet when the peer is the initiator. [SAROS-2867]

VERSION 6.1.3.8 (Bootloader 7.63) October 2018

BUG FIXES

1. Corrects an LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) defect that prevented SIMs requiring a Username and Password from successfully connecting. [SAROS-2765]
2. Corrects a defect that prevented User defined suffix and prefixes from getting inserted into IP forwarded GPS Telemetry data. [SAROS-2820, SAROS-2833]
3. Corrects a WR44 LE910-EUV2 (M7) defect that failed to write APNs if an upper case character was used in the modemcc 0 APN string. [SAROS-2823]
4. Corrects a defect with MC7455/MC7340 (M8,L9) router’s, when upgrading from prior firmware, if Auto SIM/Carrier Detect is not enabled. [SAROS-2809]

VERSION 6.1.3.7 (Bootloader 7.63) September 2018

BUG FIXES

1. Corrects a WR21/WR31 LE910-EUV2 (M7) and LE910-NAV2 (M5) defect that failed to write APNs if an upper case character was used in the modemcc 0 APN string. [SAROS-2823]
2. Corrects a WR21/WR31 problem that prevented L2 frames from being sent and DHCP address assignment when connecting devices only to LAN 1 (eth 1) and leaving LAN 0 (eth 0) unconnected. [SAROS-2781]

VERSION 6.1.3.6 (Bootloader 7.63) August 2018

BUG FIXES

1. Corrects a WR11 LE910-EU1 (M3) and LE910-NA1 (M6) defect that failed to write APNs if an upper case character was used in the modemcc 0 APN string. [SAROS-2823]
2. Corrects WR11 Ethernet issue when under severe load that caused Ethernet disconnect/connect cycling. [SAROS-2825]

VERSION 6.1.3.5 (Bootloader 7.63) July 2018

ENHANCEMENTS

1. Added a Digi Remote Manager Watchdog task that monitors the DRM client connection, as well as the low level socket connection table to ensure cloud connectivity when the cloud is enabled (cloud 0 clientconn ON). The watchdog can be disabled by setting the cloud 0 watchdog to OFF. [SAROS-2755]
2. Added GNSS support for WR31 MC7455 (M8) and MC7430 (L9), using the internal cellular module GPS. [SAROS-2744, SAROS-2774]
3. Extended the hw command to display Flash ID used. [SAROS-2743]
4. Added support for a WR44 LE910-EUV2 (M7) router. [SAROS-2721]

BUG FIXES

1. Corrected a defect related to late writing of APNs to the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7), that prevented Dual SIM failover to work properly. [SAROS-2469]
2. Corrected a defect when setting 2G, 3G, and 4G Preferred System on the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) routers. [SAROS-2735, SAROS-2738, SAROS-2758]
3. Corrected the WR21, WR31, and WR44 module power down and power up sequence that now speeds up initial cellular connections and prevents incorrect recovery during Digi SureLink recovery. [SAROS-2782, SAROS-2757]
4. Reverted SMS web page support for the LE910-EU1 (M3) and LE910-EUV2 (M7) routers. [SAROS-2718]
5. Corrected a WR44 defect that caused the SIM LED from getting relit after a Digi SureLink recovery cycle. [SAROS-2783]
6. Added a test that prevents incorrect images to be written during the Web UI Firmware Update or a Remote Manager Update Firmware process. [SAROS-1834, SAROS-2751, SAROS-1781]
7. Corrected a defect in the WR44 MC7455 (M8) and MC7430 (L9) that switched the cellular module into Low Power Airplane mode when the temperature exceeded 62C. The new trip point is now 82C. [SAROS-2788, SAROS-2800]
8. Revert LE910-EU1 (M3) and LE910-EUV2 (M7) SMS web page support that got removed in the prior release. [SAROS-2718]
9. Corrected a defect that displayed incorrect SIM Status (PIN is blocked) when SIM Card connections were momentarily disconnected. It will now say ERROR. [SAROS-2798]
10. Corrected a defect that prevented the Web Server from working over slow/narrow links, due to a failure to limit the server's maximum segment size (MSS). [SAROS-2766]
11. Corrected an Ethernet defect that prevented a VRRP enabled interface from activating and remain stuck in the INIT state. [SAROS-2796]
12. Corrected an intermittent problem that prevented LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6),

and LE910-EUV2 (M7) routers from detecting that they lost registration and would then displayed an undetectable Signal Strength and 0 RSSI value. [SAROS-2775]

VERSION 6.1.2.2 (Bootloader 7.63) May 2018

ENHANCEMENTS

1. Updates the car_7455.txt file to latest version, allowing updates for Telus, Rogers, Bell. [SAROS-2681]
2. Adds new flash support for WR44. Note when using a WR44 with this Flash type, downgrading the bootloader will be locked out. So using Flashwriter with an older version of firmware, will error out. [SAROS-2724, PCN-201]

