

Rugged Operating System v3.9.1 Release Notes

May 18, 2011

Copyright © 2011 RuggedCom Inc.

Overview

ROS® v3.9.1 adds new features and fixes some issues found in previous versions.

This firmware release supports all RuggedSwitch® and RuggedServer™ product series.

For the RMC30 model:

- File name: "ROS-CF52_Main_RMC30_v3-9-1.zb"
- Build date: May 18 2011 09:36 File Size: 662281

For all other RuggedSwitch®, RuggedServer™ and RP110 models:

- File name: "ROS-CF52_Main_v3-9-1.zb"
- Build date: May 18 2011 09:26 File Size: 1118017

User Guides

All user Guides are available from the RuggedCom Web site at www.RuggedCom.com.

! ATTENTION !

Starting with the ROS® v3.9.1 release, the RMC30 product model requires an upgrade file, which is specific to the RMC30 model. This compressed executable file is identified as: <ROS-CF52_Main_RMC30_v3-9-1.zb>.

All other models belonging to the RuggedSwitch® and RuggedServer™ product series will continue to be upgraded with a common compressed executable file identified as: <ROS-CF52_Main_v3-9-1.zb>.

Changes In v3.9.1 (4087)**LLDP announces ifName type with ifAlias info**

Type: Major
Products: All except RMC30 and RP110
ID: 4088

Device sends LLDP Port ID TLV with Port ID subtype equal to Interface Name (ifName), but actual Port ID is retrieving value of the object ifAlias. This is a major problem because RuggedNMS cannot identify the links between devices.

Changes In v3.9.0 (2690)

IEEE1588: Support of Boundary Clock

Type: New feature
Products: RSG2288
ID: 3703

There exist applications or locations where a GPS clock source cannot be justified due to the cost. In these scenarios a clock signal needs to be provided via the WAN and this may be realized by the Precision-Time-Protocol (PTP) Boundary Clock.

The PTP Boundary Clock can be described as a IEEE1588 gateway. The Boundary Clock translates the PTP messages between PTP regions, which may be implementing different transport and messaging protocols, or different PTP profiles. A typical deployment is the Boundary Clock for example acting as a timing sink (i.e. PTP Slave) from a Telecom network, and providing a timing distribution source (i.e. PTP master) within a power substation environment.

Support for Copper SFP

Type: New feature
Products: RS900G, RSG2100, RSG2200, RSG2300
ID: 2987

This version of firmware supports Delta's LCP-1250RJ3SR-L (Copper SFP with Rx-LOS). Supported speeds are 1000Mbps and 100Mbps.

SNMP support for serial ports

Type: New feature
Products: RuggedServer
ID: 2151

Improved monitoring support for RS232-like-interfaces MIB and propitiatory MIB for serial ports and protocols. Serial interfaces are supported via the interfaces MIB as well.

SNMP support for Link Aggregation

Type: New feature
Products: All except RS400, RMC30, RP110 and RS8000/RS1600 family
ID: 2754

Support for Link Aggregation via SNMP makes aggregated links and their states available for presentation on the graphical map on our RuggedNMS™. The standard 802.3ab defines LAG-MIB. Our implementation support manual configuration of aggregated ports.

Support for additional RFC 3580 attributes

Type: New feature
Products: All except RS400, RMC30 and RP110
ID: 3130

The following (new) attributes are supported when a Radius server is involved in Port authorization and authentication:

- Tunnel Attributes (for VLAN assignment from RADIUS Server),
- NAS-Port, Calling-Station-Id (sent in access-request),
- Attributes Session Timeout and Termination Action support (related to 802.1x)

Support for RP110 product model

Type: New feature
Products: RP110
ID: 2689

The (new) RP110 is a product which serves as a serial/ethernet media-converter providing two serial ports and Power-Over-Ethernet (PoE) capabilities. This firmware supports the RP100 model.

