

Rugged Operating system on Linux (ROX) Release Notes v1.14.3

July 6th, 2010

Copyright © 2010 RuggedCom Inc.

Summary

ROX 1.14.3 - Overview.....	4
IMPORTANT NOTES.....	4
New Upgrade Procedure.....	4
Upgrade of T3 Firmware for E3 support.....	4
IPsec Transition from KLIPS to Netkey.....	4
Removal of Automatic Upgrade Option.....	5
Use of /32 instead of /30 for static routes in WAN connections.....	5
RX1100 Units equipped with 256 MB flash drive.....	5
User Guides and Notes.....	5
Changes in ROX 1.14.3 (2666).....	6
Provide external trigger to backup link tests (E 2730).....	6
Provide SNMP trap upon power supply state change (E 2744).....	6
AM: Deleted ports/protocols are still available (Ma 2501).....	6
RX1000 v1 occasionally stops receiving unicast traffic (Ma 2336).....	6
T1 card generate lots of OOF alarms (Ma 2773).....	6
wanpipe interface generates an inordinate amount of overruns (Ma 2775).....	7
DHCP Relay does not work over GRE tunnel or WAN interface (Ma 2781).....	7
V1 router crashed when heavy traffic is sent on Ethernet ports(Ma 2783).....	7
T1/E1 channel group with non-continuous time slot is broken (Ma 2820).....	7
DS3 Communications cannot resume after cable re-connected (Ma 1851).....	7
rip does not advertise routes correctly at startup time (Mi 2134).....	8
webmin static route page should not automatically add default gateway (Mi 2181).....	8
Some webmin page access control does not work properly (Mi 2810).....	8
webmin: link backup time calculation incorrect (Mi 2776).....	8
XON/XOFF chars is still filtered when flow control is disabled (Mi 2937).....	8
Release Notes of Previous ROX Releases.....	9
Changes in ROX 1.14.2 (2345).....	10
Access Manager (NF 2358).....	10
SNMP trap on configuration changes (E 2287).....	10
IPSec hash option (E 2440).....	10
MTU Configuration for GRE tunnel (E 2442).....	10
sysobjectID update(E 2456).....	11
NTP sending packet binding to source IP address (E 2372).....	11
keepalive_route restart bind9 on master/slave/fault changes (E 2423).....	11

Signal strength detection for PCI/based cellular modems (E 1959).....	11
IPsec routes vanish in some cases (Ma 2387).....	11
Link backup incorrectly does ping tests on primary ethernet interfaces (Ma 2130).....	12
SNMP daemon memory leak (Ma 2250).....	12
Sensor test in BIST array of tests (Ma 2335).....	12
"Static Routes" page disappeared (Mi 2143).....	12
RIP interface Authentication changes not saved (Mi 2096).....	12
No SNMP V3 trap sent when auth = SHA1 (Mi 2517).....	13
ROX 1.14.1 - Overview.....	14
IMPORTANT NOTES.....	14
New Upgrade Procedure.....	14
Upgrade of T3 Firmware for E3 support.....	14
IPsec Transition from KLIPS to Netkey.....	15
Removal of Automatic Upgrade Option.....	15
Use of /32 instead of /30 for static routes in WAN connections.....	15
User Guides and Notes.....	15
Changes in ROX 1.14.1 (1887).....	15
PCI based cellular modem - CDMA/EVDO and HSxPA (NF 1959).....	15
Watchdog not functional (C 1916).....	15
VRRP state change on ppp interfaces (Ma 1656).....	16
ipsec does not work with Greenbow client (Ma 1858).....	16
T3 / E3 Performance degradation on Smaller Packet Size (Ma 1877).....	16
Primary link cannot take over after reboot when link backup configured (Ma 1914).....	16
Customer Banner does not work properly for webmin (Mi 1917).....	16
DHCP client does not update the default gateway address (Mi 1772).....	17
Webmin archive restore is broken (Mi 1923).....	17
MLPPP clock changing will lost mlppp interface (Mi 1912).....	17
Chassis photo of 100FX MM LC(12-11-0046) missing (Mi 1927).....	17
MLPPP cannot resume after cable plug back to CISCO (Mi 1931).....	17
Webmin prevents entering several access srcIP under same community name (Mi 1951).....	17
Generic ping link verification (Mi 1956).....	18
ROX 1.14.0 - Overview.....	19
User Guides.....	19
Changes in ROX 1.14.0 (1495).....	20
BGP Protocol (NF 1498).....	20
Routing of packets according to specific types (NF 1497).....	20
IPv6 Phase 1 (NF 1501).....	20
Synchronous serial (NF 1507).....	20
Limited LAN Bridging (NF 1509).....	20
Link Layer Discovery Protocol (LLDP) (NF 1558).....	21
Telnet access (NF 1625).....	21
PPP Dial on Demand (NF 1629).....	21
Multilink PPP (NF 1557).....	21
En/disabling of sending ICMP redirects (NF 1678).....	21
E3 Support (NF 1696).....	21
PPP/L2TP (NF 1459).....	22
DHCP relay (NF 1782).....	22
SNMPv3 access control settings cause snmpd to stop (Ma 1705).....	22
Unwanted DNP debug notifications caused DNP message losses (Ma 1619).....	22
Wanpipe driver update (Ma 1646).....	22

