



Rugged Operating System v3.4.8 Release Notes

October 27, 2008

Copyright © 2008 RuggedCom Inc.

Overview

ROS™ v3.4.8 adds a single enhancement.

- This firmware release supports all RuggedSwitch™ and RuggedServer™ product series.
- Build date: Oct 17 2008 18:12 File Size: 1857570

User Guides

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



Changes In v3.4.8(1604)

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 3.4.x version.

Changes In v3.4.7 (1450)

Added duplicate message elimination for TIN mode2 protocol.

Type: New feature
Products: All RuggedServer™ products
ID: 1377

Software keeps track of messages received from WRD and sent to RBC. Duplicated messages received within a configured time are discarded.

Fixed generating nuisance alarm by multicast filtering

Type: Enhancement
Products: All except RMC30
ID: 738

Switch generates alarm when MAC address can not be learned by switch fabric. As this alarm can be false indication if multicast stream is present in traffic, it is not generated for dynamically learned multicast addresses. It will always be generated on failure to learn unicast address, multicast address configured statically and layer 2 protocol multicast addresses (e.g. STP, GARP, LLDP).

Changes In v3.4.6 (1405)

Fixed “false positive” Port Guard activation

Type: Minor
Products: All except RMC30
ID: 1400

A similar issue was addressed in v3.4.5. However, it was learned that even when tolerating continuous port ‘bouncing-link’ conditions for 3 seconds, there are still occurrences of ‘false positive’ Port Guard activation resulting in shutting down ports for some end devices. It was recognized that responding to a ‘sustained’ bouncing link condition on a port by disabling the port may be too aggressive as it is causing interruption to a customer network.

The instantaneous CPU response to a port ‘bouncing-link’ condition is now mitigated by modulation (i.e. varying the ‘On/Off’ time duty cycle) of the port (PHY) interrupt response – referred to in ROS as the ‘Fast-Link-Detection’ (FDL) facility. In addition the final (steady state) response to a prolonged ‘bouncing-link’ condition will be filtered by significantly lengthening the tolerance-window (to greater than 2 minutes) before a decision will be reached to raise an Alarm to indicate that Port Guard has latched FDL in a disabled state. Unless this alarm has been raised, the ‘Port Guard’ will continuously recover from intermittent ‘bouncing-link’ conditions, without network interruption or manual intervention.

Fixed Relay Agent Operation

Type: Critical
Products: All
ID: 1389

If switch was acting as Relay Agent, the DHCP frames received from client were corrupted during frame type determination. Corrupted frames were not recognized as DHCP frames, but instead were sent to IP stack for processing, which could cause system to crash. This is fixed.



Changes In v3.4.5 (1353)

Fixed “false positive” Port Guard activation

Type: Minor
Products: All except RMC30, RS8000 and RS1600
ID: 1343

The Port Guard feature was implemented to protect the device CPU from being overloaded by processing frequent Ethernet link state changes (i.e. bouncing link) caused by a faulty end device or invalid cable connection (e.g. 10Base-FL to 100Base-FX connection). However, link bouncing for a short period of time (less than a second) is apparently normal for some end devices. Such an event could trigger an undesirable Port Guard activation. To prevent such a “false positive” event, Port Guard is only activated if the link is bouncing for a minimum of 3 seconds.

Changes In v3.4.4 (1323)

Command enhanced to add developer level information for Debugging Purposes

Type: Enhancement
Products: All
ID: 1262

The last ROS™ release (v3.4.3) introduced some significant new OS ‘hardening’ technologies (See ID # 1312). The intended set of diagnostics and recovery enhancements were incomplete however, due to release deadline obligations, and so the implementation has been continued (and validated) with this release.

Specifically, an enhancement to a (‘factory’ mode) system command (‘klog’) was originally planned (for the previous release) to facilitate capturing data which is useful for developer debugging and diagnostics purposes, from the running ‘C’ stack of suspended tasks. Although originally planned to be included in the previous release, the command was NOT fully operational until now.