BUG FIXES

1. Corrected a defect that prevented a firmware update via HTTPS. [SAROS-2736]
2. Corrected a defect that prevented an LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) module firmware update when flashing a router with 6.0.0.6 and then upgrading to 6.1.1.2. [SAROS-2728]
3. Corrected a defect that prevented simultaneous Wi-Fi AP and client mode from working. [SAROS-2662]
4. Corrected a defect that prevented multiple Wi-Fi APs from working. [SAROS-2671]

VERSION 6.1.1.2 (Bootloader 7.62) April 2018

ENHANCEMENTS

1. Extends the OpenVPN ovpn command to include an sslcli_add field, allowing the router to choose the specific SSL client instance. [SAROS-2687]
2. Adds wifistat output to the debug.txt [SAROS-2190]

BUG FIXES

1. Corrected a defect that prevented HE910-D (U9) routers from reattaching after an Over Temperature shutdown event. [SAROS-2609]
2. Corrected defects in the Getting Started SIM Wizard when attempting to use slot 2 as highest priority SIM. [SAROS-2288, SAROS-2639]
3. Corrected an error in the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) factory default settings for cmd 0 asyled modem from “2” to “1” [SAROS-2686]
4. Corrected a defect in the WR44 802.11N radio that mistakenly removed the WiFi station WEP security options. Note the 802.11ac radio does not include this option. [SAROS-2462]
5. Corrected a defect when Ethernet cables are removed and re-inserted, intermittently caused USB Host Controller failures that took down the cellular module. [SAROS-2701, SAROS-2711]
6. Corrected a defect when SIM failover is configured (e.g. Dual SIM wizard) but no SIM is inserted. The system will now recognize the SIM error immediately and switch to the other SIM slot. [SAROS-2022]
7. Corrected a defect in the Getting Started Wizard when no SIM was inserted into slot 1, but inserted into slot 2, the APN was erroneously being applied to slot 1 instead of slot 2. [SAROS-2288]
8. Corrected a defect in the Dual SIM Wizard when selecting SIM slot 2 as the high priority slot, where the slot 2 SIM never connects and always falls back to the slot 1 SIM. [SAROS-2639]
9. Corrected a defect in modemstat ? that left out the IMEI after a SIM switch. [SAROS-2550]
10. Corrected a cellular defect where routers that were connected and had an IP address would appear to remain connected with an IP address after executing a de-activate request (ppp 1 deact_rq).
11. Corrected a defect with the WR44 802.11ac radio that prevented scanning of WiFi channels 12 through 14. [SAROS-2688]
12. Corrected a defect with Web server session cookie, used to track an authenticated user, that caused a “medium” security vulnerability. The cookie now uses the secure flag for HTTPS connections and no longer triggers the vulnerability. [SAROS-2693]
13. Corrected a problem using asterisk (*) in the Configuration - Network > Interfaces > Ethernet > MAC

Bridging section. [SAROS-1884]
14. Corrected Web UI/Digi Remote Manager inconsistencies related to SSH servers, IP Routing settings and Routes. [SAROS-2201, SAROS-2202, SAROS-2207]
15. Corrected CLI usbcon flashkey/eflashkey versus Digi Remote Manager USB Security inconsistencies. [SAROS-2206]
16. Corrected defects that prevented registered python rci.add_rci_callback functions from receiving data through SCI do_command calls. [SAROS-2244]
17. Corrected a defect that erroneously reset the serial settings to their factory default state after a firmware update. [SAROS-2618]
18. Removed erroneous factory default setting for LE910-NA1 (M6), LE910-NAV2 (M5), LE910-EU1 (M3) and LE910-EUV2 (M7) routers. This had no effect on behavior, but misguided users on what settings to use. [SAROS-2686]
19. Corrected a defect in the Analyzer code that prevented proper encoding of NDIS cellular modules that do not use an Ethernet MAC header (i.e., MC7455/M8). [SAROS-2694]