Support for ‘MAC Authentication Bypass’ mode

Type: New feature
Products: All except RS400, RMC30 and RP110
ID: 2768

A ‘MAC authentication bypass’ mode is an alternative to 802.1X port-security, that similarly controls network access to devices (such as printers and IP phones) which do not otherwise have the 802.1X supplicant capability. The ‘MAC authentication bypass’ utilizes the MAC address of the connecting device in conjunction with remote authentication (Radius) to permit or deny network access.

Support for RS900GP (RS900G+PoE) product model

Type: New feature
Products: RS900GP
ID: 2985

The (new) RS900GP is a product which extends the capabilities of the RS900G model by adding 8-port Power-Over-Ethernet (PoE) capabilities. The RS900GP provides the same port density and network capabilities as the RS900G and supports the same options on ports 9 and 10. This firmware supports the RS900GP model.

“Unknown unicast” flood blocking

Type: New feature
Products: All except RMC30 and RP110
ID: 3427

This feature allows the user to optionally disable “unknown unicast” traffic forwarding over specified ports. Note that the feature cannot be enabled on secure ports.

The implementation uses this rule to control “unknown unicast” forwarding: Unknown unicast egress is allowed if the port is “non-secure” AND Unknown-Unicast Flood is enabled on the port.

A “DNP aware” Raw Socket

Type: New feature
Products: RuggedServer
ID: 2973

This feature extends the RuggedServer™ functionality to add an encapsulation which is somewhere between the existing “DNP3 protocol” mode and the existing pure “raw socket” mode. Another way of describing the operation is to say that it provides a Raw Socket type protocol encapsulation that is packetizing per the DNP protocol packetization rules. The implementation recognizes DNP packets on the serial line and uses this as a trigger to transmit the packet out using the TCP/UDP transport.

SNMP support for PoE products

Type: New feature
Products: All with PoE ports
ID: 3814

SNMP support added for PoE ports monitoring.

Support for Syslog.txt flash file rotation

Type: Enhancement
Products: All
ID: 2216

The <syslog.txt> flash file contains logs of important system runtime information. Since the file size is limited due to flash hardware capacity, only a limited number of log entries can be stored within the file. In previous ROS® versions, whenever the file reached its maximum size the logging was stopped until the user manually clears old logs. The new feature is now implemented to automatically clear the oldest log entries to make room for new logs if the file has reached its maximum size.

IEEE1588: Improvement in Clock Accuracy presentation

Type: Enhancement
Products: RS416v2, RSG2288
ID: 2857

In the previous version of ROS® clock accuracy was the reflection of clock accuracy enumeration defined within the IEEE1588-2008 table 6. This enhancement presents the same information in a more user friendly format.

IEEE1588: Control over participation of clock in BMC election

Type: Enhancement
Products: RS416v2, RSG2288
ID: 2858

With this feature, the user is able to enable/disable participation of the PTP clock in “Best-Master-Clock” (BMC) election by configuring a newly introduced attribute called “Slave-Only” clock.

IEEE1588: Transparent Clocks should forward unknown PTP messages

Type: Enhancement
Products: RSG2288
ID: 3428

In older firmware versions the Transparent Clock (TC) feature discards any PTP message which is not defined within the IEEE1588-2008 standard. This behavior may create problems for proprietary Master and Slave extensions which are transparent to the TC. This enhancement forwards undefined PTPv2 messages instead of discarding them.

Static MAC address-based authorization should use wildcards to authorize a range of MAC addresses

Type: Enhancement
Products: All except RMC30 and RP110
ID: 3584

Static MAC address-based authorization can use wildcards to authorize a range of MAC addresses. This permits the user to enter the manufacturer portion of the MAC address and thus allow/restrict access to the switch ports, to specific manufacturer's devices.

WLAN: Usage of special characters in the passphrase

Type: Enhancement
Products: All supporting WLAN
ID: 3828

Usage of special characters like "\$", "@" and "?" in the IEEE 802.11g WLAN passphrase was not supported in previous version. This enhancement allows user to use special characters in the WLAN passphrase.