SNMPD has memory leak and crash sometime (Ma 1452).....	23
GRE not working after wanrouter restarted (Ma 1683).....	23
Failure to generate SNMPv3 Traps when link up/down (Ma 1655).....	23
SerServer stop running when using TCPModbus (Ma 1649).....	23
CDMA Cellular Modem Support (E 1118).....	23
2-stage upgrade procedure (E 1693).....	23
SNMP traps: textual interface name in ifName OID (E 1861).....	24
System logs: Added support for custom src IP (E 1865).....	24
Radius enhancement - source IP customization (E 1866).....	24
VRRP monitoring of physical interfaces (E 1867).....	24
Improve GOOSE tunnels performance (E 1771).....	24
GMT/UTC time options (E 1607).....	25
IPSec extra configuration options (E 1508).....	25
GRE IP address / multicast configuration (E 1677).....	25
Trace function for DDS in Frame Relay mode broken (Mi 1638).....	25
Webmin and time zone changes (Mi 1574).....	25
Frame Relay configuration accept invalid DLCI number (Mi 1762).....	25
MTU default values not restored by Webmin (Mi 1706).....	26
Snort local logging to different log files (Mi 1484).....	26
Online help: Some graphic formats are not handled (Mi 1609).....	26
Unable to clear the Frame Relay interface statistics (Mi 1623).....	26
Webmin accept illegal character (Mi 1621).....	26
Invalid DNS server makes Webmin slow to serve pages (Mi 1511).....	26
Radius Server Adjustments (Mi 1700).....	27
Traffic Control rules on the modem PPP link is broken (Mi 1682).....	27
Webmin allows the taken 24th time slot to be configured (Mi 1681).....	27
Quagga doesn't restart after NTP server restarted (Mi 1680).....	27
Non-default Snort rules were restored to default values (Mi 1675).....	27
RIP version control on T1/E1 fails (Mi 1685).....	28
Dummy interface is accepting invalid IP address (Mi 1742).....	28
Automatic Upgrade Feature Removal (Mi 1823).....	28
Security Updates.....	29
Remote Vulnerability with Openswan (CVE-2009-0790).....	29
SNMPv3 Authentication Bypass Vulnerability (CVE-2008-0960).....	29
Integer overflow in net-snmp (CVE-2008-4309).....	29
Buffer overflow in the __snprint_value function (CVE-2008-2292).....	29
SNMPv3 HMAC verification vulnerability (CVE-2008-0960).....	30
Signal handler race condition (CVE-2006-5051).....	30
Upgrade Instructions.....	31
Type of Changes.....	34
Contacting RuggedCom.....	35

ROX 1.14.3 - Overview

ROX 1.14.3 builds on the features introduced in the previous ROX 1.14.n versions (see second part of these Release Notes for a description of the previous ROX releases), adds some bug fixes as well as a few enhancements such as a Power Supply state change SNMP trap and the capability of triggering link failover tests remotely.

IMPORTANT NOTES

New Upgrade Procedure

The upgrade procedure now allows a *direct upgrade* from previous ROX versions as early as ROX 1.10.0. It is now possible to do a one-step upgrade from an earlier version of ROX to ROX 1.14.x. In order to do so, the upgrade procedure is now in two subsequent phases. When upgrading from a previous ROX version that is older than ROX 1.14.x, a first upgrade stage consisting of a Webmin upgrade will take place. Following that stage, the upgrade procedure should be manually re-started for the full upgrade to take place. See also 'Upgrade Instructions' at the end of this document.

Upgrade of T3 Firmware for E3 support

ROX 1.14.x includes an updated WAN driver that supports E3 functionality when the appropriate hardware is found. In order to function properly with ROX 1.14.x the firmware of the T3/E3 cards must be upgraded during a ROX upgrade. A warning to that effect is issued during the upgrade procedure. The actual T3/E3 firmware update will be performed at the end of the upgrade. On slower routers this may take up to 20 minutes, whereas on version 2 routers this is a matter of 3-4 minutes. The warning notice issued during the upgrade procedure will give an estimate of the needed time. During the firmware upgrade, all T3 interfaces will be non-operational. Please reschedule the upgrade to a convenient time if it is deemed that the firmware upgrade downtime is significant. This firmware update is mandatory since ROX 1.14.x will not interoperate with older T3 firmware versions.

IPsec Transition from KLIPS to Netkey

ROX 1.14.x's IPsec mechanism now works only in Netkey mode. When doing an upgrade, units using a KLIPS configuration will issue a warning pertaining to the update of the configuration to Netkey prior to perform a system upgrade. In such cases, the KLIPS configuration will have to be moved to a Netkey configuration using the existing unit. Only after this is done can a system upgrade be performed. See the "Upgrade Instructions" section for an example of this warning message. As described in the warning notice, you can use the Server Configuration option to then switch to policy-based VPN (i.e. Netkey) and the adjust your existing firewall rules. After this is

done, you can move forward with the upgrade procedure.

Removal of Automatic Upgrade Option

The Automatic Upgrade option has been removed in ROX 1.14.x. If this feature was previously enabled, any scheduled upgrade times will no longer be observed after the upgrade. This was removed to support the new upgrade procedure.

Use of /32 instead of /30 for static routes in WAN connections

The netmask of point-to-point configurations is now fixed to /32. Previous configurations using /30 will be converted to /32 during the upgrade and a static route will be added.

RX1100 Units equipped with 256 MB flash drive

Very few RX1100 units were shipped at an early phase, equipped with 256 MB flash cards. With the additional packages required to have Access Manager the disk space on 256 MB flash cards becomes too little for a RX1100 units equipped with such flash disks to support this feature. In such a case RuggedCom support should be contacted. Any attempt to upgrade such a unit will abort with a warning.

User Guides and Notes

All user guides are available from the RuggedCom Web site at www.RuggedCom.com. Please refer to the ROX 1.14.3 user guide. Please also refer to the 1.14.3 Process List description for detailed information about the running processes that constitutes the ROX system.

Changes in ROX 1.14.3 (2666)

Provide external trigger to backup link tests (E 2730)

Type: Enhancement
Products: RX1000/1100
ID: 2730

This enhancement provides a means of scheduling backup link tests via

SSH with the same functionality as provided by the user interface. This was previously Service Bulletin RC-1142-006.

Provide SNMP trap upon power supply state change (E 2744)

Type: Enhancement
Products: RX1000/1100
ID: 2744

This is an enhancement to the SNMP offering of the RX1000. It consists of being able to send a SNMP trap when the status of a power supply changes, according to the OID definition of RUGGEDCOM-TRAPS-MIB. A power supply trap will be sent once the SNMP traps are configured on a unit. See the Ruggedcom MIBs for trap definition.

AM: Deleted ports/protocols are still available (Ma 2501)

Type: Major
Products: RX1100
ID: 2501

This addresses the complete deletion of access rights when a user was allowed to access secured devices over a set of ports and protocols. The access was still available even after the user was removed from Access Manager. Updating the Secpac had no effect.

RX1000 v1 occasionally stops receiving unicast traffic (Ma 2336)

Type: Major
Products: RX1000
ID: 2336

This item fixes a problem in which it was observed that on older V1 RX1000 routers occasionally would stop receiving unicast traffic.

T1 card generate lots of OOF alarms (Ma 2773)

Type: Major
Products: RX1000/RX1100
ID: 2773

This fix addresses a problem in which a T1 card repeatedly goes OOF and after 10s seconds, go to connected again. Then after several minutes (sometimes 6 minutes, sometimes 15 minutes, sometimes 30 minutes), it goes OOF again.

wanpipe interface generates an inordiante amount of overruns (Ma 2775)

Type: Major
Products: RX1000/RX1100
ID: 2775

This fixes a problem in which an extremely large amount of overruns were generated by the wanpipe driver, each one of them logged and causing the router to slow down to a crawl.

