

Rugged Operating System v3.6.4 Release Notes

April 27, 2009

Copyright © 2009 RuggedCom Inc.

Overview

ROS® v3.6.4 fixes some bugs and adds some enhancements.

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

- Build date: Apr 21 2009 09:26 File Size: 2193502

User Guides

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

! ATTENTION !

- 1. Upgrading to ROS® v3.6.1 or later revision is strongly recommended for ROS® v3.6 users who use a management VLAN ID other than #1 (default).**
- 2. Upgrading to ROS® v3.6.3 or later revision is strongly recommended for all RuggedServer™ users.**
- 3. Upgrading to ROS® v3.6.4 or later revision is strongly recommended for ROS® v3.6 users who use SNMP to monitor and manage network.**

Changes In v3.6.4 (1811)

Switch scanned by RuggedNMS stops responding to management applications.

Type: Critical
Products: All except RMC30
ID: 1812

After continuous NMS scanning switch with several unused VLANs, the retrieval of MAC address table via SNMP was interfering with the update of internal MAC address tables from the switch fabric. The unit could enter into a state whereby the management IP interface became unreachable. The only way to manage the switch after this condition was via the serial console. This has been fixed.

2GB TX interface support for i802 product.

Type: New feature
Products: i802
ID: 1641

Support for a new interface type 2GB copper option has been added to the i802 product family.

Breaking aggregated link caused crash if IGMP and GVRP were enabled.

Type: Major
Products: All except RMC30
ID: 1726

The breaking of an aggregated link could force the unit to reboot. This has been fixed.

Wireless daughter card settings not updated after new configuration file download.

Type: Major
Products: RS900W
ID: 1798

After a ROS® configuration file was download, the device was automatically rebooted but without applying the downloaded configuration to the wireless daughter-card. To fix this problem, before rebooting the device all wireless settings are now transferred to the daughter card.

Default Gateway is not saved if IP address obtained dynamically via DHCP or BOOTP.

Type: Minor
Products: All
ID: 1776

If an IP address is to be assigned by DHCP or BOOTP protocol, the 'default gateway' parameter provided by the assigning-server was not saved to the IP Gateways table. The switch would lose connectivity with devices outside of its own subnet. This has been fixed.

System Identification text was too short.

Type: Minor
Products: All
ID: 1785

Customer requested an extension of System Identification as 19 characters was too short for their naming convention. System Identification is now expanded to 24 characters.

Crashlog.txt entry created during 802.1x authentication if backup server is configured

Type: Minor
Products: All except RS400 and RMC30
ID: 1796

If the backup authentication server (RADIUS or TACACS+) is configured, an entry in crashlog.txt file will be created whenever the primary server does not answer. There were no implications to the switch functionality.

Modbus TCP connection not reestablished over auxiliary IP port after serial port reset

Type: Minor
Products: All RuggedServer™ products
ID: 1785

If a modbus connection was open via an auxiliary IP port, it would be permanently lost after issuing a 'reset' command over the serial port. Upon 'reset' the serial port command connection is not closed anymore.

Software watchdog occasionally resets device.

Type: Minor
Products: All
ID: 1813

Erratic unit reset problems were observed upon intensive SSH scan-test caused by minor software design issue.

Changes In v3.6.3 (1736)**Address based protocols unable to route protocol packets.**

Type: Major
Products: All RuggedServer™ products
ID: 1737

This bug was inadvertently introduced in v3.6.2. After booting up, the 'Device Address Table' was not correctly initialized from the configuration database and so the serial-server could not route packets. All protocols using static device address entries were affected.

Changes In v3.6.2 (1684)

Device crash upon receiving corrupted Microlok packet from serial port.

Type: Major
Products: All RuggedServer™ products
ID: 1657

Improper handling of corrupted a 'Microlok' protocol packet where the length of the destination address given by an escape sequence is greater than 15 digits (corrupted highest 4 bits of lower byte of address length) may cause device to crash.

Duplicated entries allowed to be inserted to the Device Address Table could corrupt binary files

Type: Major
Products: All RuggedServer™ products
ID: 1716

Within the Device Address Table, duplicated entries (the same protocol address configured for multiple local ports) are allowable. Immediate deletion of such an entry could cause a configuration file to grow too large and its backup to be written to the flash, which in turn could corrupt other files.

