



Rugged Operating System v3.5.3 Release Notes

October 27, 2008

Copyright © 2008 RuggedCom Inc.

Overview

ROS™ v3.5.3 adds a single enhancement.

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

- Build date: Oct 17 2008 18:30 File Size: 1994890

User Guides

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



Changes In v3.5.3(1605)

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 3.5.x version.

Changes In v3.5.2 (1543)**RSTP generates BPDUs which are padded with 'additional' (unused) data bytes**

Type: Major
Products: All except RMC30
ID: 1545

With the introduction of MSTP feature supported in ROS v3.5, all BPDUs traffic (regardless of whether the switch is configured for RSTP or MSTP) was being transmitted with a minimum length which was governed by the frame size of the MSTP BPDUs (in bytes). Note that the MSTP standard does not stipulate that 'additional' unused bytes within the BPDU frame should cause any BPDU to be discarded. RuggedCom switches do not discard these longer BPDUs, but rather simply ignore any unused bytes which may be carried within the BPDU frame. However, some third party switches were encountered which do silently discard such BPDUs. This behavior resulted in a failure of the RSTP operation and allowing network loops to be inadvertently created within the network. These extra (unused) data bytes have now been removed from the RSTP BPDU frame.

Changes In v3.5.0 (1165)

Added support for LLDP.

Type: New feature
Products: All except RMC30
ID: 645, 1277

LLDP is a neighbor discovery protocol. It defines a standard method for Ethernet network devices such as switches and routers to advertise information about themselves to other nodes on the network and store the information they discover. Details such as device configuration, device capabilities and device identification can be advertised using this protocol. The LLDP MIB is supported via SNMP.

Added support for MSTP.

Type: New feature
Products: All except RMC30, RS400 and RS8000 and RS1600 families
ID: 845

The *Multiple Spanning Tree Protocol* (MSTP) defines an extension to the RSTP protocol to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks the links that are redundant within each Spanning Tree. If the network contains more than one VLAN, the logical network configured by single STP would work, but it is possible to make better use of the redundant links available by using an alternate spanning tree for different (groups of) VLANs.

Added support for Mirrored Bits serial protocol.

Type: New feature
Products: All RuggedServer™ products
ID: 981

The SEL Mirror Bits communications is a direct relay-to-relay communication protocol that allows protective relays to exchange information quickly and securely.

NOTE: This protocol, even with only one serial port in use utilizes significant CPU resources and is intended for products with a lower number port density (as RMC30).

Added TACACS+/RADIUS based Authorization functionality.

Type: New feature
Products: All
ID: 1205

In previous versions, TACACS+ and RADIUS servers would only *authenticate* users that wanted to log into the device. Privilege level was derived on the device from the username (one of three: guest, operator and admin). *Authorization* functionality is now added, so servers can be configured to assign the correct privilege level to the user.

Backup server is available for both, TACACS+ and RADIUS authentication and authorization.

Add wireless 'Client/IPBridge' Mode to the WLAN Interface.

Type: New feature
Products: RS9x0W
ID: 1218

The 'Client/IP Bridge' feature is the integration of IEEE 802.11 STA and layer 2 NAT functionality. It is based on the following assumptions:

- Only IPv4 and ARP traffic will be bridged
- ARP packets and IP header received over ENET interface should be unencrypted.
- Layer 2 NAT is only applicable to STA (i.e. there is no effect on the is AP).
- Layer 2 NAT is based on {Source Ethernet MAC Address, Source IP Address} for Ethernet frames received on ENET interface of the STA.
- All Ethernet devices on the fixed side of the AP can only see the Ethernet address of STA (not device(s) connected to STA).

Added support for RS i80X Product Series

Type: New Feature
Products: RS i80x series
ID: 1290

The RuggedSwitch™ i800, or *i*-Series, is a family of compact, fully managed Ethernet switches specifically designed to operate reliably in harsh industrial environments. The flexibility of the i800 family allows the user to choose from managed or unmanaged, regular or extended temperature, fiber optical or copper interfaces, and fast or Gigabit Ethernet with up to nine Ethernet ports.

Added support for DHCP server on wireless interface.

Type: New feature
Products: RS9x0W
ID: 1317

The ROS WLAN UI includes new WLAN DHCP table in order to configure DHCP Server functionality in the wireless module.

Added 'Force Half Duplex' mode of operation on serial ports.