DHCP Relay does not work over GRE tunnel or WAN interface (Ma 2781)

Type: Major
Products: RX1000/RX1100
ID: 2781

This fixes a problem in which using DHCP Relay over GRE tunnel did not work.

V1 router crashed when heavy traffic is sent on Ethernet ports(Ma 2783)

Type: Major
Products: RX1000/RX1100
ID: 2783

This fixes a problem in which early versions of the RuggedRouter (V1 with the lesser RAM and CPU capabilities) crashed when being under exterme Ethernet data load. Please note that V1 RuggedRouters stopped shipping by the end of 2007, the current V2 units taking over.

T1/E1 channel group with non-continuous time slot is broken (Ma 2820)

Type: Major
Products: RX1000/RX1100
ID: 2820

This fixes a problem in which it was found that E1 did not work with channel group with non-continuous time slot. That was observed when trying to connect to a Cisco router in E1 mode with non-continuous time slot.

DS3 Communications cannot resume after cable re-connected (Ma 1851)

Type: Major
Products: RX1000/RX1100
ID: 1851

This fixes a problem in which it was found that DS3 did not re-established when the physical link was brought down.

rip does not advertise routes correctly at startup time (Mi 2134)

Type: Minor
Products: RX1000/1100
ID: 2134

This fixes a problem in which if the peer router reboots, the subnet will be advertised from the peer router even if the ethernet cable is not connected on the interface of the peer router.

webmin static route page should not automatically add default gateway (Mi 2181)

Type: Minor
Products: RX1000/1100
ID: 2181

This fixes a problem in which when the default gateway is obtained dynamically, the Webmin user interface static route page will still automatically add this default gateway when user clicks this page.

Some webmin page access control does not work properly (Mi 2810)

Type: Minor
Products: RX1000/1100
ID: 2810

This item fixes the ability for a guest user login to change the settings for the irigb/1588 and cell modem.

webmin: link backup time calculation incorrect (Mi 2776)

Type: Minor
Products: RX1000/1100
ID: 2776

This fixes a problem in which the user interface webmin did not calculate the time correctly when setting a test interval for the backup link.

XON/XOFF chars is still filtered when flow control is disabled (Mi 2937)

Type: Minor
Products: RX1000/1100
ID: 2937

This addresses a problem in which control code characters were still filtered out of the data stream even when flow control was disabled, preventing some data payloads to be transferred.

Release Notes of Previous ROX Releases

The following sections starting next page recalls the Release Notes of the previous ROX releases of the same 1.14.x series.

Changes in ROX 1.14.2 (2345)

Access Manager (NF 2358)

Type: New Feature
Products: RX1100
ID: 2358

Industrial Defender's Access Manager secure communications system provides a system-level approach to protecting substation equipment from unauthorized access and enables compliance with NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) 002-009 Cyber Security standards. See the Access Manager documentation for server side installation. The RX1100 provides on-line installation instructions for the client agent, in the Release Notes of the Industrial Defender Main Menu.

SNMP trap on configuration changes (E 2287)

Type: Enhancement
Products: RX1000, RX1100
ID: 2287

ROX 1.14.2 enhances the SNMP functionality by allowing one v2c or v3 trap to be sent when a configuration change is made. The trap definition is contained in RUGGEDCOM-TRAPS-MIB, as 'cfgChangeNoRevTrap'. The configuration change trap is configured in the SNMP Trap Configuration section.

IPSec hash option (E 2440)

Type: Enhancement
Products: RX1000, RX1100
ID: 2440

IPsec is enhanced by being able to specify which method to use for IKE/ESP amongst either MD5 or SHA1.

MTU Configuration for GRE tunnel (E 2442)

Type: Enhancement
Products: RX1000, RX1100
ID: 2442

GRE Tunnel functionality is augmented by being able to specify the MTU value. This allows for fine-tuning in some network setups. Previously the MTU was fixed to 1476.

sysobjectID update(E 2456)

Type: Enhancement
Products: RX1000, RX1100
ID: 2456

In order to identify itself better and being able to distinguish between various types of RuggedRouters, the sysobjectOID was modified in the following way: the RX1000's value is: .1.3.6.1.4.1.15004.2.4.1 whereas the RX1100 value is: .1.3.6.1.4.1.15004.2.4.2. This new sysobjectOID is sent on configuration change traps (2287) only.

NTP sending packet binding to source IP address (E 2372)

Type: Enhancement
Products: RX1000, RX1100
ID: 2372

This enhancement allows the ntp daemon to actually bind to a source IP address from an assigned interface when sending packets. Previously the ntp daemon would only use the dummy interface.

keepalive_route restart bind9 on master/slave/fault changes (E 2423)

Type: Enhancement
Products: RX1000, RX1100
ID: 2423

bind lacks in automatic recognition of new IP addresses. Having keepalive restarting bind helps in quick updating of the system when interface status changes are happening.

Signal strength detection for PCI-based cellular modems (E 1959)

Type: Enhancement
Products: RX1000, RX1100
ID: 1959

This enhancement adds the ability of getting the signal strength value of PCI-based cellular modems by using the PCI bus of the modem (as opposed to using a serial interface). This allows for being able to get the signal strength when an active connection is taking place.

IPsec routes vanish in some cases (Ma 2387)

Type: Major
Products: RX1000, RX1100
ID: 2387

When a PPPoE connection on ADSL goes down, the ppp interface goes away until the PPPoE session returns. This takes out static routes created by ipsec and they are not restored unless

ipsec is restarted. The related static routes of ipsec tunnels are now added when the ppp interface is brought up.

Link backup incorrectly does ping tests on primary ethernet interfaces (Ma 2130)

Type: Major
Products: RX1000, RX1100
ID: 2130

This fixes the link backup utility which tried to reach a ping target beyond the reach of the primary ethernet interface by using the source ip when the first ping failed.

SNMP daemon memory leak (Ma 2250)

Type: Major
Products: RX1000, RX1100
ID: 2250

This fixes a memory leak in the SNMP daemon.

Sensor test in BIST array of tests (Ma 2335)

Type: Major
Products: RX1000, RX1100
ID: 2335

The CPU voltages, as well as the PS2 and battery voltages were added to the tests in BIST mode.