RSTP “Fast Root Failover” should be plug-and-play

Type: Enhancement
Products: All except RMC30 and RP110
ID: 2926

The “Fast Root Failover” feature is an excellent solution for improving the performance of the root-bridge failure scenario. To avoid possible mis-configuration of the parameter attribute, it is now “plug-and-play”.

- default setting is ON (enabled)

- when the root-bridge fails, any operational edge port will not change its status (i.e. RSTP will keep running without restarting the port), so that the failover time observed on the port will be same as on other non-edge ports. The user does not need to configure the "Edge" parameter to "True", or to disable the RSTP on that port for fast root failover, but it should remain at the default value which is “Auto”.

Expected privilege levels should be configurable for each user profile (TACACS+)

Type: Enhancement
Products: All
ID: 2971

Configuration option is added to allow the user to configure a number of (non default), or a range for each user type (Admin, Guest, Operator). The received authorization from TACACS+ server is then compared against the value(s) configured on the device and based upon this the user is assigned the appropriate authorizations.

Alarm and Safe Fail Relay contact state should be accessible by Modbus management

Type: Enhancement
Products: All
ID: 3581

Two points are added to monitor device status via Modbus management:

- Fail Safe Relay status (energized – 1, de-energized -2)
- Indication that at least one alarm in the Alarm Table is ERROR, Alert or CRITICAL level

Topology Change trap must reflect stable network topology

Type: Enhancement
Products: All except RMC30 and RP110
ID: 2739

A (new) topology-change trap (rcRstpNewTopology) is defined in the proprietary MIB (RUGGEDCOM-STP-MIB). This trap is generated after a topology change is detected on one port and a stable topology is insured on all ports.

Configurable “hold down” timer to shut down flapping Ethernet ports

Type: Enhancement
Products: All except RMC30 and RP110
ID: 2996

A (new) parameter Link Detection Time is added to the Link Detection table. It allows the user to configure the time within which the Link that is changing state from ‘down’ to ‘up’ (i.e. flapping) must be stable in order to detect active link.

Configuration of multiple SNMP trap receivers with same community string and IP address checking of incoming request

Type: Enhancement
Products: All
ID: 2997

Community string has been added to the user table to be able to add users with the same community name but assigned with different IP addresses. This simply means that multiple users can be now configured with the same community name on different management stations.

For security reasons the source address of the incoming SNMP request is checked and if the user/community address is configured with that address (or if the field value is left empty), then the request will be served. Any requests matching the user/community string with an IP address that is not assigned to the user in the table will be discarded.

Classification of ROS® based devices in the RuggedCom MIBs is updated

Type: Enhancement
Products: All
ID: 3121

The classification of ROS® based devices will be based on the core functionality of the product. Note that a device may have one or more of these properties and thus the order of precedence in classifying the device is:

- 1) RuggedAir
- 2) RuggedServer
- 3) RuggedSwitch

All SNMP Trap/Notification variable bindings now contain 'sysObjectID'

Type: Enhancement
Products: All except RMC30 and RP110
ID: 3233

It is very useful for any NMS to know from which device type a trap/notification is coming. The 'sysObjectID' identifies RuggedCom as a vendor of a specific device type, so it is now included in the variable binding of every trap/notification being generated from RuggedCom devices.

Agent Capabilities statements have been reorganized

Type: Enhancement
Products: All
ID: 3848

In a (new) organization of Agent Capabilities, each supported MIB is accompanied with MIB containing its agent capabilities statement. One MIB might have more than one Agent Capabilities statements if different products support different groups of objects. susORTable retrieves all the entries that specific product supports.

Switch sometimes crashes in mesh topology when RSTP root-bridge fails

Type: Critical
Products: All except RMC30 and RP110
ID: 3865

The problem occurs when the "Transmit Count" setting is set to a very high number (including the value 'unlimited'). Because of this the neighbor switches become very busy endlessly processing received BPDU frames upon a root-bridge failure. A critical software process indefinitely blocks other lower priority tasks and eventually the switches get rebooted by the software watchdog mechanism after one minute. This problem has been fixed.