Device sometimes reboots when it tries to establish a connection with a non-responsive IP address.

Type: Minor
Products: All RuggedServer™ products
ID: 1663

An improperly closed-connection process when calling out for serial protocols could cause the device to lose information about already established connections and cause the device to reboot.

Modbus RTUs do not respond to read/write registers function (23).

Type: Minor
Products: All RuggedServer™ products
ID: 1673

If several Modbus RTUs are configured for one serial port (Modbus Server) and one of them is disconnected, all other devices could become unresponsive because of an incorrectly calculated expected-response time.

Accessing the MSTP menu screen from SSH caused device to reset.

Type: Minor
Products: All except RMC30 and RS400
ID: 1694

Accessing MSTP menu screen in SSH was improperly handled and could cause device to reset.

IP interface for RMC30 cannot be changed through Web server.

Type: Minor
Products: RMC30
ID: 1698

Changing the IP interface configuration for RMC30 via the Web server failed with the information “No data found”.

Device experiences slow memory leak on IP port scanning.

Type: Minor
Products: All
ID: 1699

Device was slowly losing memory while scanning SSH and TFTP IP ports. After a long run the device would eventually reset to recover.

Factory defaults can not be loaded via SNMP.

Type: Minor
Products: All
ID: 1704

Device responded with “no such object” to the attempt to set factory default values via SNMP.

Device experiences slow memory leak on sending RMON Alarms via SNMP.

Type: Minor
Products: All except RMC30
ID: 1707

Sending RMON alarms to SNMP management station caused a slow memory leak. After a long run the device would eventually reset to recover.

Visiting TACACS+ Web table caused change to the web user’s access level.

Type: Minor
Products: All
ID: 1709

The ‘+’ sign was not properly parsed by the web server query, and caused information following it to be lost. User information was lost, so a wrongly identified user was assigned “NULL” access.

Password can not be shortened more than one character at a time.

Type: Minor
Products: All
ID: 1710

Once configured the password could not be reconfigured to any string which was shorter by more than one character.

Password tables are visible by 'non-administrative' access.

Type: Minor
Products: All
ID: 1715

Tables containing passwords (SNMP Users, Radius, TACACS) were previously viewable to 'guest' and 'operator' account users. Additionally in versions 3.5.0 through 3.6.1 even the 'Password Table' was visible for 'non-administrative' account users. Password fields were not masked, so credentials were compromised. This has been fixed.

Changes In v3.6.1 (1612)

Value range for the DNP timeout field changed.

Type: Enhancement
Products: All RuggedServer™ products
ID: 1608

The range for the DNP time out is changed to 60 – 10800 (1 min to 3 hours) to accommodate customer requests.

Management VLAN is defaulted to #1 after rebooting device.

Type: Critical
Products: All except RMC30
ID: 1608

The loss of the management VLAN ID (if configured to any VLAN ID other than default) in the IP Configuration Table caused the device to lose connectivity after a reboot.

Both direction calls for RawSocket are sometimes not reestablished.

Type: Major
Products: All RuggedServer™ products
ID: 1597

If a call directed over a device RawSocket port configured for “both” directions was disconnected in some circumstances it would not be reestablished. The serial port would appear to be non-responsive.

TFTP Client fails to properly download file with non-printable characters.

Type: Minor
Products: All
ID: 1577

If the user attempts to download a file (from PC to device using the TFTP Client) which contains nonprintable characters, it would be refused by the device – even though the received file is still usable.

UI screen does not contain "A-Apply" message in display footer after changing the record value.

Type: Minor
Products: All
ID: 1576

If the value of a configuration record is changed, the “Apply” button must be shown in the footer and the change can be saved at any time without leaving the display screen.

Device resets itself after an unsuccessful config.csv download.

Type: Minor
Products: All
ID: 1595

ROS[®] 3.6.0 introduced a change to “reset” the device automatically after a config.csv file is downloaded and saved. However, the device should not reset itself after an unsuccessful config.csv download.

Setting the DB to default caused RuggedServer device reset.

Type: Minor
Products: All RuggedServer™ products
ID: 1596

This problem would happen only if calls from the device are in progress. Calling sockets must be properly shutdown while applying a new configuration.