"Static Routes" page disappeared (Mi 2143)

Type: Minor
Products: RX1000, RX1100
ID: 2143

The Resolution order option in DNS configuration made the static route page disappear in Webmin by bypassing any use of the static hosts definitions. Several components are using this static definition if only for the localhost entry. Option was removed.

RIP interface Authentication changes not saved (Mi 2096)

Type: Minor
Products: RX1000, RX1100
ID: 2096

This fixes a bug related to the update of ripd configuration when authentication parameters changed.

No SNMP V3 trap sent when auth = SHA1 (Mi 2517)

Type: Minor
Products: RX1000, RX1100
ID: 2517

This fixes a bug regarding the configuration of SNMP V3 traps when a trap was configured with authentication set to SHA1.

Rugged Operating system on Linux (ROX) Release Notes v1.14.1

July 29th, 2009
Copyright © 2009 RuggedCom Inc.

ROX 1.14.1 - Overview

ROX 1.14.1 builds on the features introduced in ROX 1.14.0 (see second part of these Release Notes for a description of ROX 1.14.0) and adds bug fixes regarding the watchdog functionality, Greenbow IPsec Windows client support, T3/E3 performance improvements.

IMPORTANT NOTES

New Upgrade Procedure

The upgrade procedure now allows a *direct upgrade* from previous ROX versions as early as ROX 1.10.0. It is now possible to do a one-step upgrade from an earlier version of ROX to ROX 1.14.x. In order to do so, the upgrade procedure is now in two subsequent phases. When upgrading from a previous ROX version that is older than ROX 1.14.x, a first upgrade stage consisting of a Webmin upgrade will take place. Following that stage, the upgrade procedure should be manually re-started for the full upgrade to take place. See also 'Upgrade Instructions' at the end of this document.

Upgrade of T3 Firmware for E3 support

ROX 1.14.x includes an updated WAN driver that supports E3 functionality when the appropriate hardware is found. In order to function properly with ROX 1.14.x the firmware of the T3/E3 cards must be upgraded during a ROX upgrade. A warning to that effect is issued during the upgrade procedure. The actual T3/E3 firmware update will be performed at the end of the upgrade. On slower routers this may take up to 20 minutes, whereas on version 2 routers this is a matter of 3-4 minutes. The warning notice issued during the upgrade procedure will give an estimate of the needed time. During the firmware upgrade, all T3 interfaces will be non-operational. Please reschedule the upgrade to a convenient time if it is deemed that the firmware upgrade downtime is significant. This firmware update is mandatory since ROX 1.14.x will not interoperate with older T3 firmware versions.

IPsec Transition from KLIPS to Netkey

ROX 1.14.x's IPsec mechanism now works only in Netkey mode. When doing an upgrade, units using a KLIPS configuration will issue a warning pertaining to the update of the configuration to Netkey prior to perform a system upgrade. In such cases, the KLIPS configuration will have to be moved to a Netkey configuration using the existing unit. Only after this is done can a system upgrade be performed. See the "Upgrade Instructions" section for an example of this warning message. As described in the warning notice, you can use the Server Configuration option to then switch to policy-based VPN (i.e. Netkey) and the adjust your existing firewall rules. After this is done, you can move forward with the upgrade procedure.

Removal of Automatic Upgrade Option

The Automatic Upgrade option has been removed in ROX 1.14.x. If this feature was previously enabled, any scheduled upgrade times will no longer be observed after the upgrade. This was removed to support the new upgrade procedure.

Use of /32 instead of /30 for static routes in WAN connections

The netmask of point-to-point configurations is now fixed to /32. Previous configurations using /30 will be converted to /32 during the upgrade and a static route will be added.

User Guides and Notes

All user guides are available from the RuggedCom Web site at www.RuggedCom.com. Please refer to the ROX 1.14.1 user guide. Please also refer to the 1.14.0 Process List description for detailed information about the running processes that constitutes the ROX system.

Changes in ROX 1.14.1 (1887)

PCI based cellular modem - CDMA/EVDO and HSxPA (NF 1959)

Type: New Feature
Products: RX1000, RX1100
ID: 1959

Watchdog not functional (C 1916)

Type: Critical
Products: RX1000, RX1100
ID: 1916

A new configuration option for the watchdog feature made it incompatible with the system. This bug fixe re-establishes watchdog functionality.

VRRP state change on ppp interfaces (Ma 1656)

Type: Major
Products: RX1000, RX1100
ID: 1656

This bug fix addresses a situation in which VRRP would not observe a state change on PPP interfaces.

ipsec does not work with Greenbow client (Ma 1858)

Type: Major
Products: RX1000, RX1100
ID: 1858

This problem resolution addresses the functionality of IPsec when a Greenbow client is used. This bug happens not only for aes128, but for all of the phase 1 protocols as far as the remote side chooses DH group other than 1024/1535.

T3 / E3 Performance degradation on Smaller Packet Size (Ma 1877)

Type: Major
Products: RX1000, RX1100
ID: 1877

A degradation in performance was noticed when using small UDP packets of 512 bytes and below. This bug fix addresses this problem and brings performance back to the regular level.

Primary link cannot take over after reboot when link backup configured (Ma 1914)

Type: Major
Products: RX1000, RX1100
ID: 1914

This problem resolution addresses a situation where, once a primary link has failed and is available again after a reboot of the unit, the route would not be set to go through this link if the ping target for the link backup function is not directly connected.

Customer Banner does not work properly for webmin (Mi 1917)

Type: Minor
Products: RX1000, RX1100
ID: 1917

This minor bug fix addresses a problem in which webmin would not display the session message as part of the login screen after the banner was modified.

DHCP client does not update the default gateway address (Mi 1772)

Type: Minor
Products: RX1000, RX1100
ID: 1772

This bug fix addresses a minor problem where the DHCP client gets the Default gateway address from the DHCP server, but when the Default Gateway address is changed in the DHCP server, the DHCP client would not notice it.

Webmin archive restore is broken (Mi 1923)

Type: Minor
Products: RX1000, RX1100
ID: 1923

This minor bug fix concerns the quagga file ownership, which is not set properly after a webmin archive restore was made. This would prevent quagga from restarting after a reboot of the unit.

MLPPP clock changing will lost mlppp interface (Mi 1912)

Type: Minor
Products: RX1000, RX1100
ID: 1912

This minor bug fix addresses a situation in which the changing of T1's clocking on a T1 maxim card would result in loosing the MLPPP interface (ppp50). Note: MLPPP interface would not disappear if the router providing the Master Clocking is changed later.

