



Rugged Operating System v3.3.5 Release Notes

October 27, 2008

Copyright © 2008 RuggedCom Inc.

Overview

ROS™ v3.3.5 adds a single enhancement.

- This firmware release supports all RuggedSwitch™ and RuggedServer™ product series.
- Build date: Oct 20 2008 11:18 File Size: 1696434

! ATTENTION !

1. Upgrade ROS™ v3.3.x revision is strongly recommended. It is especially recommended to RuggedServer™ users.
2. Upgrade to ROS™ v3.3.x revision is a must for ROS™ v3.2.x users who use RSTP in conjunction with Link Aggregation.
3. If RC-TFTP utility is used to perform ROS™ firmware upgrades, you will have to use RC-TFTP version higher than 1.15 after upgrading to ROS v3.3.x.

User Guides

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



Changes In v3.3.5(1603)

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 3.3.x version.

Changes In v3.3.4 (1099)

Fixed losing Serial IP connectivity after clearing long-time inactive connection

Type: Major
Products: All RuggedServer™ products
ID: 1086

If RuggedServer™ had several serial-over-TCP connections serving the same serial protocol and one of the connections was for some reason cleared simultaneously by both ends, one of the connections (either remaining or the one being cleared) could permanently lose connectivity on a serial protocol level which could not be restored even by trying to reestablish the TCP connection. This 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.

Fixed retrieving RSTP timer values from BRIDGE-MIB dot1dStp table

Type: Minor
Products: All except RMC30
ID: 1068

BRIDGE-MIB dot1dStp table timer values should be retrieved in units of 0.01s (centi-seconds). Due to a firmware bug the values were retrieved in units of 0.1s, so that a retrieved number would be 10 times smaller than a proper number of centi-seconds. This is fixed.

Fixed duplicate RawSocket IP packets sent upon “Pack Character”

Type: Minor
Products: All RuggedServer™ products
ID: 1074

If RuggedServer™ was configured to packetize Raw Socket serial data upon receiving a “Pack Character”, two duplicate IP packets were sometimes sent. This is fixed.

Fixed Serial IP functionality in RS416 with missing serial modules

Type: Minor
Products: RS416
ID: 1087

If some serial modules were not installed in a RS416 unit and thus serial port numbers were not sequential, the device didn't function as RuggedServer™, even if it was properly configured. This is fixed.

Fixed retrieving MIB objects from port-based tables

Type: Minor
Products: All RuggedServer™ products
ID: 1090

If some Ethernet modules were not installed in a ROS™ device and thus serial port numbers were not sequential, invalid values could be retrieved from port-based MIB tables. This is fixed.

Fixed remote DNP address auto-learning

Type: Minor
Products: All RuggedServer™ products
ID: 1096

RuggedServer™ didn't auto-learn remote DNP addresses from received IP packets in the following cases:

- the configured DNP learning interface's subnet mask is not its "natural" subnet mask
- a packet was received from a subnet different than the configured DNP learning subnet.

This is fixed.

Changes In v3.3.3 (1072)

Fixed opening Telnet/SSH session during HTTPS service scan

Type: Major
Products: All products
ID: 1059

Some Network Management Software packages may scan different IP services of the device management interface to verify their availability. If such a scan was performed for the HTTPS service, it could cause Telnet and SSH management connections to be undesirably closed immediately after opening. This is fixed.

Fixed updating connection counter when closing SSH connection

Type: Major
Products: All products
ID: 1076

When an SSH connection was being closed ROS™ erroneously kept counting the connection as “open”. As a result, after SSH connections were opened and closed several times the connection counter reached the maximum number of allowed connections and no more SSH connections could be established until the system reset. This is fixed.

Fixed Telnet/SSH connection time-out while not logged-in

Type: Minor
Products: All products
ID: 1062

If the user opened a Telnet/SSH connection to a ROS™ device but didn't proceed to configuration menus, the connection would never time out and remain open, thus reducing the number of available connections. This is fixed.



Changes In v3.3.2 (1049)

Fixed processing RawSocket-over-UDP packets from unknown sender

Type: Major
Products: All RuggedServer™ products
ID: 983

This issue has already been addressed in ROS™ v3.3.1 , however it was only fixed partially – the fix only took effect, if the ROS™ serial port trace utility was enabled. It is fixed properly now.

Changes In v3.3.1 (994)

Fixed processing RawSocket-over-UDP packets from unknown sender

Type: Major
Products: All RuggedServer™ products
ID: 983

Receiving RawSocket-over-UDP packets from an unknown IP address caused RuggedServer™ to loose memory buffers without returning them to the pre-allocated buffer pool. As a result, all buffers in the pool could be lost after a while, thus entirely breaking serial-over-IP communication. This is fixed.