Time Difference found monitoring Master and Slave

Type: Major
Products: RSG2288
ID: 3711

Two or three seconds of time difference is displayed between the Master and Slave in the 'Time and Data' table as the table was not updated on the Master to reflect the correct time signals in the time keeper. This problem has been fixed.

DUT keeps the old IP address even if the IP address Pool is changed in the DHCP Server

Type: Major
Products: All
ID: 2888

Upon the expiration of the DHCP Lease, the DUT keeps the old IP address even if the IP address Pool is changed at the DHCP Server. This problem has been fixed.

System performance is improved for GMRP when a large number of VLANs are configured

Type: Major
Products: All except RMC30 and RP110
ID: 3388

It was found with many VLANs configured GMRP is very slow and the device may stop responding to ping (requests). Under the same conditions the user-interface (UI) responsiveness may be very poor. This problem has been fixed.

The unit may crash if polled via multiple Modbus management connections

Type: Major
Products: RuggedServer
ID: 3747

A unit which is polled via multiple Modbus management connections sometimes crashes due to bug caused by a dead mutex lock. This problem has been fixed.

TelnetComPort protocol crashes due to mutex deadlock

Type: Major
Products: RuggedServer
ID: 3840

A unit running TelnetComPort sometimes crashes due to a bug caused by a cross-locked mutex between two tasks. This problem has been fixed.

IEEE1588 failed to converge when announce interval configured as 16 and 32

Type: Minor
Products: RSG2288
ID: 3799

The BMC failed to converge when the announce interval is configured as 16 and 32 seconds. The problem was located in the setting of timers within BMC (Best Master Clock) algorithm. This problem has been fixed.

SFP information may not be properly displayed under Port Status screen

Type: Minor
Products: RSG2100, RSG2200, RS900G,
ID: 2059

Due to inconsistencies in SFP datasheets with slightly differing information, our ROS® firmware was not resolving the differences and to correctly report the SFP supported distance for all SFP modules. This problem has been fixed.

Auto negotiation on gigabit fiber is not working properly

Type: Minor
Products: RuggedSwitch
ID: 2393

Link partners can not communicate with each other when Auto Negotiation is turned off on one side of 1000Base-X. Therefore according to standard IEEE802.3, it should not be possible to disable Auto Negotiation on 1000Base-X link. This problem has been fixed.

A unit running MSTP becomes unreachable when set to VLAN 'unaware' mode

Type: Minor
Products: All except RMC30 and RP110
ID: 3110

A unit with 255 static VLANs may become unreachable after the VLAN awareness parameter value was changed to 'unaware'. As it does not make any sense to configure MSTP and VLAN 'unaware' mode, this combination is not allowed. Switching to VLAN 'unaware' mode will automatically set Spanning Tree to RSTP. This problem has been fixed.

IP address assigned by DHCP server is still used after lease time expired

Type: Minor
Products: All
ID: 3803

The RuggedSwitch™ still retains the old IP address assigned by DHCP server after the lease has expired and there was not a renewal of the address. This problem has been fixed.

RawSocket running on management VLAN was not updated by dynamically obtained management IP address

Type: Minor
Products: All
ID: 3853

The RawSocket local interface has to be configured manually even in the case when the IP address is obtained dynamically via DHCP or BOOTP protocol. The Management address IP was not updated in that case. This problem has been fixed.

Changing a working DHCP interface to Static creates a crashlog

Type: Minor
Products: All
ID: 3889

When a properly working DHCP Mgmt IP address is changed to static address, a (nuisance) crashlog entry of ALERT level is created. This problem has been fixed.

