



Rugged Operating System v3.2.4 Release Notes

August 15, 2008

Copyright © 2008 RuggedCom Inc.

Overview

ROS™ v3.2.4 fixes some problems found in the previous versions.

- This firmware release supports all RuggedSwitch™ and RuggedServer™ product series.
- Build date: Aug 18 2008 14:42 File Size: 1584662

! ATTENTION !

Upgrade to ROS™ v3.2.1 or higher is strongly recommended for network topologies with extensive link redundancy (mesh topology).

! ATTENTION !

If RC-TFTP utility is used to perform ROS™ firmware upgrades, it is strongly recommended to use RC-TFTP version 1.10 or higher.

User Guides

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

Changes In v3.2.4(1526)**Add Support for M29W320ET70N6E and MX29LV320DTTI-70G Flash Memory**

Type: Internal

Products: All

ID: 1518

New flash memory chips are soon to be used in the devices. Support for these flash chips is added to this release to get software ready for customers that have standardized on the 3.2.x version.

Fixed data lost while transferring file to the serial device over 'RawSocket'

Type: Major

Products: All RuggedServer™

ID: 1524

For any Serial protocol if data are sent via IP faster than the serial ports can transfer them, IP packets could be discarded. This is the case when transferring a large file to the device served over RawSocket. This bug is fixed allowing TCP to flow control the remote side.

Changes In v3.2.3 (1110)

Add Support for Atmel AT49BV322D(T) Flash Memory

Type: Internal

Products: All

ID: 1104

Flash memory chip AT49BV322AT was discontinued and replaced by AT39BV322DT. The new chip could not be recognized by older versions of software and the bootup error “Unknown Flash memory” was reported. New driver is implemented to recognize new chip. This problem is fixed.

Fixed unexpected reboot with “G.Link read response error” crashlog report

Type: Major

Products: RS1600,RS8000

ID: 1101

Due to a marginal value of some software driver timeout, the device could occasionally reboot, if it was continuously receiving a very high volume of broadcast traffic. This is fixed.

Changes In v3.2.2 (795)

Fixed logging multiple failed login attempts

Type: Minor
Products: All
ID: 810

ROS™ implements a multiple failed login attempts protection mechanism - if too many failed login attempts occurred within a 5 min time period over the same interface (console , Telnet etc.), the interface login access is completely blocked for as long as an hour. When this happens an appropriate alarm is generated reporting the interface type where the event is detected.

That feature implementation had a bug - if the multiple failed login attempts were detected via Web Server or CLI shell, the alarm didn't specify any interface type name or specified the wrong interface type. This is fixed. Also, every single failed login attempt is reported in the syslog now.

Added back some deprecated MIB objects

Type: Minor
Products: All except RMC30
ID: 822

The ifInNUcastPkts and ifOutNUcastPkts IF-MIB (former MIB-II) objects were deprecated by rfc2863 and, thus, removed from ROS™ MIB support. However, some NMS packages still attempt to retrieve those objects. To guarantee full compatibility with such NMS packages, those MIB objects are supported by ROS™ again.

Port Mirroring configuration is now persistent

Type: Enhancement
Products: All except RMC30
ID: 813

Port Mirroring configuration was not saved in non-volatile memory to guarantee it would be disabled after system reboot. However, research showed that having that configuration persistent would be useful for many network administrators. So Port Mirroring settings are now saved in non-volatile memory like any other feature settings.

Added support for M-family products

Type: New
Products: M2100,M2200,M969
ID: 820

The M-family is a MIL-STD hardened version of RuggedCom products – M2100 is a hardened version of RSG2100, M2200 is a hardened version of RSG2200 and so on.

Changes In v3.2.1 (505)

Improved/fixed RSTP operation in complex network topologies

Type: Critical
Products: All except RMC30
ID: 663

The original RSTP standard (IEEE 802.1w-2001) had multiple weaknesses/errors so that even implementation compliant with the standard couldn't guarantee proper network topology reconfiguration in some scenarios. Complex network topologies (i.e. mesh, multiple rings etc.) were especially vulnerable to such RSTP flaws. The new RSTP standard (IEEE 802.1D-2004) addresses most of those weaknesses/errors and also improves RSTP performance. This ROS™ version upgrades RSTP implementation to the IEEE 802.1D-2004 standard.