VERSION 6.1.0.6 (Bootloader 7.62) May 2018

ENHANCEMENTS

1. Extended the python socket limit from 10 to 30 sockets. [SAROS-2661]

BUG FIXES

1. Corrected a defect that prevented the LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), and LE910-EUV2 (M7) routers from reconnecting to cellular after any momentary disconnect. They would only recover after a SureLink (Link Retry reset). [SAROS-2670]
2. Corrected a defect that prevented Username/Password protected SIM accounts from connecting using LE910-EU1 (M3), LE910-NAV2 (M5), LE910-NA1 (M6), or LE910-EUV2 (M7) routers. [SAROS-2566]
3. Corrected a defect with router access when TACACS+ service is down using local authentication, which last worked in 5.2.17.12. [SAROS-2632]
4. Corrected a defect on the Network->Virtual Private Networking (VPN)->IPSec->IPsec Tunnels->IPsec 0->Advanced Web page where the default setting of the “link tunnel with interface” can get altered if navigating away and then back. [SAROS-2617]
5. Corrected an errant Sprint WR11 LE910C1-NS (M4) Mobile Setting web page that used “Your.APN.Goes.Here” instead of “none” as the APN default. [SAROS-2664]
6. Corrected a defect where the Cellular Link Retry counter did not get cleared after establishing a successful connection. This caused modems to unnecessarily reset when SureLink protection was enabled. [SAROS-2585]
7. Corrected a defect in the VRRP Probe Priority adjustment (vprobeadj) that erroneously had values greater than 128 wrapping, so the values appeared lower in priority. [SAROS-2647]
8. Corrected a defect that used incorrect source addressing for syslog packets when setting ‘syslog 0 source_ent “eth”’. [SAROS-2659]
9. Corrected a WR31 defect that prevented the Management Telemetry GPIO UI from using the GPIO Analog/Current mode. [SAROS-2669]
10. Corrected a defect that prevented long OpenVPN digest algorithms from getting properly displayed in the OpenVPN Configuration->Virtual Private Networking (VPN)->OpenVPN->OpenVPN1 web UI. [SAROS-2504]
11. When using a Roaming SIM, cellular connections could take over 2 minutes to establish connections when using MC7455 (M8). [SAROS-2518, SAROS-2593]

VERSION 6.1.0.3 (Bootloader 7.62) January 2018

ENHANCEMENTS

1. Added support for the Sprint WR11 LE910C1-NS (M4). [SAROS-2327]
2. Added Stateful Firewall extensions for IPv6, including support for IPv6 addresses and prefixes, icmpv6-type and ICMPv6 unreachable support and IPv6 Subnet IDs. [SAROS-2428, SAROS-2530, SAROS-2531, SAROS-2533, SAROS-2535, SAROS-2536, SAROS-2541, SAROS-2541, SAROS-2542]
3. Added WR11 LE910C1-AP (M9) module download capability via the carrier command, which now has support for a GENERIC firmware (20.00.251) and a Telstra firmware (20.00.252) [SAROS-2513, SAROS-2514]
4. Optimized WR11 L6/L7/L8/M9 modemoff/modemon behavior to enable faster failover and recovery. [SAROS-2605, SAROS-2580, SAROS-2615]
5. Updated the factory default setting for link_retries (and link_retries_2) from 20 to 100 for LE910-NAG (L6), LE910-EUG (L7), and LE910-SVG (L8) Category 3 LTE modules. The value of 20 was much too low and was non-compliant with Verizon and AT&T networks. The original value of 20 could cause a SureLink modem recovery in 3 minutes, whereas now it will take closer to 17 minutes for SureLink modem recovery. This change is only observed if you factory default your modem. [SAROS-2621]

BUG FIXES

1. Addressed CVE-2008 SSH Vulnerability by configuring CBC ciphers to 0 (disabled) and added the following new CTR ciphers: AES-128-CTR, AES-192-CTR, and AES-256-CTR, with default priority 1 (enabled). Note this change could affect timing of SSH authentication. [SAROS-2612, SAROS-2650]
2. Corrected a defect where VRRP would continuously (and incorrectly) switch back and forth between the Master and Backup interfaces. [SAROS-2625]
3. Corrected Device Cloud lock ups when importing an XML configuration from an incompatible product (for example, a exporting from a WR44 with DSL into a WR44 that does not unclude DSL). [SAROS-2432, SAROS-2587]
4. Corrected IPsec VPN data stream problem when IKEv2 renegotiated SAs with Cisco ASA routers [SAROS-1990]
5. Corrected LE910 NA1 (M6) update command: “carrier all” failing due to incorrect FTP path and firmware update failures when running the Verizon image. [SAROS-2586, SAROS-2631]
6. Corrected LE910 NA V2 (M5) update command: “carrier all” failing due to incorrect FTP path. [SAROS-2592]
7. Corrected defect in Dual SIM Wizard that caused premature SIM switching (instead of retrying the same SIM) due to improper setting of the PPP pdacttries. [SAROS-2187]
8. Corrected an Ethernet defect that prevented the router from receiving any packets when fragmented IPv4 broadcast frames are present either at start up or when the Ethernet cable is plugged in. [SAROS-2648]
9. Corrected problem with OpenVPN that caused a system crash on start up. [SAROS-2643]
10. Corrected MC7354 (L5) .rom and .sbios file naming error in Flashwriter files, which broke the disaster recovery procedure. [SAROS-2643]