Chassis photo of 100FX MM LC(12-11-0046) missing (Mi 1927)

Type: Minor
Products: RX1000, RX1100
ID: 1927

This bug fix concerns a 100FX MM LC card chassis picture that would not be shown in the webmin user interface, as part of the unit's picture.

MLPPP cannot resume after cable plug back to CISCO (Mi 1931)

Type: Minor
Products: RX1000, RX1100
ID: 1931

This bug fix addresses a situation when all cables are unplugged and plugged back in a short time, preventing mlppp re-negotiation of the link.

Webmin prevents entering several access srcIP under same community name (Mi 1951)

Type: Minor

Products: RX1000, RX1100
ID: 1951

This bug fix concerns a situation where Webmin would prevent the creation of different source IP under the same community name, even though the functionality was allowed.

Generic ping link verification (Mi 1956)

Type: Minor
Products: RX1000, RX1100
ID: 1956

This addition enables the pinging of a target and, in case of failure, to perform an action. Two pre-defined actions are included, one concerning MLPPP and one concerning the cellular modem functionality. It is also possible to add any other customized action.

Rugged Operating system on Linux (ROX) Release Notes v1.14.0

June 3rd, 2009

Copyright © 2009 RuggedCom Inc.

ROX 1.14.0 - Overview

ROX™ v1.14.0 introduces major features for the RuggedRouter® such as BGP, Synchronous Serial support, Multilink PPP, E3 support on compatible hardware, LLDP, a first phase of IPv6 support, routing of ISO protocol packets, and limited L2TP and LAN bridging. ROX 1.14.0 also includes major fixes to SNMP, Serial DNP, DDS trace functionality, Wanpipe driver, and upgrade procedure.

User Guides

All user guides are available from the RuggedCom Web site at www.RuggedCom.com. Please refer to the ROX 1.14.0 user guide.

Changes in ROX 1.14.0 (1495)

BGP Protocol (NF 1498)

Type: New Feature
Products: RX1000, RX1100
ID: 1495

This new feature adds the Border Gateway Protocol version 4 functionality to the routers.

Routing of packets according to specific types (NF 1497)

Type: New Feature
Products: RX1000, RX1100
ID: 1497

The RuggedRouter now allows the tunneling of layer 2 packets from one RuggedRouter to another based upon a user specified Ethernet type or the predefined ISO protocol.

IPv6 Phase 1 (NF 1501)

Type: New Feature
Products: RX1000, RX1100
ID: 1501

This new feature adds basic IPv6 support to the RuggedRouter. It consists at the moment of the ability to forward IPv6 packets on a LAN.

Synchronous serial (NF 1507)

Type: New Feature
Products: RX1000, RX1100
ID: 1507

This new feature adds synchronous serial support.

Limited LAN Bridging (NF 1509)

Type: New Feature
Products: RX1000, RX1100
ID: 1509

This new feature adds limited LAN bridging. This is useful in small installations where a dedicated switch is not called for. Hence it is possible for instance to bridge 3 RTUs. The bridging feature is intended to be limited as far as it applies only to a limited number of devices, usually low-traffic RTUs.

Link Layer Discovery Protocol (LLDP) (NF 1558)

Type: New Feature
Products: RX1000, RX1100
ID: 1558

This new feature adds LLDP support. It is enabled by default, but can be switched off using the 'Bootup and Shutdown' menu. When SNMP is activated, LLDP information can be queried through SNMP using the standard LLDP MIB.

Telnet access (NF 1625)

Type: New Feature
Products: RX1000, RX1100
ID: 1625

This new feature enables the use of telnet to connect to the router. Please note that telnet is provided by request and is inherently an insecure way of accessing the unit but can be useful in very specific circumstances. Telnet is disabled by default. The starting and stopping of the telnet service can be made via the 'Telnet Server Configuration' menu.

PPP Dial on Demand (NF 1629)

Type: New Feature
Products: RX1000, RX1100
ID: 1629

This new feature adds to the current PPP functionality by providing a 'dial on demand' option.

Multilink PPP (NF 1557)

Type: New Feature
Products: RX1000, RX1100
ID: 1557

Multilink PPP allows the use of multiple ports in order to provide a greater bandwidth. Packets smaller than 128 bytes will not be split and will be sent using a single channel.

En/disabling of sending ICMP redirects (NF 1678)

Type: New Feature
Products: RX1000, RX1100
ID: 1678

This feature is about disabling/enabling the sending of ICMP redirects. This is useful for security reasons

E3 Support (NF 1696)

Type: New Feature
Products: RX1000, RX1100

ID: 1696

On selected hardware (AFT-A301-SH cards featuring an updated CPLD and FW version 11 or above) E3 is now supported. Please note that older T3 cards will have to get their firmware updated as part of the ROX upgrade procedure. See 'IMPORTANT NOTES' at the beginning of this document.

PPP/L2TP (NF 1459)

Type: New Feature
Products: RX1000, RX1100
ID: 1459

This feature adds L2TP support. The L2TP implementation supports most of RFC2661. The only exception being is the PPP proxy AVPs. All other RFC2661 AVPs are supported. Please note that there's a limitation on the transferred data for the L2TP feature of approx. 100 MBytes. After which the connection will be dropped until a new key exchange happens, usually lasting around 40 seconds. Auto-recovery data transfer protocols which are automatically retrying after connection losses will not be affected by this. HTTP and SSH sessions could see pauses of 40-60 seconds before resuming their operations. On the other hand FTP transfers can be terminated.

DHCP relay (NF 1782)

Type: New Feature
Products: RX1000, RX1100
ID: 1782

This new feature adds the capability of relaying DHCP requests.

SNMPv3 access control settings cause snmpd to stop (Ma 1705)

Type: Major
Products: RX1000, RX1100
ID: 1705

This update addresses a problem found during the configuration of the SNMP daemon in which case the daemon would stop.

Unwanted DNP debug notifications caused DNP message losses (Ma 1619)

Type: Major
Products: RX1000, RX1100
Type: 1619

Removed extra debugging messages which introduced delays in processing and caused restarting of the serial server.

Wanpipe driver update (Ma 1646)

Type: Major
Products: RX1000, RX1100
ID: 1646

Updated driver for E3 interface support. Addition of an optional disabling of PPP magic number to deal with hosts not supporting that option.