IGMP and GMRP traffic blocks upon breaking an aggregated link

Type: Minor
Products: All except RS400, RMC30, RP110 and RS8000/RS1600 family
ID: 2881

If the primary link is broken, traffic is temporarily blocked on the secondary link. The Filtering table does not show Join/Router ports properly. After 1 query interval all traffic resumes. All the ports in an aggregated link were not properly added to the flooding ports list where that multicast traffic should be forwarded upon link failure. This problem has been fixed.

Multicast group learned from GMRP never ages out, if it was also learned from IGMP

Type: Minor
Products: All except RMC30 and RP110
ID: 3161

A Multicast group learned by GMRP and IGMP will never age out for GMRP. GMRP join messages are propagated by the DUT even after the subscriber has stopped requesting. This problem has been fixed.

Ports 2 - 16 not working when upgrading RS1600 from v3.1.4 to v3.8.2

Type: Minor
Products: RS1600
ID: 3341

When the RS1600 is upgraded from ROS 3.1.4 to the latest release of ROS 3.8.2 all the ports except for port 1 stops communicating. This problem has been fixed.

RSTP failover time is “very long” if GVRP is enabled and many VLANs are configured

Type: Minor
Products: All except RMC30 and RP110
ID: 3558

If GVRP is enabled on a switch port and there are many VLANs configured on the adjacent switches, the Fail over time measured is “very long”. This problem has been fixed.

Static MAC Address Table accepts configuration of switch port's MAC address

Type: Minor
Products: All except RMC30 and RP110
ID: 3705

Configuration of MAC address that are "reserved" for the device itself was allowed in static MAC address table. The device's own MAC address includes either the device's "global" MAC address (used for the management IP interface) or one of the switch ports' unique MAC addresses (used as a source MAC address by some Layer 2 control protocols like RSTP). This problem has been fixed.

Incorrect entry is logged to <syslog.txt> file upon unsuccessful login when RADIUS server is used

Type: Minor
Products: All
ID: 3716

If the username or the password was incorrect while logging to the device via a Radius server configured for authentication, "Radius server is unreachable" was logged to the syslog.txt, even when the Radius server is reachable. This problem has been fixed.

GMRP Dynamic port not shown properly on aggregated links

Type: Minor
Products: All except RS400, RMC30, RP110 and RS8000/RS1600 family
ID: 3727

The GMRP Dynamic port is properly identified on aggregated links after breaking and restoring the primary link. Only the secondary port is displayed as GMRP Dynamic. This problem has been fixed.

The <Syslog.txt> needs to be rotated after flash memory is exhausted

Type: Minor
Products: All
ID: 2216

When the <syslog.txt> file is full, no new entries were logged until the logs were cleared. Information that could be of importance for troubleshooting was lost. This problem has been fixed.

The SD card is not updated with new binary loaded to the i80x device

Type: Minor
Products: i80x
ID: 2469

The device still runs the original firmware if the firmware was upgraded and followed by a quick reset. The SD card was not updated upon firmware upgrade. This problem has been fixed.

TelnetComport protocol does not work with Tactical SerialIp redirector

Type: Minor
Products: RuggedServer
ID: 2887

When break signal is received from the network, it has not been passed to the serial port. This problem has been fixed.

Non-router multicast producer may potentially be flooded

Type: Minor
Products: All except RMC30 and RP110
ID: 3213

In the IGMP implementation, all multicast producers were treated as routers. Thus the producer would receive all multicast traffic. This will flood the producer unnecessarily if it is not actually a router. This problem has been fixed.

Device reboots continuously logging long syslog.txt entries

Type: Minor
Products: i80x
ID: 3458

The unit may crash while logging the difference found in <config.csv> and i80x SD card. The logged message was longer than 270 bytes, which was a limitation for the <syslog.txt> entry. The entry is now truncated to the limitation value. This problem has been fixed.

TelnetComPort protocol crashes due to mutex deadlock

Type: Minor
Products: RuggedServer
ID: 3840

A crash in device is caused by cross-locked mutex between two tasks. This problem has been fixed.