Prevented corruption of firmware binary file during firmware upgrade

Type: Critical
Products: All
ID: 735

Firmware upgrade process consists of two steps – firmware binary file download and device reboot. If reboot was performed very shortly after the file download and upon high network activity, the firmware could be corrupted, thus making the device not operational. This is fixed.

Fixed potential broadcast storm after using Port Mirroring

Type: Critical
Products: RS900,RS900G,RS969,RSG2100,RSG2200
ID: 779

If Port Mirroring was used on the device and the device was not rebooted after that, port 1 (and also port 17 in RSG2100) could become a source of a broadcast storm due to looping broadcast frames back or sending them out of the port regardless of its RSTP forwarding state. This is fixed.

Fixed retrieving MIB objects with multiple GetNext requests in one SNMP PDU.

Type: Major
Products: All
ID: 687

If one SNMP PDU contained multiple GetNext requests for different tables, wrong objects could be retrieved. This is fixed.

Fixed operation of some device applications with dynamic IP address assignment.

Type: Major
Products: All
ID: 688

Some ROS™ applications (e.g. IGMP, RADIUS authentication) didn't accept dynamically assigned IP address and were working with IP address of 0.0.0.0. This is fixed.

Fixed losing TCP Raw Socket connectivity after Ethernet link failure and recovery.

Type: Major
Products: RS400,RMC30
ID: 718

If Ethernet link failed in the middle of TCP Raw Socket connection, no connections could be established after the link recovery unless the Raw Socket outgoing device received new data from its serial port. This is fixed.

Fixed failing to boot up with long RADIUS authentication key configured.

Type: Major
Products: All
ID: 721

If RADIUS Authentication Key configured in the device was longer than 8 characters (and RADIUS authentication enabled) and the device was rebooted, it could end up rebooting continuously and never coming up. This is fixed.

Fixed failing to establish Raw Socket call when both call directions are enabled.

Type: Major
Products: All
ID: 725

Raw Socket call might not be always established, if the Raw Socket "Call Direction" configuration parameter was set to "Both". This is fixed.

Fixed loss of some device functionality when configuring RMON History Control via SNMP.

Type: Major
Products: All except RMC30
ID: 726

Attempt to configure RMON History Control parameters via SNMP was causing loss of some device functionality (e.g. device management interface). This is fixed.

Fixed using wrong SNMP access level.

Type: Major
Products: All
ID: 728

When SNMP configuration parameters were changed, the access level configuration might not be updated properly. As a result, the previously configured access level could still be used. This is fixed.

Fixed rebooting if login screen refreshed in the middle of uploading firmware/configuration file.

Type: Major
Products: All
ID: 729

If the device login screen had to be displayed/refreshed (e.g. if the user was starting another login session) in the middle of firmware or configuration file upload process, the device could unexpectedly reboot. This is fixed.

Prevented ability to login into Web-based management session without proper credentials.

Type: Major
Products: All
ID: 764

Certain sequence of activities in Web browser could let the user login into a device management session even without entering proper username and password. This is fixed.

Prevented denial of Secure Shell service.

Type: Major
Products: All
ID: 770

Continuous frequent SSH connection requests (e.g. TCP port scanning) could cause denial of SSH service. This is fixed.

Fixed long Command Line Interface input causing device reboot.

Type: Major
Products: All
ID: 774

Very long CLI input (above 680 characters) was causing device reboot. This is fixed.

Fixed not updating 802.1X Port Security status.

Type: Minor
Products: All RuggedSwitch™ products
ID: 617

The displayed 802.1X Port Security status was not updated in a timely fashion. This is fixed.

Fixed Modbus Server not sending packets to multiple RTU's.

Type: Minor
Products: RS400,RMC30
ID: 625

When waiting for response from one RTU Modbus Server was not able to send packets to other RTU's. This is fixed.

Fixed wrong alarm names displayed by “alarm” CLI command.