IP config table's ID can not be modified through UI.

Type: Minor
Products: All RuggedServer™ products
ID: 1606

This problem forced a modification of the ID whenever a new record was inserted with the same ID, this would overwrite the old ID. It is now fixed, so that entries are correctly stored in the database.

A Crashlog.txt file was falsely created when a telnet client from device shell is used.

Type: Minor
Products: All
ID: 1618

When a connection to a peer host-device is established via Telnet client (from the ROS[®] serial console shell), then after closing the connection a crashlog.txt file is created. This was a false alarm.

TFTP client blocked after IP interface is changed once via UI System.

Type: Minor
Products: All
ID: 1620

After changing the IP address or any VLAN configuration manually, the UI System is set to a high task priority. This prevented the TFTP client from downloading.

Some objects from ifTable and ifXTable improperly retrieved for dynamically assigned IP address.

Type: Minor
Products: All except RMC30
ID: 1622

If the IP address was dynamically assigned, values for objects from ifTable and ifXTable could be improperly retrieved.

SNMP Agent: mishandling of a negative Request-ID.

Type: Minor
Products: All
ID: 1610

If an SNMP request was received with a negative Request-ID, then the response from the unit contained an incorrect (bad format) Request-ID - which was an error condition.

Changes In v3.6.0 (1412)

Add support for RSG2300 model.

Type: New feature
Products: RSG2300
ID: 1385

The RuggedSwitch® RSG2300 is a fully managed Ethernet switch with 32 ports. The RSG2300 uses a brand new combination of switch and PHY chips (1 88E6185 and 4 88E6095F) to provide increased port density and GigE port support. On board RAM memory has been extended to 32 MB and Flash memory is extended to 8 MB.

Add support for i800 and i801.

Type: New feature
Products: i800, i801
ID: 1492

Device models i800 and i801 are new additions to the i8xx family of products. These two products provide 8 TX, 8 TX+1G fiber or 8 TX+1G copper port combinations.

Add support for FAT Flash-File-System (FFS).

Type: New feature
Products: i80x
ID: 1415

The i8xx family models are built with removable 1GByte Secure Digital (microSD) flash cards. For interoperability with PC systems, the microSD card is partitioned and formatted with the FAT file system for which support is now available within ROS®. The user is able to utilize this card as standard removable disk media on Linux and MS Windows systems. The primary “use-case” scenario is to backup, restore, and upgrade both firmware and working configuration in the so called “redundant mode” context.

Add support for GMRP.

Type: New feature
Products: All except RMC30
ID: 664

The GARP Multicast Registration Protocol (GMRP) provides a mechanism that allows end stations and MAC Bridges to dynamically register (and subsequently deregister) Group membership information with Bridges attached on the same LAN, and disseminates that information across all the Bridges that support Extended Filtering Services within the Bridged Local Area Network. The operation of GMRP relies upon the services provided by GARP. GMRP support is implemented per IEEE 802.1d – 2004 Clause 10.

Add support for Q-Bridge MIB.

Type: New feature
Products: All except RMC30
ID: 33

The Q-Bridge MIB is the VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks as defined by IEEE 802.1Q-2003, including Restricted Vlan Registration as defined by IEEE 802.1u-2001 (RFC 4363).

Added support for IP MIB.

Type: New feature
Products: All except RMC30
ID: 1306

The IP-MIB is the MIB module for managing IP and ICMP implementations (based on RFC 2011).

Multiple Active Topologies supported by other system modules.

Type: Enhancement
Products: All except RMC30 and RS8000 and RS1600 families
ID: 1384

The MSTP (Multiple Spanning Tree Protocol) introduced the concept of multiple active (logical) topologies per physical topology. RSTP constructs a single spanning tree – referred to as the Common Spanning Tree (CST) - and maintains a single Port State for each Port. MSTP constructs multiple spanning trees - the Common and Internal Spanning Tree (CIST) as well as additional Multiple Spanning Tree Instances (MSTI) - and maintains a Port State for each spanning tree for each Port.

The release enhances Port Security, IGMP Snooping, GMRP and Link Manager applications for operation and awareness over multiple active topologies, rather than the CIST only.