VERSION 6.0.0.6 (Bootloader 7.62) November 2017

ENHANCEMENTS

1. Added cellular modem support for WR11 LE910-NA1 (M6) and WR21/WR31 LE910-NAV2 (M5). [SAROS-2327]
2. Added cellular modem support for WR11 LE910C1-AP (M9). [SAROS-2327]
3. Added support for IPv6 over Ethernet interfaces. Each Ethernet interface may be configured as an IPv6 WAN interface or an IPv6 LAN interface. An IPv6 WAN interface learns prefixes, routes and DNS addresses from an upstream router’s Router Advertisement messages and DHCPv6. An IPv6 LAN interface advertises subnetted prefixes in Router Advertisement messages and assigns downstream hosts an address from this prefix via DHCPv6. [SAROS-2204]
4. Added support for MC7430 (L9) Auto SIM detection. [SAROS-2484, SAROS-2485]

5. Added support for LE910-EU1 (M3) and LE910-EUV2 (M7) Over-the-Air module firmware update via the carrier command. [SAROS-2559]
6. Extended the modemstat command for LE910-EU1 (M3) and LE910-EUV2 (M7) modules to include the "APN in Use" field. [SAROS-2428]

BUG FIXES

1. Corrected WR11 L6/L7/L8 modemoff behavior, which prevented the cellular module to re-enumerate, and prevented cellular connectivity until a system reboot [SAROS-2571]
2. Corrected the WR11/WR21 bootloader to properly set brownout power level, which corrects the power cycle failures where the cellular module would not boot and resulted in all LED's staying off. [WR11-222, WR11-233, SAROS-2600]
3. Corrected a rarely observed WR44v2 failure that occurred when sending large data blocks through an AES-128/SHA1 IPsec tunnel. The correction uses software authentication and has a significant impact to tunnel throughput. Using iperf over an Ethernet tunnel, the maximum throughput observed when sending 1200 byte TCP frames dropped from 62MBps to 40 MBps. And for 1000 byte UDP frames, either method could reach 54MBps, but CPU utilization increases from 60% to 97% when using the software authentication. [SAROS-2407]
4. Corrected modemcc Factory Default settings for LE910-EU1 (M3) and LE910-EUV2 (M7) modules. [SAROS-2515]
5. Corrected return value for the digihw.wr31_ain_get_value() to return a float instead of a long [SAROS-2258]
6. Corrected the link_retries value and system timing for the LE910-EU1 (M3) and LE910-EUV2 (M7) modules to recycle within one hour if connection failures persist. [SAROS-2477]
7. Corrected WR21/WR31 crash/reboot when using a 2048-bit key to connect to a Ubuntu OpenVPN server [SAROS-2481]
8. Corrected WR11 LE910-EU1 (M3) modemoff timing defect that knocked some routers off line until reboot [SAROS-2491]
9. Corrected defect when editing and saving the Firewall page using Chrome or Firefox over an HTTPS connection. [SAROS-2562]
10. Corrected the Mobile Preferred System Options pull down menu to match the actual system capability. [SAROS-2568, SAROS-2027]
11. Corrected an Ethernet defect that caused the WR21 to occasionally reboot when in Hub mode. [SAROS-2482]
12. Corrected defect that causes a "Bad Format" error message when clicking the Apply button on the Configuration – Network > Advanced Network Settings page. [SAROS-2573]

VERSION 5.2.19.12 (Bootloader 7.61) November 2017

SECURITY FIXES

1. Fixed a WPA security issue (KRACK) [SAROS-2565]

VERSION 5.2.19.11 (Bootloader 7.61) October 2017

BUG FIXES

1. Fixed a problem with MC7430 Firmware Update Failure [SAROS-2494]
2. Fixed a problem with Carrier switch wizard doesn't work for the MC7354 module [SAROS-2520]

VERSION 5.2.19.10 (Bootloader 7.61) September 2017

ENHANCEMENTS

1. Added support for Carrier xxx -ftp implementation [SAROS-2329]
2. Add a new check_reg setting (3) for reconnecting without modem reset [SAROS-2454]

BUG FIXES

1. Fixed a security issue where the Web Frontend has critical session information in URL [SAROS-2429]
2. Fixed a security issue where an Invalid input on FTP server causes router to crash KL-DIGI-2017-001 [SAROS-2435]
3. Fixed a security issue with an Overflow and device crash in SNMP Community String - KL-DIGI-2017-002 [SAROS-2440]
4. Fixed a security issue with an Overflow and device crash in SNMP OID - KL-DIGI-2017-003 [SAROS-2441]
5. Fixed a security issue with an Overflow buffer attack on command line with the insana command [SAROS-2442]
6. Fixed a problem where DPD is not working as expected, possibly sequence numbers wrong[SAROS-2450]
7. Fixed a problem Cloud Connector attempts to reconnect too rapidly to HTTP proxy after a failure [SAROS-2459]
8. Fixed a problem where the ppp phonenum didn't get updated when doing "carrier switch" to switch carrier [SAROS-2465]
9. Fixed a problem with SIM PIN support on the LE910 V2 modules [SAROS-2468]
10. Fixed a DNS Cache Snooping Vulnerability [SAROS-2473]
11. Fixed a problem with device descriptors on devices with Telit LE910 V2 modules [SAROS-2480]