SNMPD has memory leak and crash sometime (Ma 1452)

Type: Major
Products: RX1000, RX1100
ID: 1452

The SNMP daemon was updated in order to fix a problem regarding CPU consumption and memory leaks.

GRE not working after wanrouter restarted (Ma 1683)

Type: Major
Products: RX1000, RX1100
ID: 1683

GRE tunnel up/down state is now linked with the WAN interface so that the tunnel is automatically re-enabled according to the interface state.

Failure to generate SNMPv3 Traps when link up/down (Ma 1655)

Type: Major
Products: RX1000, RX1100
ID: 1655

ROX SNMPv3 MIB responds to MIB Walks but fails to send SNMPv3 trap. The SNMP daemon was updated to fix that problem.

SerServer stop running when using TCPModbus (Ma 1649)

Type: Major
Products: RX1000, RX1100
ID: 1649

When configuring TCPModbus for several serial ports, the serial server process would not restart once configured in the 'Bootup and Shutdown' menu. An adjustment in the serial server now handles this situation.

CDMA Cellular Modem Support (E 1118)

Type: Enhancement
Products: RX1000, RX1100
ID: 1118

CDMA cellular modem support is added to ROX, bringing the speed of 3G cellular communications to the RuggedRouter.

2-stage upgrade procedure (E 1693)

Type: Enhancement

Products: RX1000, RX1100
ID: 1693

Please refer to the 'Important Notes' at the beginning of this document. This allows the injection of new code in field installations in order to perform any required setup prior to the upgrade proper.

SNMP traps: textual interface name in ifName OID (E 1861)

Type: Enhancement
Products: RX1000, RX1100
ID: 1861

SNMP link up/down traps now include the ifName OID field, which includes the interface name in a character string. Please note that since the process of restarting WAN interfaces takes a few seconds to complete, the interface names might not be available during the early stages of the process. At these times, traps are nevertheless sent to reflect the changing nature of the interfaces even though no interface name can be conveyed. These traps contain only interface status and index information by way of interface identification. At all other times, the name of the interface will be transmitted with link up/down traps in the ifName field.

System logs: Added support for custom src IP (E 1865)

Type: Enhancement
Products: RX1000, RX1100
ID: 1865

The system logging facility now offers the possibility of assigning a specific source IP when logging to a remote server.

Radius enhancement - source IP customization (E 1866)

Type: Enhancement
Products: RX1000, RX1100
ID: 1866

The Radius functionality is now enhanced with the possibility of assigning a specific IP to bind to as source IP.

VRRP monitoring of physical interfaces (E 1867)

Type: Enhancement
Products: RX1000, RX1100
ID: 1867

The VRRP functionality has now the capability of monitoring physical interfaces instead of logical connections.

Improve GOOSE tunnels performance (E 1771)

Type: Enhancement
Products: RX1000, RX1100
ID: 1771

This enhancement improves performance of the GOOSE tunneling by approx. 10 times.

GMT/UTC time options (E 1607)

Type: Enhancement
Products: RX1000, RX1100
ID: 1607

This is an enhancement to the current Webmin System Time page to provide GMT and DST settings. This is useful for customers who like to maintain a constant time base, not subject to daylight savings time (DST) in a distributed network.

IPSec extra configuration options (E 1508)

Type: Enhancement
Products: RX1000, RX1100
ID: 1508

This enhancement adds to IPsec the following options: ike and keylife.

GRE IP address / multicast configuration (E 1677)

Type: Enhancement
Products: RX1000, RX1100
ID: 1677

Optional assignation of IP address to GRE tunnel interface (default: 127.127.0.1) and enabling multicast on GRE tunnels.

Trace function for DDS in Frame Relay mode broken (Mi 1638)

Type: Minor
Products: RX1000, RX1100
ID: 1638

When doing a trace using DDS 56K interface cards the following was shown: 'Unknown Configured Wanpipe Protocol 0x88' instead of the trace data. The WAN monitor component was updated.

Webmin and time zone changes (Mi 1574)

Type: Minor
Products: RX1000, RX1100
ID: 1574

Previously, Webmin did not react to time zone changes.

Frame Relay configuration accept invalid DLCI number (Mi 1762)

Type: Minor
Products: RX1000, RX1100
ID: 1762

This concerns a problem in filtering out invalid user entry for the DLCI values.

MTU default values not restored by Webmin (Mi 1706)

Type: Minor
Products: RX1000, RX1100
ID: 1706

This update concerns the displaying of MTU values in Webmin which were not properly reset.

Snort local logging to different log files (Mi 1484)

Type: Minor
Products: RX1000, RX1100
ID: 1484

Snort can be configured to log onto /var/log/auth.log or /var/log/syslog although the Webmin Snort option did not work. Now it is possible to specify either log files.

Online help: Some graphic formats are not handled (Mi 1609)

Type: Minor
Products: RX1000, RX1100
ID: 1609

ROX 1.14.0 now benefits from a new generation documenting system that enables better use and maintenance of both the user guide and the online help access.

Unable to clear the Frame Relay interface statistics (Mi 1623)

Type: Minor
Products: RX1000, RX1100
ID: 1623

Frame Relay interface statistics could not be cleared.

Webmin accept illegal character (Mi 1621)

Type: Minor
Products: RX1000, RX1100
ID: 1621

Minor improvement concerning the Webmin data entry field for IPsec configuration.

Invalid DNS server makes Webmin slow to serve pages (Mi 1511)

Type: Minor
Products: RX1000, RX1100
ID: 1511

A miniserv configuration option adjustment made Webmin keep the same response time in any cases.

Radius Server Adjustments (Mi 1700)

Type: Minor
Products: RX1000, RX1100
ID: 1700

In some occasions a Radius server would expect additional fields to be communicated such as the Vendor-Specific field. This adjustment enables better compatibility with differently-configured Radius servers. Another adjustment consisted of testing a somewhat slower response and suggesting a timeout of 10 seconds in those circumstances.

Traffic Control rules on the modem PPP link is broken (Mi 1682)

Type: Minor
Products: RX1000, RX1100
ID: 1682

TC rules configured under the Shorewall do not take place when the PPP0 interface is down and brought back up later. However, the rules are working fine if the Firewall Configuration is reapplied after the PPP0 interface is brought back up. Resolving this problem consisted of synchronizing Shorewall with the PPP interface.

Webmin allows the taken 24th time slot to be configured (Mi 1681)

Type: Minor
Products: RX1000, RX1100
ID: 1681

The 24th time slot had been taken by the 2nd channel of the T1-1 port, but 1st channel still can use this taken slot. The Webmin configuration was changed to prevent this.