Changes In v3.4.3 (1297)

Fixed operation under heavy multicast traffic with more than 256 multicast streams

Type: Major
Products: All except RS400 and RMC30
ID: 1289

Received multicast packets should be forwarded to the device CPU, so that ROS™ would be able to perform multicast filtering (IGMP Snooping). Even if a multicast packet shouldn't be filtered by IGMP Snooping, ROS™ still applies internal "multicast filters" to protect the device CPU from being overloaded by processing continuously received multicast frames (streams). The number of such multicast filters was limited to 256, so any additional multicast streams kept being forwarded to the CPU and those streams could overload the CPU, thus blocking different ROS™ applications. To prevent such scenario, forwarding multicast frames to the CPU is disabled, as long as IGMP Snooping is disabled. NOTE: In some products (i.e. RS8000 and RS1600 series), disabling of forwarding multicast frames to the CPU may not be possible due to hardware constraints, so the problem is solved by significantly increasing the number of multicast filters created by the software upon detection of multicast streams.

Fixed processing IP broadcasts received on non-management VLAN on DHCP Relay Agent access ports

Type: Minor
Products: All except RMC30
ID: 1299

ARP packets (broadcasts) received on non-management VLANs on a switch DHCP Relay Agent access port, were ignored. As a result, devices on corresponding VLAN interfaces would be unreachable for IP communication. This is fixed.

Improved ROS™ System Diagnostics and Recovery Capability

Type: Enhancement
Products: All
ID: 1312

ROS™ implements continuous system monitoring which is able to detect and report system anomalies (e.g. insufficient memory resources etc.). ROS™ also takes some actions to recover from detected anomalies.

Those monitoring and recovery mechanisms are now significantly improved:

1. Assigning memory resources to device critical applications (such as RSTP) is prioritized.
2. Detection of and recovery from accidental system lockup (potentially caused by network anomalies, such as DoS attack or traffic bursts) is improved.
3. Better system diagnostic information is available in case of system anomalies detection or/and recovery activation.

Changes In v3.4.2 (1211)

Added support for RS920L Serial Device Server

Type: New Feature
Products: RS920 series
ID: 1129

The RuggedVDSL RS920L is an industrially hardened serial device server and managed Ethernet switch supporting Ethernet over VDSL (EoVDSL). The RS920L can be configured with up to 2 EoVDSL interfaces and 2 serial ports (RS485/RS422/RS232).

Added support for Long-Reach Ethernet-over-VDSL (EoVDSL) Interface

Type: Enhancement
Products: RS900L, RS930L, RS910L, RS920L
ID: 1108

As opposed to the previously supported 2.5Km distance EoVDSL interface, the Long-Reach EoVDSL interface offers communication over a 5Km distance.

RS940G now supports 1000Base-T option for ports 7 and 8

Type: Enhancement
Products: RS940G
ID: 1232

Previously, RS940G was only available with 1000Base-X port type for ports 7 and 8. Now 1000Base-T option is also available.

Fixed problem when frequent link bouncing causes device blocking

Type: Critical
Products: All products except RMC30
ID: 694

Port Guard feature is implemented to protect against faulty end devices or mis-matched fiber ports causing the system to detect a large number of link state change events in a short period of time (link bouncing) causing network failure and device to become unresponsive since most of the system resources are used to process these events. Device would not be able to keep even essential network application properly running (such as RSTP).

If the Port Guard feature is enabled, it can detect abnormal number of link changes. Once problem is detected, the port in question will be disabled to release other device resources to keep network alive.

Fixed unexpectedly closing TCP connections

Type: Minor
Products: All products
ID: 1120

Sometimes a just opened TCP connection (either incoming or outgoing) was unexpectedly closed by ROS™ after about 5 seconds. This is fixed.

Fixed loading factory default configuration

Type: Minor
Products: All products
ID: 1127

Very rarely, running the “Load Factory Default Configuration” command could cause the ROS™ management session to hang and any IP connectivity with the device to be lost until the device reboot. This is fixed.