VERSION 5.2.19.6 (Bootloader 7.61) August 2017

ENHANCEMENTS

1. Added support for MC7430 cellular module. [SAROS-2121]
2. MC7455 module firmware update. [SAROS-2125]
3. Added support for an NCM CDC USB device driver. [SAROS-2296]
4. "Carrier xxx" implementation [SAROS-2192]
5. Changed the default "modemcc 0 check_reg" value to 0 so that the device will pass Verizon LTE Data Retry Test. [SAROS-2286]
6. The SureLink wizard now sets "ppp 1 norxrst" whenever it is run. A new page has been added to ask the user if the "ppp 1 rebootfails" paramter should be set. [SAROS-2350]
7. MC7430 SIM detect carrier switch implementation. [SAROS-2193]
8. Updated LTE band values returned from QMI command. [SAROS-2449]
9. Set APN to none after carrier firmware update for sierra_lte. Updated APN to none for TELIT_3G in config.fac and config.da0. Updated AT#RFSTS value for LE910-EU1 [SAROS-2445, SAROS-2446]

BUG FIXES

1. Fixed a problem where the passthrough device would not get an IP address. [SAROS-2249]
2. Fixed a problem with Cloud Connector when an HTTP proxy sends an unavailable message. [SAROS-2367]
3. Fixed a problem where 'fleet' commands were not getting saved to config.da0. [SAROS-2355]
4. Fixed a problem where IP fragments were not being passed from the WAN-side to the passthrough device. [SAROS-2199]
5. Made a change to IPsec so that when new IPsec Sas to a peer are created, duplicate SAs to a different peer (e.g. when switching to/from a backup peer) are removed. [SAROS-2364]
6. Fixed a problem where UDP NAT wasn't working. This bug was introduced with 5.2.17.x. [SAROS-2250]
7. Fixed a problem where "ppp <x> norxrst" wasn't working on NDIS interfaces. [SAROS-2348]
8. Fixed a problem where "ppp <x> lscnt" wasn't working on NDIS interfaces. [SAROS-2349]
9. Fixed HTTP GET requests so that none of them contain the 'csrftoken' as part of the URL. [SAROS-2429]
10. Fixed a problem where an RCI import of the configuration would fail due to negative 'driftppm' ntp parameter values. [SAROS-2432]

11. Added “X-Frame-Options: SAMEORIGIN” header to HTTP responses. [SAROS-2430]
12. Improved SRAM integrity testing performed at boot time. [SAROS-2164]

VERSION 5.2.18.3 (Bootloader 7.61) May 2017

ENHANCEMENTS

1. Added support for HE910-D module firmware. [SAROS-2016]
2. The device will now download the latest ‘carriers.txt’ file when performing a modem firmware update on the MC7354 “L5” module. [SAROS-2058]
3. Increased the number of QoS queues to 45. [SAROS-2118]
4. Implemented automatic carrier switch based upon the SIM detected. [SAROS-2124]
5. Implemented Wi-Fi roaming support on the Wi-Fi client code based upon the signal strength of the connection. [SAROS-2126]
6. Added MC7455 ODIS DHIR support. [SAROS-2129]
7. Added QoS feature to update IP packet DSCP values based upon the measure throughput. [SAROS-2135]
8. Made a change to automatically update SIERRA_3G configurations to SIERRA_LTE. [SAROS-2136]
9. Added support for diffie-hellman-group-exchange-sha256 into the SSH server. [SAROS-2140]
10. Added support for “nand” utility commands. [SAROS-2154]