Quagga doesn't restart after NTP server restarted (Mi 1680)

Type: Minor
Products: RX1000, RX1100
ID: 1680

An update of the script used to start/restart Quagga fixed the use of the ntp_corr variable.

Non-default Snort rules were restored to default values (Mi 1675)

Type: Minor
Products: RX1000, RX1100
ID: 1675

During upgrades of older configuration, as in the case when upgrading a ROX 1.10.1 configuration, the non-default Snort rules were restored to default values.. An adjustment of the pre and post install scripts when doing upgrades fixed this minor bug.

RIP version control on T1/E1 fails (Mi 1685)

Type: Minor
Products: RX1000, RX1100
ID: 1685

When using RIP routing on a T1/E1 link, RIP sends both v1 and v2 updates although it is configured to send and only v1. The solution to this problem consisted of adding a Send version parameter to RIP global parameter page to control RIP Send Version to neighbor.

Dummy interface is accepting invalid IP address (Mi 1742)

Type: Minor
Products: RX1000, RX1100
ID: 1742

Webmin was updated in order to better validate user input for the dummy interface.

Automatic Upgrade Feature Removal (Mi 1823)

Type: Minor
Products: RX1000, RX1100
ID: 1823

The Automatic Upgrade feature is removed from ROX 1.14.0. This will allow greater flexibility in doing adapted scheduled upgrades, as well as status tracking from a centralized location.

Security Updates

Remote Vulnerability with Openswan (CVE-2009-0790)

Component: Openswan

Overview: The pluto IKE daemon in Openswan and Strongswan IPsec 2.6 before 2.6.21 and 2.4 before 2.4.14, and Strongswan 4.2 before 4.2.14 and 2.8 before 2.8.9, allows remote attackers to cause a denial of service (daemon crash and restart) via a crafted (1) R_U_THERE or (2) R_U_THERE_ACK Dead Peer Detection (DPD) IPsec IKE Notification message that triggers a NULL pointer dereference related to inconsistent ISAKMP state and the lack of a phase2 state association in DPD.

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0790>

SNMPv3 Authentication Bypass Vulnerability (CVE-2008-0960)

Component: net-snmp

Overview: A vulnerability in the way implementations of SNMPv3 handle specially crafted packets may allow authentication bypass.

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0960>

Integer overflow in net-snmp (CVE-2008-4309)

Component: net-snmp

Overview: Integer overflow in the netsnmp_create_subtree_cache function in agent/snmp_agent.c in net-snmp 5.4 before 5.4.2.1, 5.3 before 5.3.2.3, and 5.2 before 5.2.5.1 allows remote attackers to cause a denial of service (crash) via a crafted SNMP GETBULK request, which triggers a heap-based buffer overflow, related to the number of responses or repeats.

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4309>

Buffer overflow in the __snprint_value function (CVE-2008-2292)

Component: net-snmp

Overview: Buffer overflow in the __snprint_value function in snmp_get in Net-SNMP 5.1.4, 5.2.4, and 5.4.1, as used in SNMP.xs for Perl, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large OCTETSTRING in an attribute value pair (AVP).

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2292>

SNMPv3 HMAC verification vulnerability (CVE-2008-0960)

Component: net-snmp

Overview: SNMPv3 HMAC verification in (1) Net-SNMP 5.2.x before 5.2.4.1, 5.3.x before 5.3.2.1, and 5.4.x before 5.4.1.1; (2) UCD-SNMP; (3) eCos; (4) Juniper Session and Resource Control (SRC) C-series 1.0.0 through 2.0.0; (5) NetApp (aka Network Appliance) Data ONTAP 7.3RC1 and 7.3RC2; (6) SNMP Research before 16.2; (7) multiple Cisco IOS, CatOS, ACE, and Nexus products; and (8) Ingate Firewall 3.1.0 and later and SIParator 3.1.0 and later relies on the client to specify the HMAC length, which makes it easier for remote attackers to bypass SNMP authentication via a length value of 1, which only checks the first byte.

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0960>

Signal handler race condition (CVE-2006-5051)

Component: OpenSSH

Overview: Signal handler race condition in OpenSSH before 4.4 allows remote attackers to cause a denial of service (crash), and possibly execute arbitrary code if GSSAPI authentication is enabled, via unspecified vectors that lead to a double-free.

Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5051>

Upgrade Instructions

Before upgrading we recommend:

- Reviewing all the changes to ensure an upgrade is merited.
- Upgrading a test unit to ensure you understand the upgrade process.
- Planning for a temporary network outage.

The upgrade procedure works by using a set of upgrade files accessible from a web server. These files are distributed in the form of a .zip archive and should be unpacked in a location on a web server that's accessible from the router. Using Webmin Upgrade -> System on a router, the configuration is made using 'Change Repository Server' to point to that location on the web server. Once done, a test run of the upgrade can be made by setting the 'Only show which packages would be upgraded' option to Yes (default setting) and doing an 'Upgrade Now'. When everything is found satisfactory, setting the same option to No and doing an 'Upgrade Now' will actually launch the upgrade process.

Depending on the nature of the upgrade, you might be asked to confirm if a reboot of the unit is deemed necessary with the following message: "It has been detected that your router must be rebooted after the upgrade. Do you want to continue at this time?"

If you are not prepared to have the router go through a reboot phase, then you can decline the upgrade simply by clicking on any other Webmin menu option and then perform the upgrade at a more convenient time.

As mentioned in the notes at the beginning of this document, when upgrading from a ROX version that is older than 1.14.0, a first step upgrade of Webmin will be performed after which the upgrade procedure must be launched again to perform the rest of the upgrade. This allows for performing a straight path upgrade from older ROX versions as well as identifying and coping with new upgrade needs using existing ROX installations in the field.

If you choose not to do the full upgrade right now and only have Webmin upgraded, it is then strongly recommended that you do not use Webmin and immediately schedule a time to perform the rest of the upgrade as soon as possible.

If the unit is equipped with any T3/E3 interface that has a firmware version older than V11, the firmware will be upgraded as part of the main upgrade. An information screen will be displayed before the upgrade starts that includes the approx. time required to do (on older, slower units, close to 20 minutes - and on newer units, 3 to 4 minutes). The user can choose whether or not to perform the whole upgrade at that moment.