Fixed retrieving some RSTP status MIB objects

Type: Minor
Products: All except RMC30
ID: 1132

If ‘dot1dStpPortDesignatedBridge’ and ‘dot1dStpPortDesignatedPort’ MIB objects were retrieved for a port trunk’s non-primary port, the ROS™ SNMP response improperly specified their length to be 0 which could cause confusion to some network management applications. This is fixed.

Fixed closing connections by TCP client

Type: Minor
Products: All products
ID: 1143

When trying to close a previously established TCP connection the ROS™ TCP client sometimes failed to do so, so that the connection was only closed later by a TCP timeout. This is fixed.

Fixed simultaneous IP configuration from several management sessions

Type: Minor
Products: All products
ID: 1180

If IP interfaces were configured from several management sessions simultaneously (which is definitely not a normal way of configuring devices), it could cause some IP services to become inaccessible. This is fixed.

Fixed false RSTP “Looped back BPDU” alarm

Type: Minor
Products: All except RMC30
ID: 1184

The RSTP "Looped back BPDU" alarm should be generated when a port receives back the BPDU just sent out of that very port, i.e. actually when a loop-back cable is plugged in the port. However, the alarm was improperly generated, even if two different ports of the switch were interconnected. This is fixed.

Fixed memory leak upon device configuration

Type: Minor
Products: All products
ID: 1189

Modifying some configuration parameters could cause a minor memory leak (note that, although any memory leak is obviously an improper event, the amount of lost memory was totally insignificant for the system operation). This is fixed.

Forwarding static multicast group traffic now always obeys VLAN rules

Type: Minor
Products: RS8000, RS1600
ID: 1230

If a RS8000/RS1600 series device was rebooted or its VLAN configuration was changed after a static multicast group was configured, the multicast group traffic forwarding might not obey VLAN rules (port membership and VLAN tagging) of the VLAN on which the multicast group was configured. This is fixed.

Changes In v3.4.1 (1142)

Added support for 10Base-FL Ethernet ports in RS910

Type: Enhancement
Products: RS910 series
ID: 1129

RS910 can now be populated with Ethernet ports of the 10Base-FL type.

Fixed Web Page Menu shift

Type: Cosmetic
Products: All products
ID: 1126

When expand web server "Configure SNMP" submenu, the submenus: "Configure Security Server", "Configure DHCP Relay Agent" and "Configure Remote Syslog" shifted one level up, which means these submenus became same level as "Administration" main menu instead of under Administration". This is fixed.

Changes In v3.4.0 (987)

Added Preemptive Raw Socket mode

Type: New feature
Products: All RuggedServer™ products
ID: 847

Most SCADA protocols are master/slave and support only a single master device. However some applications want the ability to have multiple masters communicating to IEDs. For example, the SCADA master polling device is the normal background process collecting data from the IED. Occasionally, IED maintenance, configuration, or control may be required from a different master.

This feature allows a maintenance/configuration/control master to interrupt the polling master (i.e. close the TCP connection) in an automatic fashion. The connection with the polling master is automatically restored after the maintenance/configuration/control session is done.

Added TACACS+ security protocol client functionality

Type: New feature
Products: All
ID: 869

TACACS+ protocol provides access control for networked devices via one or more centralized servers. TACACS+ client accepts a username and password and sends a query to a TACACS+ authentication server.

Added support for RS930, RS910, RS940G

Type: New feature
Products: RS930, RS910, RS940G
ID: 870

The RS910 family is an industrially hardened serial device server with an integrated, fully managed, Ethernet switch. It has 2 serial ports, 2 Fast Ethernet ports and one optional EoVDSL (RS910L) or IEEE 802.11 (RS910W) port.

The RS930 family is an industrially hardened, fully managed Ethernet switch supporting EoVDSL. The RS930 has 6 Fast Ethernet 10/100Base-TX ports, one EoVDSL port and one optional EoVDSL (RS930L) or IEEE 802.11 (RS930W) port.