Type: New feature
Products: All RuggedServer™ products
ID: 1342

With Force Half Duplex turned 'on' on serial port, the RuggedServer™ can be used to connect one serial master or Ethernet master to multiple devices (slaves) in a fiber ring. The serial port on the server which communicates with master and is connected to the ring must be full duplex mode (RS232 or RS422) and configured to 'Force Half Duplex' mode to block all data received back (i.e. due to the ring topology) during transmission.

Extended ability to manage devices via SNMP.

Type: Enhancement
Products: All
ID: 1304

Rugged NMS needs to collect information about the version of Main and Boot firmware and Configuration files from devices in network. Ability to retrieve required information and issue system commands via SNMP is added.

Increased number of supported VLANs.

Type: Enhancement
Products: All except RMC30, RS400 and RS8000 and RS1600 families
ID: 1333

The maximum number of VLANs is increased to 255 on all products where hardware support is available for such quantity. Limitations on the maximum number are matched to the true hardware capabilities.

Added configurable option for login banner security.

Type: Enhancement
Products: All
ID: 1341

A new configuration option is added to restrict information revealed in the login screen. If the secure option is configured, identity information for the device will not be displayed.

Temperature reading added to the syslog entries.

Type: Enhancement
Products: All
ID: 1345

Each record in syslog.txt file shows temperature reading at the time the record is created. 'Err' would be shown if failing to read temperature.

Added configurable syslog level.

Type: Enhancement
Products: All
ID: 1390

The local syslog.txt file is created to log information useful for monitoring and troubleshooting during the operation. To get as much information as possible for troubleshooting problem in the field, but still avoid unnecessarily huge syslog.txt files in normal operation, a configurable syslog level is supported.

Fixed RMC30 crashing while receiving data.

Type: Major
Products: All
ID: 1052

RMC30 device was crashing when a particular source of data (pt-to-pt radio) was connected to the port. The problem was created by delays between data characters (about the time needed to transfer 64 characters) introduced by data source.

Fixed STP status on WLAN port when link is down.

Type: Major
Products: RS9x0W
ID: 1137

Although WLAN was disabled, STP status on port remained 'forwarding'; consequently RSTP did not function properly if the WLAN port was involved. From now on, the WLAN port will always act as an 'edge' port from an STP prospective.

Fixed failure to save file to flash if 'reset' was issued right after file was transferred to the device.

Type: Major
Products: All
ID: 1248

Issuing reset command too soon after file transfer is finished sometimes prevented file from being saved. The process that saves data is not activated as soon as file is transferred. Resetting device after finishing transfer, but before activating task to save it to the flash memory would result in failure to save transferred file. This problem is solved by properly synchronizing the two tasks that handle file transfer and saving to the flash memory.

Fixed problem when IGMP did not work If many static MAC addresses were configured.

Type: Major
Products: All
ID: 1321

This problem was a result of insufficient internal resources reserved for this feature.

Fixed false indication of configuration suspect when forbidden ports are configured for VLAN.

Type: Minor
Products: All
ID: 792

A false alarm was generated due to internal tables' interdependences when forbidden ports were checked prior the all other tables have been initialized and set.

Fixed failure to update/retrieve for modular devices by SNMP and/or SQL command.

Type: Minor
Products: All
ID: 1107, 1147

Traversing port tables for modular devices where some ports where missing was improper.

Fixed problem with IP communication when multiple gateways were configured.

Type: Minor
Products: All
ID: 1130

Gateways were not implemented properly in conjunction with multiple interfaces (one per IP Interface). For example, when ping command was issued, a list of gateways was used in round-robin fashion to send response ; some responses were lost for ICMP message sender.

Gateways are removed from the IP Interfaces table. New UI menu item is added to properly configure and use the list of gateways.

Fixed toggling safe fail relay pin after reboot.

Type: Minor
Products: All
ID: 1155

The 'Fail-Safe' relay was set to the OFF state at the end of the boot up process which improperly indicated false state of device.

Fixed failure to retrieve RMON History Samples entry with SNMP Get command.

Type: Minor
Products: All
ID: 1162

When trying to retrieve a value from RMON History Samples table entry using Get command (specific index), devices returned 'nosuchInstance', although object existed in the table.

Fixed retrieval of ifSpeed object on 100FX ports if link was down if speed setting is 'Auto'.

Type: Minor
Products: All
ID: 1163

For link down, capability on 100FX link was mistakenly marked as 1GB in 'Auto' setting of speed variable.