TimeDate configuration not converted after upgrade from ROSv3.3.6

Type: Minor
Products: All except RMC30 and RP110
ID: 3705

This problem has been fixed.

STP events alarm do not generate trap and Alarm Table record

Type: Minor
Products: All except RMC30 and RP110
ID: 2495

Even if Trap and Latch are turned 'on' for STP events alarm, "stp events" are logged in the <syslog.txt> file but there is no corresponding alarm or a Trap being generated. This problem has been fixed.

Serial protocols can not establish connection upon IP address change

Type: Minor
Products: RuggedServer
ID: 2878

If one device communication to the RuggedServer breaks communication with the remote device, and then the IP address is changed on one device, then the communication is not immediately restored. It will restore only after the TCP keepalive timer expires. This problem has been fixed.

Device crashes if Protocol of serial port is changed to 'None' while traffic is present

Type: Minor
Products: RuggedServer
ID: 2793

The unit may crash if the protocol is changed to none or any other protocol because of a mutex lock error which is causing the serial server to block for more than one minute. This problem has been fixed.

SNMPv1 traps not properly generated

Type: Minor
Products: All
ID: 2913

RuggedCom devices generate SNMPv1 traps with improper generic ID enterprise numbers (per RFC 1157). This problem has been fixed.

Device does not close connection if IP address is changed via Telnet or SFTP

Type: Minor
Products: All
ID: 3045

If the IP interface record was changed over TCP - Telnet or SFTP, the TCP connection is not closed as the IP interface was destroyed and reconfigured before closing, so the connection remained 'half-open' on the remote side. This problem has been fixed.

sysServices object value retrieved from RuggedServer does not reflect functionality of server (SNMP)

Type: Minor
Products: RuggedServer
ID: 3118

The 'sysServices' object value retrieved by SNMP from the RuggedServer reflects only bridging functionality. For RuggedServer products it should reflect 'end-to-end' (IP hosts) and applications functionality as well. This problem has been fixed.

Msg security level in SNMP request not properly checked

Type: Minor
Products: All
ID: 3135

The message security level in the SNMP request was being checked against the value from the Users table rather than from SecurityToGroup and Access Table, so access was not authenticated per the minimum security level required by the AccessTable. This problem has been fixed.

GMRP and static multicast don't interact according to spec

Type: Minor
Products: All except RMC30 and RP110
ID: 3136

Enabling/Disabling GMRP globally is not working correctly per the protocol specification. Configuration of GMRP is not properly applied when changed. This problem has been fixed.

SSH connection closed by device if packet delay is introduced by network

Type: Minor
Products: All
ID: 3143

During an SSH session from any client to the ROS® based device at the moment of password entering, an error would be generated from the switch: 'SSH application error Type 11'. This problem has been fixed.

LLDP User Interface displays corrupted neighbor Port ID information

Type: Minor
Products: All except RMC30 and RP110
ID: 3705

Port ID information in the User Interface was being presented in the form of an IP address. This problem has been fixed.

The value of object dot1dStpTxHoldCount might be retrieved out of limits

Type: Minor
Products: All except RMC30 and RP110
ID: 3370

The value of object 'dot1dStpTxHoldCount' might be retrieved out of limits. In RuggedCom devices that object might take any value from 3 to 100 or 0 (unlimited). The Bridge MIB defines this object with a value of 3 to 10. In order to retrieve the proper value, new object in RUGGEDCOM-STP-MIB is defined which 'expands' the value of standard object.

This problem has been fixed.

RuggedCom Discovery Protocol multicast MAC address not reinstalled upon mgmt VLAN change on new VLAN

Type: Minor
Products: All except RMC30 and RP110
ID: 3415

The RuggedCom Discovery Protocol (RCDP) multicast address is installed only on the management VLAN within the switch fabric ASIC. If the management VLAN is changed, the address was not removed and reinstalled on the new management VLAN. The unit would not be discovered using RCDP (L2 discovery on RuggedCom Explorer) until the unit is rebooted. This problem has been fixed.