The RS940 is an industrially hardened, fully managed Gigabit Ethernet switch that has 6 10/100/1000Base-T copper ports and two optional 1000Base-X fiber ports.

Added IEEE 802.11 wireless client/bridge functionality

Type: New feature
Products: RS900W, RS930W, RS910W
ID: 982

The IEEE802.11 definition of a (wireless) station limits the station context to a single *endpoint* in a wireless network. The interaction between a single *associated* station and an IEEE802.11 Access-Point (AP) (in *infrastructure mode*) does NOT support layer 2 bridging of traffic for wired devices located 'behind' a wireless station. In other words, the wireless network model expects that only the AP device will be connected to a 'wired' LAN (i.e. fixed-end distribution service), while each station will represent an individual (stand-alone remote) client with a single network address. Examples of a typical IEEE802.11 station device include PDA, mobile gaming consoles (e.g. Sony PSP) and laptops.

The RuggedWireless™ network model extends the IEEE802.11 *infrastructure mode* functionality to provide seamless wireless connectivity to (multiple) network devices connected to the 'switched' LAN side of a single wireless station device. In this way, full layer 2 traffic bridging is achieved between the 'switched' LAN on the AP device and the 'switched' LAN on the Client/Bridge device, while communicating over a wireless medium.

The RuggedWireless™ Client/Bridge extensions include the integration of the following functionality:

- 802.11 infrastructure mode STA
- WDS (Wireless Distribution System) and
- Ethernet bridging

Loaded old format config.csv file is now automatically converted to new format

Type: Enhancement
Products: All
ID: 680

The set and format of ROS™ device configuration parameters have been modified in some major ROS™ versions. So, if a config.csv file originally downloaded from an older ROS™ version was used to configure a device running a newer ROS™ version, some configuration parameters could be lost causing loss of appropriate functionality. Now, when an old format config.csv file is loaded to a device all parameters are automatically converted to the format supported by the running ROS™ version.

Power Supply status information is available via Modbus management

Type: Enhancement
Products: All
ID: 925

Ability to access some basic system control/status parameters via Modbus-over-IP management interface was already supported in previous ROS™ versions. Power Supply status is now added to the set of accessible parameters.

EoVDSL configuration is more flexible

Type: Enhancement
Products: RS900L
ID: 1007

Trying to guarantee reliable EoVDSL connectivity, the EoVDSL control algorithm was too conservative about link quality parameters – a few second noise burst could cause the algorithm to lock on a data rate lower than the one actually provided by the VDSL link. To prevent such scenarios and still always guarantee a reliable link, the following enhancements were made to EoVDSL support:

- EoVDSL throughput can only drop during automatic link scanning. Once locked on the detected best available data rate, EoVDSL does not downgrade throughput.
- In addition to an automatic optimal data rate selection mode, predefined data rates can be configured, thus providing link control flexibility.

Added 'resetserialport' and 'clearserstats' CLI commands

Type: Enhancement
Products: All RuggedServer™ products
ID: 1100

The 'resetserialport' and 'clearserstats' commands are identical to the corresponding existing commands available from the user interface menus, but can be invoked from the command line shell.

Increased maximum outgoing IP packet length

Type: Enhancement
Products: All
ID: 1119

The maximum ROS™ outgoing IP packet length was limited to a single Ethernet frame length. Any application request for a longer packet transmission was discarded by the IP layer and the packet was not sent out. This caused a problem with responding to some NMS SNMP requests which required very long responses.

The maximum outgoing IP packet length increased to 4K bytes.

Fixed DHCP Relay Agent processing of long DHCP packets

Type: Major
Products: All except RMC30
ID: 999

DHCP Relay Agent was failing to properly process DHCP packets longer than a certain limit. As a result, malformed DHCP packets could be sent by DHCP Relay Agent to DHCP clients, if DHCP Server's "Offer" packets contained multiple DHCP options. This is fixed.

Fixed downloading ROS™ file with PuTTY 0.60 SFTP Client

Type: Major
Products: All
ID: 1000

Downloading ROS™ files with PuTTY 0.60 SFTP Client was failing due to improper interaction between the client and server in handling SSH window size. This is fixed.