Fixed inability to forward longer DNP messages on low baud rates.

Type: Minor
Products: All RuggedServer™
ID: 1219

DNP messages received on serial port that were longer than 52 bytes if baudrate was 1200 bps could not be handled properly. Data were mistakenly discarded due to improper time measuring between two characters received on serial port.

Fixed crashing when configuration file with long strings was downloaded.

Type: Minor
Products: All
ID: 1264

If configuration file was created with tools that generate comas rather than empty lines, this problem occurred as empty line is always expected and must be present in configuration table before table names. Problem is resolved allowing two comas (that are created rather than empty line) to represent empty line in configuration file.

Fixed erroneous retrieval of objects with syntax unknown for SNMPv1.

Type: Minor
Products: All
ID: 1265

Objects with SNMPv2c syntax that was not supported and is not compatible with any SNMPv1 syntax (Counter64) were retrieved, which is an error condition for SNMP management tool. These objects will not be retrieved and 'No such name' will be returned as per rfc 3548.

Fixed losing SSH connectivity caused by command execution required.

Type: Minor
Products: All
ID: 1287

Command execution via SSH opening sequence is not supported. After receiving such a request, current connection was not properly clean up and new connection could not be established.

Fixed losing IP Interface configuration when switching to VLAN-unaware mode.

Type: Minor
Products: All
ID: 1292

If maximum number of VLANs supported by device was configured and device reconfigured to VLAN-unaware mode, management interface information (IP address) was lost.

Fixed losing SSH connectivity after attempt to open multiple SFTP sessions.

Type: Minor
Products: All
ID: 1300

After file transfer was finished SSH/SFTP connection was erroneously marked as closed. To continue function properly, connection had to be closed by the client before new one was requested. Problem is fixed leaving connection in proper open state until it is deliberately closed.

Fixed 100FX FEFI support in M969.

Type: Minor
Products: M969
ID: 1316

In M969 products 100FX FEFI feature erroneously was always disabled.

Fixed response to Set Request for some objects from BRIDGE-MIB.

Type: Minor
Products: All except RMC30
ID: 1339

Set request for object dot1dStpPriority from BRIDGE-MIB was reported as success, but actually, value erroneously has not been changed in configuration file.

Fixed contents of variable bindings for SNMPv1 LlinkUp/LinkDown trap.

Type: Minor
Products: All except RMC30
ID: 1383

Link Up/Down traps (SNMPv1) were sent without variable bindings defined by IF-MIB. Information about failed, so for NMS it was unknown for which port link changed.

Fixed crashing when SQL command with '*' character was issued from Linux.

Type: Minor
Products: All
ID: 1407

Problem is caused because the Linux command line substituted the symbol '*' with very long string (all file names in current directory). RSH module was not protected from cases like that.

Fixed configuration update for Radius Server.

Type: Minor
Products: All
ID: 1421, 1442

Radius Server configuration did not accept change of 'secret' or management IP address. To apply changes, device had to be rebooted.

Fixed update of number of MAC addresses learned in Port Security table.

Type: Minor
Products: All
ID: 1437

Number of learned MAC addresses in Port Security table sometimes appeared to be negative (-1).

Fixed temporary data storm occurring after switch reboot.

Type: Minor
Products: All except RMC30
ID: 1440

Because of flow in shutdown process, system crashed after issuing reset command before actually ports were disabled. That cause neighbor ports RSTP state to be improperly changed from blocking to forwarding and storm occurred for certain amount of time, until switch is booted up.

Removed trace entry created on TIMEOUT on serial ports.

Type: Minor
Products: All RuggedServer™
ID: 1445

Timeout is a legal event which can happen several times before complete packet is received on serial port, so this trace was very confusing: customers complained about seeing many TIMEOUTs before receiving full packet, considering them as faulty conditions.

Fixed losing VLAN membership for dynamically learned VLANs.

Type: Minor
Products: All except RMC30
ID: 1446

VLANs membership was lost for some dynamically learned VLANs due to packets loss caused by improper initialization of learning process.



Fixed failure to set RSTP port priority to 192

Type: Minor

Products: All except RMC30

ID: 1447

Mistakenly, value of 192 for RSTP port priority could not be set. The value of 194 was allowed instead.

Fixed help text for private and encryption keys in SNMP User Table.

Type: Cosmetic

Products: All

ID: 1199

Help text did not describe all the possible values for private and encryption keys.

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