Fixed config.csv file 'ROS_VERSION' directive

Type: Minor
Products: All
ID: 988

The 'ROS_VERSION' config.csv file directive allows to apply different subsets of the configuration parameters depending on the revision of ROS™ running in the device. However, due to a bug in the version number parsing the directive didn't always work properly. This is fixed.

Fixed closing SFTP connection

Type: Minor
Products: All
ID: 993

SFTP server was not closing connections neither upon receiving an appropriate command (e.g. "bye", "exit", "quit"), nor upon expiration of the inactivity time-out. This is fixed.

Changes In v3.3.0 (825)

Added support for Ethernet-over-VDSL (EoVDSL) interface

Type: New feature
Products: RS900L
ID: 644

RS900L is identical to the RS900 switch with the exception that the optional Fast Ethernet port (port 9) is replaced with an EoVDSL port.

Added support for IEEE 802.11 Wireless LAN interface

Type: New feature
Products: RS900W
ID: 803

RS900W is identical to the RS900 switch with the exception that the optional Fast Ethernet port (port 9) is replaced with an IEEE 802.11 Wireless LAN interface which provides Wireless Access Point functionality.

M969 can now come with 100Base-FX ports

Type: New feature
Products: RS900W
ID: 830

Originally, M969 was equipped with 8 10/1000Base-TX (copper) ports and 2 1000Base-X (fiber) ports. Now the 100Base-FX option is available for the fiber ports.

Multiple (per VLAN) IP interfaces are supported

Type: New feature
Products: All except RMC30
ID: 844

ROS™ provides IP interfaces for several purposes:

- Device management
- Serial-over-IP support (RuggedServer™)
- Other IP related features, e.g. IGMP.

Prior to this ROS™ version, only one IP interface (residing on the Management VLAN) was supported and had to be used for all purposes. Now as many IP interfaces can be configured as many VLANs are supported by the device. This way the device management traffic can be segregated from any other IP related features traffic.

Many-to-one port mirroring is now supported

Type: Enhancement
Products: RS900, RS900G, RS969, RSG2100, RSG2200, RS416
ID: 247

Only one-to-one Ethernet Port Mirroring was supported prior to this ROS™ version, which means only one port could be configured as a Port Mirroring source. Now a list of several Port Mirroring source ports can be configured.

User names are now configurable

Type: Enhancement
Products: All
ID: 727

Prior to this version, ROS™ had a set of predefined user names (“admin”, “operator” and “guest” – each with its corresponding system login access level) and only passwords were configurable. Now the user names are configurable too, thus providing a better flexibility to the user.

Added RSTP “BPDU Guard” protection

Type: Enhancement
Products: All except RMC30
ID: 781

The RSTP standard does not address network security. RSTP must process every received BPDU and take an appropriate action. This opens a way for an attacker to influence RSTP topology by injecting RSTP BPDUs into the network. “BPDU Guard” is a feature that protects the network from BPDUs received by a port where RSTP capable devices are not expected to be attached.

MikroLok maximum message length extended to 1400 bytes

Type: Enhancement
Products: All RuggedServer™ products
ID: 790

The supported MikroLok serial protocol message length was limited to 256 bytes which was found to be not enough for some applications. Now the maximum message length is extended to 1400 bytes.

Added ability to disable fast Ethernet link detection

Type: Enhancement
Products: All except RMC30
ID: 877

Normally the switch is able to detect a link failure and act upon it immediately (within a few milliseconds) - in network architectures with link redundancy this results in a very fast network recovery. However, network devices have been seen that, under some circumstances, cause the link to be continuously bouncing as frequently as hundreds or thousands times a second. Processing so frequent link state changes might take too much of switch CPU resources which might significantly slow down or even block critical switch management applications, such as RSTP. And if RSTP operation is blocked in some switch, it might result in network loops and thus bring the entire network down. So, if there is a reason to believe that end devices attached to the switch can show the described behavior, the user is now able to disable fast link detection to protect the network from a potential serious failure.

Fixed losing management access and serial-over-IP functionality

Type: Critical
Products: All RuggedServer™ products
ID: 852

In a very special, hardly reproducible scenario that involved intensive traffic over device serial ports the device could get locked in some internal process, thus entirely blocking any management and serial-over-IP communication. This is fixed.

Fixed losing DNP.3 connectivity

Type: Critical
Products: All RuggedServer™ products
ID: 854

Upon a certain coincidence of opening and closing DNP sessions, RuggedServer™ could stop accepting any more DNP-over-IP requests until it is rebooted. This is fixed.

Fixed memory leak upon closing Telnet/SSH connection

Type: Critical
Products: All
ID: 912

There was a small memory leak in the process of closing Telnet or SSH management connections. Intensively opening and closing such connections (which some NMS packages do as a part of the network devices discovery process) might eventually cause the system to be unable to open any more management connections. This is fixed.