Fixed LED panel operation

Type: Minor
Products: RSG2100, RSG2200, RS416
ID: 882

Device LED panel was not operational, if any ROS™ file writing (e.g. clearing system log files by invoking "clearlogs" CLI command) was performed immediately after the device bootup. This is fixed.

Fixed SNMPv1 response when retrieving non-existing MIB object

Type: Minor
Products: All
ID: 898

Upon receiving a request to retrieve a non-existing MIB object, SNMPv1 was sending an invalid response. This is fixed.

Fixed configuring SNMPv3 Authentication Key

Type: Minor
Products: All
ID: 957

ROS™ allowed to configure SNMPv3 Authentication Protocol without Authentication Key (i.e. with an empty key string). This is fixed.

Fixed resetting "Time and Date" configuration parameters to factory defaults

Type: Minor
Products: All
ID: 980

When resetting "Time and Date" parameters to factory defaults some parameters should be preserved (e.g. Time, Date and Time Zone) while others should be set to their default value (e.g. NTP Update Period). However, no parameters were set to default. This is fixed.

Fixed TFTP server operation after invalid request

Type: Minor
Products: All
ID: 1003

After an attempt to download ROS™ binary file in ASCII mode TFTP server was no longer accepting any requests, always responding with “TFTP Server Busy” error. This is fixed.

Fixed disabling SNMP authentication traps

Type: Minor
Products: All
ID: 1005

The ‘nmpAuthTrapsEnabled’ MIB object value was not properly checked when sending SNMP Authentication traps, so that the traps were sent, even if they were disabled. This is fixed.

Fixed Telnet login with RADIUS authentication

Type: Minor
Products: All
ID: 1039

User was able to login to a ROS™ management session using configured local credentials, even if the device was configured for RADIUS server authentication. This is fixed.

Fixed processing SNMP multiple bindings set requests

Type: Minor
Products: All
ID: 1044

Setting multiple indexed objects in the same MIB table with one SNMP set request didn't work properly. This is fixed.

Fixed SNMPv3 operation with dynamic IP address

Type: Minor
Products: All
ID: 1057

SNMPv3 didn't respond to any requests, if the device was configured for dynamic IP address assignment. This is fixed.

Fixed unassigning serial protocol from serial port while receiving data

Type: Minor
Products: All RuggedServer™ products
ID: 1103

RuggedServer™ could crash, if a serial port reconfiguration involving unassigning serial protocol from the port was performed while the port was receiving data. This is fixed.

Fixed sending SNMP trap when generating “Crashlog created” or “Configuration suspect” alarm

Type: Minor
Products: All
ID: 1111

The “Crashlog created” and “Configuration suspect” are ROS™ common alarms alerting the user about certain system abnormalities (see appropriate alarm description using ROS™ “alarms” CLI command). When such an alarm is generated an appropriate SNMP trap should be sent. However, the trap was not sent for these two alarms. This is fixed.

Fixed updating Serial Device Address Table in conjunction with RuggedServer™ reboot

Type: Minor
Products: All RuggedServer™ products
ID: 1115

If RuggedServer™ was rebooted after removing and reinserting entries in its Serial Device Address Table, some device functionality (e.g. console interface) could get permanently not functional once traffic was received from a remote serial device server. This is fixed.

Fixed configuring RMC30 serial port #2 via console

Type: Minor
Products: All
ID: 1116

If RMC30 booted in console mode, it would reboot upon an attempt to configure serial port #2, so that configuring serial port #2 via console was not possible. This is fixed.

Fixed configuring SNMPv3 for unsecure mode of operation

Type: Minor
Products: All
ID: 1121

If SNMPv3 parameters “Authentication Protocol” and “Privacy Protocol” were reconfigured from some secure settings to “no authentication” and “no privacy” respectively and the device was not rebooted, SNMPv3 kept rejecting unsecure requests, as if it was still configured for secure mode. 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