LLDP Remote Mgmt Address Table data not properly stored to DB nor retrieved by SNMP

Type: Minor
Products: All except RMC30 and RP110
ID: 3460

Objects of 'lldpRemManAddrEntry' are not properly indexed when retrieved by SNMP. Using SQL commands retrieved values from the database (DB) table are not correct. The Management Address Subtype was always marked as value '4', which is the MAC Address type. The Management Address in indexes was marked with length of 5 instead of 4. This problem has been fixed.

Default loaded to the ipIfCfg table after file download without IP Address but with Gateway address configured

Type: Minor
Products: All
ID: 3705

ROS® loads the factory default on the ipIfCfg table when the IP address is missing, but the gateway information is present if the file generated in ROS® version 3.3.0 to 3.3.4x was previously downloaded. This problem has been fixed.

Link Detection Table conversion from version older than 3.4.2 fails

Type: Minor
Products: All except RMC30 and RP110
ID: 3801

The Fast Link Detection Table parameter conversion from version older than 3.4.2 is set always to a default value of 'on_with_portGuard' after an upgrade to software versions \geq 3.4.6. This problem has been fixed.

TACACS & RADIUS server unreachable event notification should be configurable in Alarm table

Type: Minor
Products: All
ID: 3832

Failure to contact TACACS and RADIUS server was not a configurable event.

The implementation has been refactored to create an alarm object within the DB_Server table. That way the same code supports all servers that can be configured with both a 'primary' and 'secondary' (NTP, RADIUS, TACACS+) server at this time. Two new objects are added to the 'rcsysinfo.mib' to retrieve the status of Radius and TACACS+ server in the same way as NTP server via SNMP. This problem has been fixed.

Incorrect values retrieved by SNMP for ipAdEntReasmMaxSize and ifHighSpeed

Type: Minor
Products: All except RMC30 and RP110
ID: 2520

Polling of SNMP objects ipAdEntReasmMaxSize and ifHighSpeed returned the incorrect values. This problem has been fixed.

GMRP Global Enable works differently when static multicast entry has Ports set to 'none'

Type: Minor
Products: All except RMC30 and RP110
ID: 3885

When the static multicast entry is created for an address with Ports set to 'none' and GMRP is globally enabled then the unit behavior is confusing. If ports are configured for GMRP disabled then traffic is not sent to any port, which is not correct. That traffic should be sent to all GMRP disabled ports. This problem has been fixed.

Some objects from LLDP-MIB retrieved with wrong data type

Type: Minor
Products: All except RMC30 and RP110
ID: 3409

Some objects from LLDP-MIB are reporting the incorrect data type – INTEGER rather than Counter32 or Unsigned32. This problem has been fixed.

There is no method to retrieve/verify that Gateway was learned via DHCP

Type: Cosmetic
Products: All
ID: 3885

ROS® is capable of receiving its gateway configuration from a DHCP server. However, there is no way to verify that the gateway configuration parameter was indeed received. The Default Gateway is added as information retrieved by the 'ip' CLI command.

Critical alarm sometimes generated when configuration file was uploaded

Type: Cosmetic
Products: SII
ID: 3693

Sometimes closing the configuration file after writing the flash file happens before the transport (xmodem, tftp) has closed the file. This information is logged to the <syslog.txt> file as critical, although all data was saved intact and ready to use. This problem has been fixed.

STP Root change is not always notified

Type: Cosmetic
Products: All except RMC30 and RP110
ID: 2843

Sometimes when an STP Root change event is not properly recorded within the Alarms table, the corresponding <syslog.txt> file entry is not created and an SNMP trap is not generated. This problem has been fixed.

Aged MAC Address indication not properly supported

Type: Cosmetic
Products: All except RMC30, RP110, RS8000 and RS1600
ID: 3425

If a unit MAC address is supposed to be unlearned upon receiving a NEW MAC address interrupt (with AGED flag set), it would be unlearned on an incorrect VLAN. This problem has been fixed.