Fixed updating dynamic Serial-over-IP Device Address Table

Type: Critical
Products: All RuggedServer™ products
ID: 933

When a serial device address is being dynamically relearned its corresponding device address table entry is updated according to the new learned parameters. However, updating the table under a high-rate serial traffic sometimes caused the serial device address table corruption, thus causing loss of connectivity with serial devices. This is fixed.

Fixed RSTP operation on Port Trunk in Alternate/Backup role

Type: Critical
Products: All except RMC30, RS400, RS8000, RS1600
ID: 944

In some cases Port Trunk in Alternate or Backup role was not properly put in RSTP discarding state, even though RSTP Port Status indicated so. It means all ports of the Port Trunk were still forwarding traffic which resulted in network loops and could cause loss of connectivity. This is fixed.

Fixed updating dynamic TIN Device Address Table

Type: Critical
Products: All RuggedServer™ products
ID: 954

Updating the TIN dynamic device address table didn't take effect, so that traffic was still routed to the old path. (NOTE: this problem was created when adding support for TINmod2.) This is fixed.

Fixed losing RawSocket data upon timeout when configured to work with Pack Character

Type: Major
Products: All RuggedServer™ products
ID: 849

When Raw Socket serial-over-IP protocol was configured to pack data for IP transmission upon receiving a Pack Character over a serial interface it discarded the portion of data, if the serial interface timeout expired without receiving the Pack Character. This is fixed – the portion of data is packed and sent out upon the timeout as well.

Fixed occasionally dropping RawSocket-over-TCP connections

Type: Major
Products: All RuggedServer™ products
ID: 880

Upon a certain coincidence of opening and closing RawSocket-over-TCP connections by the end device, RuggedServer™ could improperly drop some new incoming connections. This is fixed.

Fixed slow response to management requests in presence of high-rate broadcast traffic

Type: Major
Products: All except RMC30,RS8000,RS1600
ID: 884

ROS™ implements a mechanism of protecting the device CPU resources from being exhausted in case of a potential Denial-of-Service (DOS) attack. To make the protection as reliable as possible, the parameters of the algorithm were set to some conservative values which caused the protection mechanism to get activated as a result of receiving relatively high-rate broadcast traffic sometimes used in network applications. Activation of the DOS attack protection mechanism caused slow responses to any device management requests (e.g. SNMP, Telnet etc.). This is fixed – the protection algorithm parameters were made less conservative preventing it from being undesirably activated. However, the device is still efficiently protected against a DOS attack.

Fixed losing connectivity between URPC Modbus management application and RTUs

Type: Major
Products: All RuggedServer™ products
ID: 917

In some cases the same IP packet was erroneously sent twice from Modbus Client to Modbus Server (and forwarded by the Modbus Server to the destination RTU). It caused the destination RTU to handle too many requests and thus to delay sending responses. As a result, the requests timed-out in the URPC and the URPC made a decision that connectivity with RTUs was permanently lost. This is fixed.

Fixed detecting Ethernet link state change in timely fashion

Type: Major
Products: RSG2200
ID: 927

Normally ROS™ detects an Ethernet link state change within a few milliseconds. However, if link was lost at least once on port 11 of RSG2200, fast link state detection was not possible any more (link state detection time was up to 2 seconds) until the device reboot. This is fixed.

Fixed RSTP operation on Port Trunk when primary port is down

Type: Major
Products: All except RMC30, RS400, RS8000, RS1600
ID: 938

Port Trunk link is considered to be up, if any of its ports' link is up. However, if Port Trunk primary port's link was down, RSTP always interpreted it as the whole Port Trunk link down. As a result, RSTP put the whole Port Trunk in discarding state, thus preventing any communication through the Port Trunk. This is fixed.

Fixed handling multiple Modbus management connections

Type: Minor
Products: All RuggedSwitch™ products
ID: 723

In some scenarios (e.g. when a link to the device breaks and recovers in the middle of Modbus management polling), the management station opens new Modbus management connection(s) causing the device to handle multiple connections simultaneously. Handling simultaneous Modbus management connections wasn't done properly and sometimes even caused the device reboot. This is fixed.

Fixed read/write access for ROS™ “syslog” and “crashlog” files

Type: Minor
Products: All
ID: 791

ROS™ “syslog” and “crashlog” diagnostic files should have a read-only management access. However, they erroneously had a read/write access. This is fixed.

Fixed SSH session timeout

Type: Minor
Products: All
ID: 796

Once opened, a Secure Shell session stayed permanently open and didn't get closed upon any timeout. This is fixed.

Fixed losing configured Ethernet port name

Type: Minor
Products: All except RMC30
ID: 798

Upgrade to ROS™ v3.2 was causing all configured Ethernet port names to be reset to default names. This is fixed.

Fixed rebooting when processing random input to Telnet TCP port

Type: Minor
Products: All
ID: 828

Sending random data to Telnet TCP port continuously for several minutes could sometimes cause ROS™ to reboot. This is fixed.