Add support for 100FX on eligible Ethernet ports.

Type: Enhancement
Products: RS2200, RS2300
ID: 1424

Configuration support for running 100FX over a Gigabit Ethernet slot has been added. At present, this feature is supported in selected products.

Add 'operEdge' RSTP status parameter to the RSTP Port Stats Table.

Type: Enhancement
Products: RS940
ID: 1463

The 'operEdge' value is a very important RSTP status parameter used internally by the RSTP/MSTP state machines. The value of this parameter (determined automatically by RSTP/MSTP operation) has dramatic influence on the time when a switch port is put to Learning and Forwarding state.

Add 'restrictedRole' and 'restrictedTch' configuration parameters to MSTP Port Configuration Table.

Type: Enhancement
Products: All except RMC30 and RS8000 and RS1600 families
ID: 1464

The 'restrictedRole' and 'restrictedTcn' parameters are added to the MSTP configuration on a per port level.

Menu and data selection 'wrap-around' is supported in UI System.

Type: Enhancement
Products: All
ID: 1478

Moving through the menu entries or a data list in the User Interface (UI) System is made more convenient to the user by allowing the cursor selection to 'wrap-around' at the edges. For example, after the last item on the page has been reached, the cursor will be moved to the first item again with 'cursor down' key; or from the first item to the bottom item with 'cursor up' key.

Supported new time zone for Venezuela (UTC -4.30).

Type: Enhancement
Products: All
ID: 1556

New time zone has been added to support time zone change in Venezuela.

Supported loading factory defaults to all database tables.

Type: Enhancement
Products: All
ID: 1479

Loading defaults to the configuration system now supports two options: 'selected' or 'all'. Option 'selected' will preserve IP address on management interface and default gateway if it is on the management subnet, and SNMP configuration to keep the RuggedSwitch® accessibility for management applications. Option 'all' will set ALL of the configuration tables back to the default values, with no exceptions.

Extended range of local IP ports configured for RawSocket.

Type: Enhancement
Products: All RuggedServer™ products
ID: 1549

The so called 'well known' reserved IP port range (1 to 1024) was previously excluded for selection from 'listening' for serial protocols within ROS®. However some devices (such as Siemens traffic controllers) and management software do use port 1000 (which falls within this range) for polling and the port number cannot be changed. The NTCIP (National Transportation Communications for ITS Protocol) standard also appears to reuse 'well known' port numbers. User selection within this range is now supported by ROS® for 'RawSocket' serial mode implementation.

Fixed ModbusServer Serial port lockup.

Type: Critical
Products: All RuggedServer™ products
ID: 1549

If too many invalid Modbus packets were received by the server destined to the serial ports configured as ModbusServer, the device could eventually become unmanageable and all serial ports would be blocked. The problem was due to a gradual starvation of free internal buffers that transfer data between transport and application layer if many invalid packets are encountered.

Fixed memory leak in IP stack and Web Server.

Type: Major
Products: All
ID: 1482

A memory leak detected in the IP stack, Web Server and irregular closing of SSH session can cause device to reboot to recover. This was detected during the time when the NMS station checks services on switches (scanning some well know IP ports periodically).

Fixed handling frames larger than 1528 bytes.

Type: Major
Products: All except RMC30
ID: 1491

If an Ethernet frame larger than 1528 bytes was received by the CPU, then the device would crash. This was caused by improper setting of the maximum buffer size in the FEC module, enabling buffers from the switch fabric to be received by the FEC.

Fixed data loss while transferring file via serial protocol.

Type: Major
Products: All RuggedServer™ products
ID: 1524

For any IP to Serial application, if traffic rate via IP was too high, data were lost since serial port could not handle all the data.

Instead of relying on high level protocol flow control ability, **ROS®** allows TCP layer to flow control. Transfer will slow down to the level that serial ports can handle incoming traffic, but data will not be lost.

Fixed potential blocking of lower priority tasks.

Type: Major
Products: All
ID: 1562

This problem was caused by improper internal timer handling by the UI system.

Fixed switching to VLAN unaware mode when high multicast traffic rate is present on the line.

Type: Minor
Products: RS8000 and RS1600 families
ID: 1521

The presence of multicast traffic on the line caused device to crash while switching to VLAN unaware mode.