Upgrade Instructions

The simplest way to upgrade the firmware is using the “RuggedCom TFTP File Management Utility” (rc-tftp.exe). This program allows upgrading of several devices at once and allows you to easily capture and store configuration files. Get a copy of that program at www.ruggedcom.com along with the binary file associated with the release and follow the instructions in the help section of the program.

Before upgrading we recommend:

- Reviewing all the changes to the firmware to ensure an upgrade is merited.
- Saving the CSV configuration file to a computer for future reference - settings may be affected after an upgrade.
- Upgrading a test unit to ensure you understand the upgrade process.
- Planning for a temporary network outage.

After upgrading we recommend the following:

- Clearing the system by running the CLI command: `clearlogs`
- Saving the CSV configuration file to a computer and compare with the CSV file captured before the upgrade. The firmware makes every attempt to carry over settings but there could be discrepancies.
- Verify that the network still operates according to your requirements.

Firmware/User Guide Version Numbering System

RuggedCom ROS® operating systems utilizes a three digit versioning number system of the form X.Y.Z where each digit is a decimal number starting from zero. This form is illustrated as:

(Functional).(Major/Branch).(Minor/Patch)

The 'X.Y' digits represent the Functional and Major version of ROS® and ROX™ respectively while the 'Z' digit represents Minor firmware updates. The 'X' and 'Y' digits are incremented for each major functional revision of the software capabilities which has been issued. The 'Z' digit is incremented for each update that is issued to address bug-fixes, critical, security, hardware related, cosmetic enhancements and other minor issues.

User guides follow the same format. In general, a user guide will have the same 'X.Y' digits as the firmware to which it corresponds.

It is RuggedCom's policy to provide Web access to only the latest 'patch' release for a version of firmware. If you decide that an upgrade is merited, then getting all the fixes only makes sense. It is for this reason that release notes are created detailing all patches for a given functional version.

Type of Changes

Each change to the firmware is categorized according to the table below to provide a guide as to whether the change justifies upgrading. As well, each change lists an internal RuggedCom change number.

Change Type	Description
Critical	Critical changes fix problems that prevent the basic operation of the device and have no workaround. Any critical changes merit a device upgrade under all circumstances.
Major	Major changes fix problems that prevent the basic operation of the device but do have a workaround. Any major changes merit a device upgrade if the workaround is not acceptable.
New Feature	New features add significant new capability to the device. Such changes may change the basic operation of the device, the user interface, and how the device is configured. New features only merit a device upgrade if the feature is required.
Enhancement	Enhancements improve existing device capability and do not significantly change the basic operation of the device, the user interface, or how the device is configured. Enhancements only merit a device upgrade if the feature is required.
Minor	Minor changes fix non-vital problems that may or may not have a workaround. Minor changes do not necessarily merit a device upgrade unless the specific problem applies.
Cosmetic	Cosmetic changes have negligible impact on device operation and include such updates as spelling mistakes, user interface adjustments, and help text improvements. Cosmetic changes rarely merit a device upgrade.
Security	Security changes usually do not have a discernable impact on normal device operation other than to improve the unit's defensive response to known exploits and vulnerabilities. This might include such updates as enhanced protection against newly discovered denial-of-service (DOS) attacks. It is left entirely to the customer's discretion to decide whether or not a security change is appropriate to merit a device upgrade.



Contacting RuggedCom

For further information on this release or technical support of any nature, please contact RuggedCom at the

Corporate Headquarters

RuggedCom Inc.
300 Applewood Cres,
Concord, Ontario
Canada, L4K 5C7

Toll-free: 1(888) 264-0006
Tel: (905) 856-5288
Fax: (905) 856-1995

Web: www.RuggedCom.com
Email: support@RuggedCom.com

US Corporate Headquarters

RuggedCom
1930 Harrison St., Suite-307
Hollywood, Florida
USA, 33020

Tel: (954) 922-7975

Technical Support:

Toll Free: 1(866) 922-7975