BUG FIXES

1. Fixed performance problems with the 802.11ac support. [SAROS-2096]
2. Fixed a problem where IO exceptions would occur if multiple python scripts attempted to write to FLASH files at the same time. [SAROS-1769]
3. Fixed a problem where Wi-Fi clients would not reconnect after being disconnected using the ‘Disconnect’ button on the web GUI. [SAROS-1810]
4. Fixed a problem where the incorrect data limit values were getting submitted to the device if the original values were in the MB or GB range. [SAROS-1859]
5. Changed the default hotspot page so that the logo image link points to “logo.png”. [SAROS-1873]
6. Made a change so that RCI descriptors support 10 ASY ports rather than 9. [SAROS-1876]
7. Made a change to the way general purpose sockets are displayed on remote Manager. [SAROS-2006]
8. Made a change so that after powerup the GPIO pullup values displayed using the “gpio diopullup” command reflect the actual pullup states (pullups enabled). [SAROS-2039]
9. Made some changes to improve TCP sequence number manipulation of FTP control socket streams when NAT is performed on the stream and when TCP retransmissions occur. [SAROS-2100]
10. Fixed a problem in the bootloader where it would allow files to be created where the filename length exceeded the limit. The bootloader will now return with an error in that case. [SAROS-2102]
11. Made some changes to fix potential buffer overruns if long filenames are specified in ‘xmodem’ commands. Made a change so that an ERROR response is returned if the xmodem file fails to open. [SAROS-2103]
12. Added SHA256 and DH group 14 into the IKE, IKEv2 and eroute RCI parameters. This was done to fix a problem where these properties could not be changed via RCI. [SAROS-2150]
13. Fixed a problem on WR44v2 devices with .ac radios installed where data transfer would break in clients ‘n’ mode connections. [SAROS-2152]
14. Fixed a problem where a Remote Manager refresh operation would fail if an eroute [x] dhgroup parameter was set to 5. [SAROS-2153]
15. Fixed a problem on WR44v2 devices with .ac radio installed. There was a problem when configured as a Wi-Fi client with intermittent slow handover when under load. [SAROS-2159]
16. Fixed a problem on WR44v2 devices where packets with non-matching destination MAC addresses would sometimes get forwarded up the stack. [SAROS-2166]
17. Fixed a problem where the analyser trace wouldn’t decode certain Wi-Fi frames if they contained an LLC/SNAP header. [SAROS-2172]
18. CWE files added to MC7354 .all files. [SAROS-2185]

19. Fixed a problem where the FTP client would fail to download
20. Fixed a problem with the MPN200 cellular regularly disconnecting from the USB bus (SAROS-2235)

VERSION 5.2.17.10 (Bootloader 7.59) January 2017

ENHANCEMENTS

1. Modified RCI support so that 'e' passwords may be set using profile manager. [SAROS-1749]
2. Added events into the eventlog when files are uploaded or downloaded using Remote Manager. [SAROS-1695]
3. Added support for SHA256 and Diffie Hellman group 14 into Ipsec. [SAROS-1996]
4. Made a change to the web server and RADIUS client so that it will send a "cmd*" AVP to the RADIUS server when authenticating HTTP requests, allowing the device to work with Cisco ACS servers. [SAROS-1886]
5. Added support for SHA256 into the SSH server. [SAROS-1894]
6. Added support for SHA256 into the SSH client. [SAROS-2029]
7. Added support for 802.11ac Wi-FI on the WR44 and WR44RR. [SAROS-1910]

BUG FIXES

1. Fixed a problem where some status menu items were not displaying on the Device Cloud menu. [SAROS-1752]
2. Fixed a problem where the cloud connector code would not always honor the reconnect wait time before establishing a connection to Device Cloud. [SAROS-2028]
3. Fixed a problem where the WR31 would crash when updating the firmware using a .all file loaded onto a USB FLASH stick. [SAROS-2000]
4. Fixed a problem in the EHCI USB driver which could result in a crash during firmware update of the Telit DE901D cellular module. [SAROS-2030]
5. Fixed a problem in the Getting Started wizard where the user would be prompted for a WPA password after configuring the device to use Enterprise mode authentication. [SAROS-2053]

VERSION 5.2.16.8 (Bootloader 7.58) December 2016

ENHANCEMENTS

1. Updated OpenSSL code to version 1.0.2h. This includes adding support for TLS1.1 and TLS1.2 [SAROS-1787]
2. Improved entropy gathering on platforms with HRNG [SAROS-1505]
3. SSL/TLS session renegotiation has been disabled [SAROS-1663]
4. Added support for the IPv4 address ID type into IKEv2 [SAROS-1669]
5. Made a change so that the device will spend up to 5 minutes after power up to get the time from the time server via SNTP. After that, the SNTP client will return to normal [SAROS-1760]
6. Made a change to the Getting Started wizard so that the user is prompted to save the configuration if there is an error during the cellular setup phase. The user will also be prompted to reboot the device (to restore previous settings) if they choose not to save the configuration [SAROS-1843]
7. Removed the tiles that display real time information from the device from the web login page [SAROS-1854]
8. Made a change so that port forwarding on an interface will work if the interface's NAT setting is set to NAT or NAPT. Previously, the setting needed to be set to NAPT for port forwarding to work [SAROS-1969]
9. A number of insecure ciphers and authentication algorithms have been removed [SAROS-1575]
10. Increased the maximum number of DHCP static lease reservations to 128 [SAROS-1616]
11. The device will now reboot if the USB memory heap is depleted. Added a new power up reason that indicates if the device rebooted due to a USB memory shortage. Added The "busb mem" command to debug.txt [SAROS-1666]
12. Added an option to the Backup/Restore web page to include debug.txt in the backup zip file [SAROS-

1713]
13. Added support for SHA256 into SCEP certificate request signatures. It is now possible to generate keys up to 3072 bits [SAROS-1895]
14. The build date embedded into firmware images is now included as a candiate for the initial time setting on devices that don't have a RTC installed [SAROS-1959]
15. Added support for the Sierra Wireless MC7455 cellular module [SAROS-1913]
16. Support for the obsolete Sierra Wireless 3G cellular modules has been removed [SAROS-1965]