Type: Minor
Products: RS400,RMC30
ID: 652

The “alarm” CLI command displays a list of all alarm types available in ROS™. However, some alarms were displayed without names while some others were displayed multiple times. This is fixed.

Fixed improperly latched Power Supply Failure Alarm.

Type: Minor
Products: RS1600,RSG2100,RSG200.RS969
ID: 686

In products with redundant power supply, a dedicated alarm is raised, if one of the power supplies fails. However, if a temporary failure occurred, the alarm was still on even after the power supply came back to normal operation. This is fixed.

Fixed inability to configure STP version via Web-based management interface.

Type: Minor
Products: All except RMC30
ID: 693

Although reporting success, the device was not accepting the STP “Version Support” parameter configured via Web-based management interface. This is fixed.

Fixed LED panel not functioning after reboot in VLAN-unaware mode.

Type: Minor
Products: RSG2100,RSG2200
ID: 700

If modular device was configured for VLAN-unaware mode and rebooted, it was coming up with the LED panel not functioning. This is fixed.

Fixed redundantly sending SNMP traps multiple times.

Type: Minor
Products: All
ID: 714

If more than one SNMP network management station was configured, SNMP traps were sent multiple times to each station. This is fixed.

Fixed discarding IGMP Join packets sent by other RuggedCom device.

Type: Minor
Products: All RuggedSwitch™ products
ID: 722

Due to very special differences in switch fabric hardware functionality, RS8000/RS1600 units were discarding IGMP Join packets sent by attached RS900/RS900G/RS969/RSG2100/RSG2200 units. This is fixed.

Fixed sending encrypted SNMPv3 traps when no security required by SNMPv3 configuration.

Type: Minor
Products: All
ID: 733

SNMPv3 traps were always sent encrypted, even if no security level was required by the device SNMPv3 configuration. This is fixed.

Fixed sending improperly formatted SNMPv3 Inform Requests (traps).

Type: Minor
Products: All
ID: 743

SNMPv3 Inform Request PDU's were used to send traps in SNMPv3 mode. However, they were sent with one of the PDU parameters (engine ID) set improperly. This problem is fixed by using encrypted SNMPv2 Traps instead of SNMPv3 Inform Requests.

Fixed loosing access to ROS™ file after multiple TFTP “get” transfers via ROS™ TFTP server.

Type: Minor
Products: All
ID: 746

Multiple repeated TFTP “get” transactions via ROS™ TFTP server could cause the ROS™ file to become not accessible. This is fixed.

Fixed failing to configure new RMON event via Web-based management interface.

Type: Minor
Products: All
ID: 749

All attempts to configure new RMON event via Web-based management interface were failing - the configuration wasn't accepted. This is fixed.

Fixed erroneous syslog success report in case of failure to save uploaded ROS™ file.

Type: Minor
Products: All
ID: 751

Even if saving uploaded ROS™ file in non-volatile memory failed, the syslog was still reporting success. This is fixed.

Fixed blocking Telnet connections by sending arbitrary data to Telnet server TCP port .

Type: Minor
Products: All
ID: 772

'CTRL-Y' character was treated by the ROS™ login process in a special way – namely, it was commanding ROS™ to move from the default menu login mode to a Command Line Interface (CLI) login mode. If an arbitrary data stream sent to ROS™ Telnet server contained 'CTRL-Y' character, it was causing the Telnet server to move to a CLI mode, thus occupying Telnet connection. Doing it multiple times could cause the maximum number of allowed Telnet connections to be used. The special treatment of 'CTRL-Y' character is eliminated.

Fixed wrong time stamp in some startup syslog entries.

Type: Minor
Products: All
ID: 782

Some startup syslog entries had time stamp not taking Time Zone into consideration. This is fixed.

Fixed wrong clock precision in sent SNTP packets.

Type: Minor
Products: All
ID: 784

All SNTP packets (both client and server) were sent with the clock precision field not set. This is fixed.

Fixed wrong Secure Shell login prompt.

Type: Cosmetic
Products: All
ID: 754

SSH login prompt was displaying "Press any key to continue..." while only "Enter" key was accepted. Now the user is only prompted for "Enter" key.