Fixed setting address aging time to default in its config table when upgrading from v3.4.7 to v3.5.0.

Type: Minor
Products: All RuggedServer™ products
ID: 1455

Improper ITCS configuration conversion between v3.4.7 and v3.5.0 cause aging time for ITCS protocol to be set to the default value.

Fixed configuration via WebServer for some database tables.

Type: Minor
Products: All
ID: 1467

Some tables like RMON History Configuration and Device Address Table could not be set via Web Server.

Fixed handling too long string by SQL command.

Type: Minor
Products: All
ID: 1487

Sending an SQL command string which was “too long” could cause the device to crash. An example of this is the ‘*’ character when load default is performed via RSH from Unix machine. The ‘*’ character would create RSH command with string containing the entire directory from which the command is executed.

Fixed ability to set object value for SNMP users with ‘write’ only access.

Type: Minor
Products: All
ID: 1490

A ‘write’ request was not accepted from a user that was allowed only ‘write’ access. Prior to this fix, ‘read/write’ access had to be allowed if writing was required.

Fixed improper retrieval of object dot1dStpPortDesignatedBridge via SNMP

Type: Minor
Products: All except RMC30
ID: 1493

The value of object ‘dot1dStpPortDesignatedBridge’ was not zeroed if the link was down. Instead, the retrieved value was that which the object contained before link down event happen.

Fixed error code handling in TacPlus

Type: Minor
Products: All
ID: 1499

Error code set by error found by server was ignored.

Fixed problem where ‘guest’ user can modify Static Multicast Group table.

Type: Minor (security)
Products: All except RMC30
ID: 1505

Previously, the ‘guest’ user was incorrectly allowed to modify the Static Multicast Group table, rather than to ‘admin’ user only.

Fixed processing link up/down events by GVRP if STP is disabled.

Type: Minor
Products: All except RMC30
ID: 1519

If link is up and RSTP is disabled, it is always in forwarding state and must support up/down events for GVRP protocol in order to learn and advertise VLANs.

Removed limitation in establishing a connection via Modbus Client, if poller (master) and slave are both on the same IP address.

Type: Minor
Products: All RuggedServer™ products
ID: 1523

This limitation is causing a problem for demonstrations where both the 'poller' and 'slave' simulator are running on the same PC, so it has been remedied.

Fixes setting objects from BRIDGE-MIB and RSTP-MIB via SNMP.

Type: Minor
Products: All except RMC30
ID: 1525

Setting dot1StpPortPriority via SNMP to any value was reflected by value 'zero' for port priority in Port RSTP parameters table.

Fixes device crashing during bootup process if traffic is present on the serial port and UDP transport is used by serial protocols.

Type: Minor
Products: All RuggedServer™ products
ID: 1527

Device sometimes crashed during bootup process if traffic was presented on serial port configured for UDP transport.

Fixes loading defaults to Radius and TacPlus Configuration Tables.

Type: Minor
Products: All
ID: 1546

When both Primary and Secondary Servers were configured for TACACAS+ and RADIUS, any attempts to Load Defaults (configuration) in these tables would fail.

Fixes problem where TFTP client can not start new session after breaking transfer from command line.

Type: Minor
Products: All
ID: 1554

If a TFTP file transfer was cancelled using CTRL+C while device was receiving a file from a TFTP server using the 'get' command, then the TFTP client would be blocked and the command will never return to UI system until the device was reset.

Fixes clearing Power Supply Failure alarm after recovery.

Type: Minor
Products: RS2100, RS2200, RS1600, i80x family of products
ID: 1561

Power Supply Alarm/Trap does not reset when backup supply is available again.

Fixes reading SFP information.

Type: Cosmetics
Products: RS2100, RS2200, RS900G, RS940G
ID: 1472

TX bias current, TX output power and RX received optical power were incorrectly calculated for internally and externally calibrated SFP.

Flash memory chips M29W320ET70N6E and MX29LV320DT supported.

Type: Internal
Products: RS2100, RS2200, RS900G, RS940G
ID: 1472

New Flash driver is implemented to recognize new flash chips used in manufacturing.

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 RuggedCom

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

Corporate Headquarters

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

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

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

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