BUG FIXES

1. Fixed an issue where the 'Connect' button displayed after doing a Wi-Fi network scan on the WEB GUI wouldn't work unless the AP security was set to 'None' [SAROS-1598]
2. Fixed an issue where the Device Cloud health metrics timestamps were incorrect due to the local time offset not being taken into account [SAROS-1625]
3. Fixed an issue where it was not possible to insert or edit firewall rules via the WEB GUI when using Firefox browsers [SAROS-1659]
4. Fixed an issue where the web GUI was displaying the incorrect text in the menu header link when the Configuration → Telemetry menu item was clicked [SAROS-1748]
5. Fixed an issue where a configuration import via the Device Cloud would fail with WR41v2 devices [SAROS-1754]
6. Fixed an issue where the Getting Started wizard would fail if using a SIM with PIN [SAROS-1761]
7. Fixed an issue where the firewall hit counters displayed on the web GUI were not refreshing [SAROS-1833]
8. Made a change so that both HTTP GET and POST requests check the CSRF token. Previously, the CSRF token was only checked on POST requests [SAROS-1839]
9. Fixed an issue where setting various 'metrics' parameter values would cause memory corruption [SAROS-1850]
10. Changed the thermal protection temperature threshold values for the ME909-501 cellular module to +85C (warning) and +100C (cut-off) [SAROS-1851]
11. Changed the thermal protection temperature threshold values for the Gobi 3K cellular module to +70C (warning) and +85C (cut-off) [SAROS-1624]
12. Changed the Getting Started wizard so that configuration changes are applied before the cellular interface connection is established so that the interface's 'nocfg' parameter value is applied [SAROS-1852]
13. Fixed some SNMP issues relating to the display of some cellular MIB variables [SAROS-1889]
14. Fix an issue where RIP advertised routes were not appearing in the routing table after an interface returns from the OOS state [SAROS-1905]
15. Fixed an issue where the Getting Started wizard would fail on devices with a MC7455 cellular module installed because the device would fail to detect the SIM [SAROS-1984]
16. Fixed an issue where devices with an MC7455 cellular module installed would fail to connect after updating the Verizon firmware [SAROS-1986]
17. The position of the 'Socket ID' field on the MultiTX configuration web page has been moved so that it is below the 'Send socket ID' field [SAROS-1738]
18. The MAC bridge configuration web page has been altered so that it will accept hostnames rather than just IP addresses [SAROS-1797]
19. Fixed problem where the router would reboot due to a USB memory shortage when transmitting large volumes of data over the cellular interface (SAROS-2005)
20. Fixed a problem where HTTPS wasn't working (SAROS-2041)

VERSION 5.2.15.6 (Bootloader 7.58) July 2016

BUG FIXES

1. With the 5.2.14.5 release, the firmware update on the WR41v2 via Remote Manager is hanging at 99% and does not complete. The firmware update can be cancelled and no files will have been updated.

Firmware update on the WR41v2 using the Web GUI is working. The firmware update on all other WR platforms is working via Remote Manager and the Web GUI. [SAROS-1856].

VERSION 5.2.15.4 (Bootloader 7.56) June 2016

ENHANCEMENTS

1. Added support for the MC7330 cellular modem [SAROS-1874]
2. Update Digi Remote Manager server URL and timeserver URL [SAROS-1778]
3. Various SNMP and MIB enhancements [SAROS-1740]
4. Create RSRP and RSRQ values as part of the CLI at\mibs=gprs.0.stats [SAROS-1808]

BUG FIXES

1. Fixed an issue that resulted in the Sprint PRL update to fail on the Telit DE910-DUAL modem [SAROS-1822]
2. Fixed an issue where the WR11 DE910-DUAL downloads the wrong firmware from the Digi ftp-site [SAROS-1867]
3. Fixed an issue that resulted in the Telit HE910-D modem update to fail [SAROS-1739]
4. Fixed an issue where MC7354 with static VZW SIM fails for 3G PSYS [SAROS-1862]
5. Fixed a cosmetic text issue in IPsec Advanced area of web interface [SAROS-1812]
6. Fixed an issue where DynDNS has no interface set by default [SAROS-1813]
7. Fixed an issue where SSH was not be able to disabled from Web UI [SAROS-1842]
8. Fixed “Invalid XML response” when SNTP enabled on services web page [SAROS-1849]
9. Fixed an issue where the firmware update on the WR44V2 does not work via Device Cloud [SAROS-1869]
10. Fixed an issue where the Getting Started Wizard was always displayed [SAROS-1864]