Added "clearethstats" CLI command.

Type: Enhancement
Products: All
ID: 461

Clearing Ethernet statistics for a specified port(s) was possible via an appropriate menu command. A corresponding shell command is now added.

System crashlog file is examined periodically.

Type: Enhancement
Products: All
ID: 618

The system crashlog file was checked at bootup and an appropriate alarm was raised, if there were any crashlog entries. However this check was only performed at bootup time, so the user was not notified about crashlog entries until the next device reboot. Now the crashlog file is checked periodically every few seconds.

Added more directives to "config.csv" file.

Type: Enhancement
Products: All
ID: 653

The set of device configuration parameters is slightly different for different RuggedCom products (or even for different revisions of the same product). As a result, various problems were encountered when trying to load the same configuration file into different products. Several new directives are supported now by the "config.csv" file (see comments in the "config.csv" file header) to allow extensive flexibility in using the same configuration file for different products.

Same UDP port is used by RuggedServer™ for both destination and source port of serial-over-UDP packets.

Type: Enhancement
Products: RS400,RMC30
ID: 665

UDP port is configurable for serial-over-UDP traffic, however, the configured value was only used as a destination port, while the source port number was chosen randomly and was different of the destination port number. That created problems with passing firewall, if one was used in the network. Serial-over-UDP packets are now using the same configured destination and source UDP port.

Increased maximum number of simultaneous TCPModbus connections to 64.

Type: Enhancement
Products: RS400,RMC30
ID: 667

Some SCADA TCPModbus applications always open a separate TCP connection for every end device, thus requiring a large number of simultaneous connections in RuggedServer™. The maximum supported number of simultaneous TCPModbus connections is increased to 64.

Added support for "Read Holding Registers (03)" Modbus management command.

Type: Enhancement
Products: All
ID: 702

ROS™ supports the ability to read some device status information via the Modbus TCP protocol. This allows system integrators to display network information on an HMI and retrieve that data using the same protocol as the other devices on the network like PLCs. Unfortunately, as of ROS v3.1, only the "Read Input Registers (04)" command was supported for so called "3X" addressing. It is more common however for PLCs and the like to support the "Read Holding Registers (03)" command for so called "4X" addressing. (The two separate commands are somewhat an artifact of Modicon PLC design and can be treated as the same command; this is done on other products supporting Modbus)

The "Read Holding Registers (03)" command is now supported as well.

Broadcast rate limiting activation is logged with "WARNING" level.

Type: Enhancement
Products: RS8000,RS1600
ID: 730

RuggedSwitch™ supports broadcast rate limiting to protect the network from potential broadcast storm. When such limiting was actually activated, an appropriate syslog entry was logged with "ERROR" log level meaning an error in the network. However, it was sometimes interpreted by the users as a ROS™ error. To avoid confusion, that syslog entry is now logged with "WARNING" log level.

"FEFI" configuration parameter renamed to "LFI".

Type: Enhancement
Products: All except RMC30
ID: 731

RuggedSwitch™ offers a special feature on some of Ethernet port types which is intended to handle link failures in one direction only. This feature stops transmitting Ethernet link integrity signal out of the port in case the port stops receiving link integrity signal. The feature was called "FEFI" (Far End Fault Indication). However, the IEEE 802.3 standard defines that name for a similar but different unique feature of 100Base-FX links. To avoid confusion, the RuggedSwitch™ feature is now called "LFI" (Link Fault Indication).

IP address assignment reported in syslog.

Type: Enhancement
Products: All
ID: 752

ROS™ syslog is a very useful resource for troubleshooting networks with ROS™ devices installed. However, the syslog didn't contain any information about the ROS™ device's IP address so it was hard to associate syslog files with the devices in the network diagram. IP address assignment is now reported in the syslog.

Added ability to disable Remote Shell.

Type: Enhancement
Products: All
ID: 760

Remote Shell is an unsecure device management method which was always enabled in ROS™ without any ability to disable it. A new configuration parameter is now added allowing to disable Remote Shell.

Disabled listening to TCP/UDP port for unused management applications.