It is important that there are no power supply interruption during the time it takes for an upgrade to complete. The following illustrations highlights the various options used in the process of

upgrading a RuggedRouter.

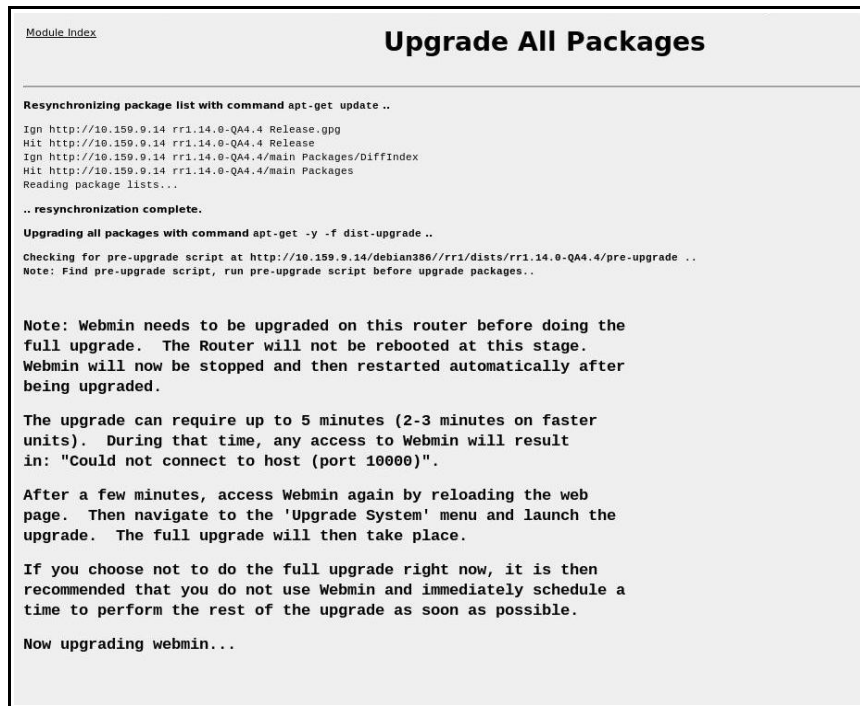
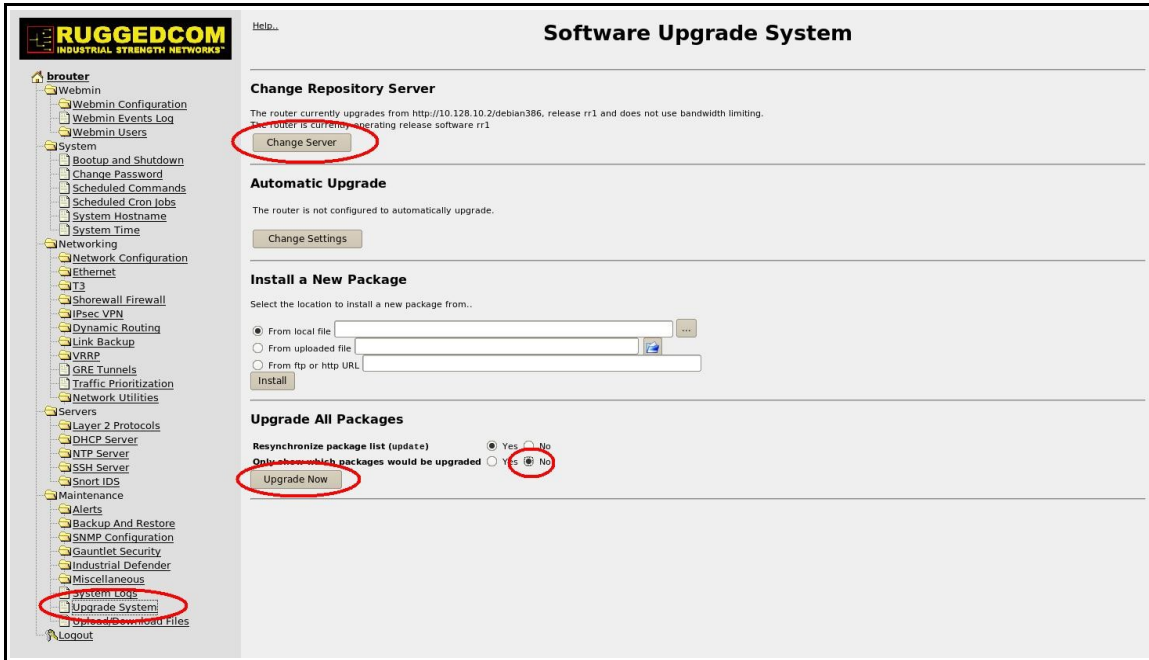


Illustration 2: Webmin Upgrade Information Page

```
Module Index
```

Upgrade All Packages

```
Resynchronizing package list with command apt-get update ..
Hit http://10.159.9.14 rr1.14.0-QA4.13/main Packages
Ign http://10.159.9.14 rr1.14.0-QA4.13/main Release
Reading Package Lists...
.. resynchronization complete.
Upgrading all packages with command apt-get -y -f dist-upgrade ..
Checking for pre-upgrade script at http://10.159.9.14/debian386/rr1/dists/rr1.14.0-QA4.13/pre-upgrade ..
Note: Find pre-upgrade script, run pre-upgrade script before upgrade packages..

Warning: The System cannot be upgraded at this moment.

It is found that your system currently running ipsec in
KLIPS mode. ROX releases now only support Netkey mode for
ipsec. You must change your configuration in the following way:

1) ipsec configuration using Netkey mode
using Networking -> IPsec VPN -> Server Configuration. In this
menu, select '[Switch to netkey (Policy Based IPSec)]'.

2) Update the firewall rules using the Shorewall Firewall menu option

You must perform this configuration change before an upgrade can be made.
Once this configuration change is made, please run the upgrade again.
```

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 (C)	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 (Ma)	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 (NF)	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 (E)	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 (Mi)	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 (Co)	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

Corporate Headquarters

RuggedCom Inc.
300 Applewood Cres. Unit 1
Concord, Ontario,
Canada, L4K 5C7

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

US Corporate Headquarters

RuggedCom
1930 Harrison St. Suite 307
Hollywood, Florida
USA 33020
Tel.: (954) 922-7975

Technical Action Center (Technical Support)

Toll Free: 1 866 922-7975

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

Release Notes

Prepared by Alain Lachapelle, Project Lead – ROX
(C) 2010 RuggedCom