VERSION 5.2.14.5 (Bootloader 7.56) May 2016

BUG FIXES

1. The Getting Started Wizard has been updated to fix a problem when attempting to bring up a connection using a SIM with SIM PIN. (SAROS-1841)
2. ADDP has been disabled by default in the factory default configuration as having ADDP enabled is considered a security risk. (SAROS-1838)
3. A bug with the management access control over Ethernet, Cellular (PPP) and Wi-Fi interfaces has been resolved. (SAROS-1837)
4. The CLI commands “memget” and “memset” have been removed the CLI. (SAROS-1836)
5. The Remote Manager support has been updated so that the device can authenticate the Device Cloud server certificate. To do this, the public Device Cloud CA certificate should be loaded onto the device and the SSL certification validation enabled using the CLI command “sslicli 0 verify 10”. The CA certificate is included in the 5.2.14.5 update ZIP file. As *.pem files are have now allowed in firmware update files up to this release, the firmware update will need to be done twice to get the CA certificate file (cadc.pem) onto the device. (SAROS-1832)
6. An issue with the Web server authentication has been resolved. (SAROS-1832)
7. An issue with the Web server authentication has been resolved. (SAROS-1831)
8. An issue when using TCP over IPsec tunnels with an interface MTU set to below 1500 could result in an invalid MSS value has been resolved. (SAROS-1802)
9. The OpenVPN support has been updated to resolve an issue when running TCP mode could sometimes result in a crash. (SAROS-1794)

VERSION 5.2.14.3 (Bootloader 7.56) March 2016

ENHANCEMENTS

1. The WR31 GPIO support have been enhanced as follows:
    - The analog and digital GPIO can be configured via the Web page “Configuration > Telemetry > GPIO”.
    - The analog and digital GPIO can be configured and saved using a new CLI command called “wr31gpio”.
    - The analog and digital GPIO status is available on the Web GUI via the Web page “Management > Telemetry > GPIO”.
    - The analog and digital GPIO status is available on the Web GUI home page by selecting the GPIO tile.
    - The analog and digital GPIO status can be forwarded to up to two IP hosts at a configurable interval.
    - (SAROS-1765, SAROS-1766, SAROS-1767)
2. The Remote Manager server has been updated to be “my.devicecloud.com”. (SAROS-1778)
3. The Getting Started Wizard has been updated to allow the user to enable or disable the Health Metrics on the Remote Manager page. The Health Metrics are enabled by default. (SAROS-1688)
4. The Web GUI look and feel has been updated to use darker colors on the menu items and to non-Google fonts. (SAROS-1762)
5. The DHCP server support has been updated to remove some unnecessary padding to reduce

BUG FIXES

1. An issue with self-signed certificates being incorrectly accepted has been resolved. A copy of the self-signed certificates needs to be loaded onto the device before it will be accepted now. (SAROS-1785)
2. The Wi-Fi probing support when in client mode has been updated to prevent corruption on the serial ports. (SAROS-1771)
3. An issue with IKEv2 not negotiating Dead Peer Detection (DPD) has been resolved. (SAROS-1548)
4. An issue where the APN configured in the factory default configuration file (config.fac) not being used when factory defaulting a unit has been resolved. This bug was introduced in the 5.2.10.7 release. (SAROS-1683)
5. An issue with firewall NAT support that was introduced in the 5.2.13.4 release has been resolved. (SAROS- 1798)
6. The network services configuration has been added to the Remote Manager support. (SAROS-1796)
7. The Ethernet driver has been updated to remove an extra byte padding for packets that were an odd length. (SAROS-1795)
8. An issue with initialising the Remote Manager support in the Getting Started Wizard has been resolved. (SAROS-1791)
9. An issue with the DHCP server where the configured custom options where not being sent has been resolved. (SAROS-1789)
10. An issue with Python digihw.wr31_dio_get_value function not working correctly has been resolved. (SAROS-1788)
11. The Web GUI has been updated to include the timeband configuration. (SAROS-1784)
12. An issue with the IKE Nat-Traversal configuration on the Remote Manager has been resolved. (SAROS-1758)
13. The SNMP Traps MIB has been updated to match the current event list. Also a SNMP Notification MIB has also been created. (SAROS-1746)
14. An issue with the SMS messages being sent using the MC7354 module not using IMS when connected to an LTE network has been resolved. (SAROS-1737)
15. An issue with the Web GUI home page interface tile not indicating the cellular interface is up when using the Telit DE910 and Cellient CDMA 450MHz modules has been resolved. (SAROS-1735)
16. An issue with the “Disconnect” button on the Wi-Fi status web page not disconnecting users have been resolved. (SAROS-1717)
17. The modemstat command has been updated to fix a problem with the “Preferred System” status which was always displaying “Auto”. (SAROS-1704)
18. The support for the MC7354 cellular module has been updated to fix an issue with locking a particular

the radio technology. (SAROS-1680)

19. The “cellular module reboot” event has been updated to make it less confusing with a device reboot event. (SAROS-1799)