Type: Enhancement
Products: All
ID: 771

Even if some management application (e.g. Telnet) was administratively disabled, the ROS™ TCP/IP stack was still listening to its dedicated TCP/UDP port making it visible to the outside world and, thus, affecting the device security. This is fixed.

Default SNMP Security Model is SNMPv3.

Type: Enhancement
Products: All
ID: 776

Although the secure SNMPv3 was supported, the default SNMP Security Model was the unsecure SNMPv2. SNMPv3 is now the default SNMP Security Model.

Eliminated false error syslog report during shutdown.

Type: Enhancement
Products: All
ID: 787

During the ROS™ shutdown process, some system error reports were sometimes logged in the syslog and/or crashlog. Those reports were created erroneously and didn't indicate actual system errors. Such syslog entries are now eliminated.

Added support for static multicast groups.

Type: New Feature
Products: All except RMC30
ID: 70

The user can now configure static Layer 2 multicast groups specifying the group MAC address and Ethernet ports the group traffic should be forwarded to.

Added support for BootP.

Type: New Feature
Products: All
ID: 524

The RuggedVue network management software supports an innovative feature (called Auto-IP) that allows IP addresses to be dynamically assigned to devices based on their location in the network. This is unlike DHCP that assigns IP addresses based on the MAC address of the device. In order for Auto-IP to work, ROS™ now supports the BootP protocol.

RuggedServer™ allows to prioritize serial-over-IP traffic from certain sources.

Type: New Feature
Products: RS400,RMC30
ID: 553

RuggedServer™ can now be configured to use DSCP (Differentiated Service Code Point) field in the IP header of serial-over-IP packets to prioritize packets originated by certain serial traffic source devices.

Added RuggedCom proprietary MIB.

Type: New Feature
Products: All
ID: 575

RuggedCom proprietary RUGGEDCOM-SYS-INFO-MIB is now supported. This MIB contains general system information about ROS™ device - generated traps (failures), system resources, hardware and software information, various status parameters (e.g. redundant power supply status, temperature sensor reading etc.).

Added support for RuggedServer™ RS416.

Type: New Feature
Products: All
ID: 615

The RuggedServer™ RS416 is an industrially hardened serial device server with an integrated, fully managed, Ethernet switch, designed to operate reliably in electrically harsh and climatically demanding environments. Featuring a modular design that can support up to 16 serial ports and up to 4 Ethernet ports, the RS416 is able to interconnect multiple types of intelligent electronic devices (IEDs) that have different methods of communications.

Added remote syslog support.

Type: New Feature
Products: All
ID: 637

The syslog protocol, defined in RFC 3164, provides a transport to allow a device to send event notification messages across IP networks to event message collectors, also known as syslog servers. ROS™ can now be configured to send syslog messages to specified server(s).

Added support for TINmode2 serial protocol.

Type: New Feature
Products: RS400,RMC30
ID: 643

The Train-to-Wayside Communication (TWC) Interface (TINmode2) device is an industrial COTS serial to Ethernet converter with custom software. The TINmode2 recovers Incremental Train Control System (ITCS) datagrams encapsulated in IP datagrams received from the trains via wayside radios and forwards them to the Radio Block Centre (RBC) via an asynchronous serial interface. The TINmode2 encapsulates ITCS datagrams received from the RBC in IP datagrams and forwards them to the one or more wayside radios for transmission to trains.

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

ROS has a three digit version numbering system of the form X.Y.Z where each digit is a number starting from zero. The 'X.Y' digits represent the functional version of ROS whereas the 'Z' digit represents firmware patches. The 'X' digit is incremented for a major functional updates of the product. The 'Y' digit is incremented for a minor functional updates of the product. The 'Z' digit is incremented for bug fixes, 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.

Contacting Technical Support

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

RuggedCom Inc,
30 Whitmore Road,
Woodbridge, Ontario, Canada
L4L 7Z4

Toll-free: 1-866-922-7975 (North America)
Tel: 905-856-5288
Fax: 905-856-1995
Email: support@ruggedcom.com
Web: <http://www.ruggedcom.com>