Fixed incorrectly retrieved “tcpMaxConn” TCP-MIB (RFC2012) object

Type: Minor
Products: All
ID: 858

According to RFC2012, -1 should be returned for the “tcpMacConn” object, if the maximum number of TCP connections is unknown. However, 0 was erroneously returned instead. This is fixed.

Fixed applying serial port configuration settings to wrong port

Type: Minor
Products: RS401
ID: 863

RS401 serial port configuration settings were actually applied to the wrong port (serial port 1's settings were applied to port 4, port 2's to port 3 and vice versa). This is fixed.

Fixed not supporting “rcDeviceStsTemperature” RUGGEDCOM-SYS-INFO-MIB object in RS8000/RS1600 product series

Type: Minor
Products: RS8000, RS1600
ID: 871

The “rcDeviceStsTemperature” RUGGEDCOM-SYS-INFO-MIB object can not be supported in the early hardware revision of RS8000/RS1600 series units manufactured before year 2003. However, that object was not supported in any RS8000/RS1600 units regardless of the hardware revision. This is fixed.

Fixed reporting reset by watchdog after user initiated reboot

Type: Minor
Products: RS8000, RS1600
ID: 906

In RS8000/RS1600 product series, ROS™ shutdown process was not completing properly, so that the system was eventually reset by the system watchdog. This is fixed.

Fixed improper display of RSTP port status for aggregated ports

Type: Minor
Products: RS900, RS900G, RS969, RSG2100, RSG2200, RS416
ID: 916

All ports aggregated in a port trunk should be displayed as one entry in the RSTP port status table. Instead, after the device reboot, aggregated ports were displayed as multiple entries, one for each port. This is fixed.

Fixed wrong default value of “snmpEnableAuthenTraps” MIB object

Type: Minor
Products: All
ID: 921

An invalid default value of 0 was assigned to the “snmpEnableAuthenTraps” MIB object upon system bootup (rather than 1-enabled or 2-disabled). This is fixed.

Fixed updating statistics data

Type: Minor
Products: All
ID: 935

If a high load on the device CPU occurred, different statistics data (e.g. Serial Port Statistics) could stop updating for a very long period of time (a few weeks) even after the high CPU load is over. This is fixed.

Fixed retrieving BRIDGE-MIB dot1dTpFdb objects

Type: Minor
Products: All except RMC30
ID: 939

BRIDGE-MIB dot1dTpFdb table is a switch MAC Address Table. Entries in the ROS™ MAC Address Table are indexed by a combination of MAC Address and VLAN ID. When more than one VLAN was configured in ROS™ device dot1dTpFdb table entries were retrieved improperly. This is fixed.

Fixed relearning single DNP address from high-rate DNP-over-IP packets

Type: Minor
Products: All RuggedServer™ products
ID: 941

If only one DNP address was present in the DNP Device Address Table and it was being relearned from a high-rate stream of DNP-over-IP packets, the following problems could show up:

- Lost IP connection to the remote RuggedServer™ device
- Lost any management access to the device

This is fixed.

Fixed loading files via Web-based management interface

Type: Minor
Products: All
ID: 952

Loading a file (e.g. while upgrading ROS™ firmware) via Web-based management interface was always failing - success was reported to the user but the file wasn't actually saved in the device memory. This is fixed.

Fixed blocking login access after excessive failed login attempts

Type: Minor
Products: All
ID: 953

To protect the system from a password guessing attack, ROS™ login access should be blocked for as long as one hour, if ten or more failed login attempts are detected within a 5 minute period. However, login access was only blocked for 5 minutes. This is fixed.

Fixed retrieving SNMPv2-MIB objects sysDescriptor and sysName

Type: Minor
Products: All
ID: 958

SNMPv2-MIB objects sysDescriptor and sysName were not retrieved properly. This is fixed.

Fixed processing incorrect URL by Web-based management

Type: Minor
Products: All
ID: 962

When working with the Web-based management interface entering an arbitrary incorrect URL could cause the device to reboot. This is fixed.

Fixed aging out dynamic DNP addresses

Type: Minor
Products: All RuggedServer™ products
ID: 968

Dynamically learned DNP device addresses should age out after a configured aging time, if no packets are received from or transmitted to those addresses. However, all DNP permanently remained in the device address table, even if no activities were detected for them. This is fixed.

Fixed displaying help text for serial port 'Type' parameter

Type: Minor
Products: All RuggedServer™ products
ID: 972

Displaying help text from the serial port 'Type' parameter could cause the device to reboot. This is fixed.



Fixed displaying zero value for Management Inactivity Timeout

Type: Cosmetic

Products: All

ID: 901

When Management Inactivity Timeout was disabled its value was displayed as zero rather than "Disabled". This is 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

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