SIEMENS

RUGGEDCOM ROS v3.11.7

User Guide

For RS950G

04/2016
RC1263-EN-01

Disclaimer Of Liability

Siemens has verified the contents of this document against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

RUGGEDCOM™ and ROS™ are trademarks of Siemens Canada Ltd.

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Third Party Copyrights

Siemens recognizes the following third party copyrights:

- Copyright © 2004 GoAhead Software, Inc. All Rights Reserved.

Open Source

RUGGEDCOM ROS contains Open Source Software. For license conditions, refer to the associated *License Conditions* document.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Warranty

Refer to the License Agreement for the applicable warranty terms and conditions, if any.

For warranty details, visit www.siemens.com/ruggedcom or contact a Siemens customer service representative.

Contacting Siemens

Address
Siemens Canada Ltd.
Industry Sector
300 Applewood Crescent
Concord, Ontario
Canada, L4K 5C7

Telephone
Toll-free: 1 888 264 0006
Tel: +1 905 856 5288
Fax: +1 905 856 1995

E-mail
ruggedcom.info.i-ia@siemens.com

Web
www.siemens.com/ruggedcom

Table of Contents

Preface

This guide describes the RUGGEDCOM ROS v3.11.7 running on the RUGGEDCOM RS950G family of products. It contains instructions and guidelines on how to use the software, as well as some general theory.

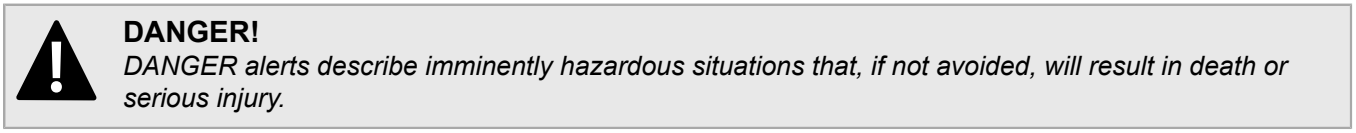
It is intended for use by network technical support personnel who are familiar with the operation of networks. It is also recommended for us by network and system planners, system programmers, and line technicians.

Conventions

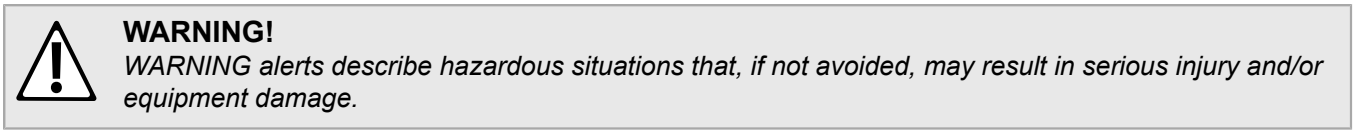
This User Guide uses the following conventions to present information clearly and effectively.

Alerts

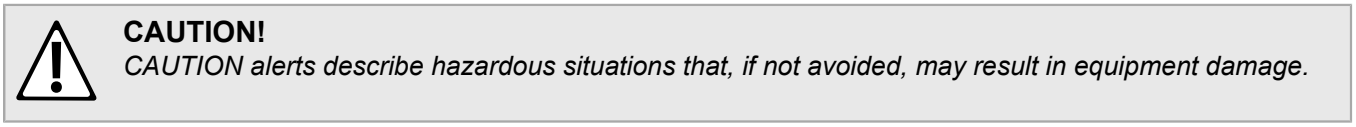
The following types of alerts are used when necessary to highlight important information.



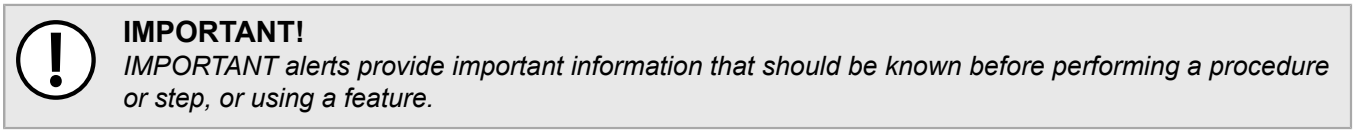
DANGER!
DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.



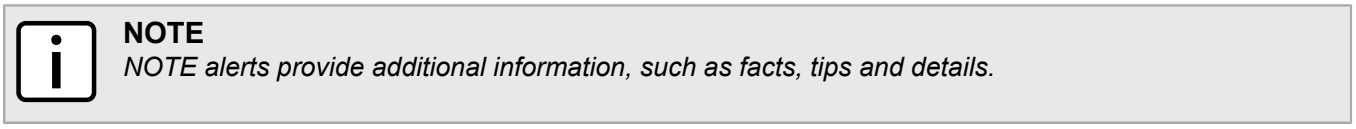
WARNING!
WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.



CAUTION!
CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.



IMPORTANT!
IMPORTANT alerts provide important information that should be known before performing a procedure or step, or using a feature.



NOTE
NOTE alerts provide additional information, such as facts, tips and details.

CLI Command Syntax

The syntax of commands used in a Command Line Interface (CLI) is described according to the following conventions:

Example	Description
command	Commands are in bold.

Example	Description
command parameter	Parameters are in plain text.
command parameter1 parameter2	Parameters are listed in the order they must be entered.
command parameter1 *parameter2*	Parameters in italics must be replaced with a user-defined value.
command [parameter1 | parameter2]	Alternative parameters are separated by a vertical bar (|). Square brackets indicate a required choice between two or more parameters.
command { parameter3 | parameter4 }	Curly brackets indicate an optional parameter(s).
command parameter1 parameter2 { parameter3 | parameter4 }	All commands and parameters are presented in the order they must be entered.

Related Documents

Other documents that may be of interest include:

- *ROS Installation Guide for RUGGEDCOM RS950G*
- *RUGGEDCOM Fiber Guide*
- *RUGGEDCOM Wireless Guide*
- *White Paper: Rapid Spanning Tree in Industrial Networks*

System Requirements

Each workstation used to connect to the RUGGEDCOM ROS interface must meet the following system requirements:

- Must have one of the following Web browsers installed:
  - Microsoft Internet Explorer 8.0 or higher
  - Mozilla Firefox
  - Google Chrome
  - Iceweasel/IceCat (Linux Only)
- Must have a working Ethernet interface compatible with at least one of the port types on the RUGGEDCOM device
- The ability to configure an IP address and netmask on the computer's Ethernet interface

Accessing Documentation

The latest user documentation for RUGGEDCOM ROS v3.11.7 is available online at www.siemens.com/ruggedcom. To request or inquire about a user document, contact Siemens Customer Support.

Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

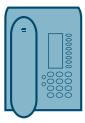
Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens Sales representative.

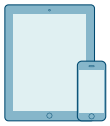
Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:

Online
Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.



Telephone
Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.



Mobile App
Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

- Access Siemens' extensive library of support documentation, including FAQs and manuals
- Submit SRs or check on the status of an existing SR
- Contact a local Siemens representative from Sales, Technical Support, Training, etc.
- Ask questions or share knowledge with fellow Siemens customers and the support community

1 Introduction

This chapter provides a basic overview of the RUGGEDCOM ROS software. It describes the following topics:

Section 1.1

Overview

Welcome to the RUGGEDCOM ROS Software User Guide for the RS950G. This Guide describes the wide array of carrier grade features made available by ROS (Rugged Operating System). These features include:

Network Resilience

- IEC 62439-3 PRP
- IEC 62439-3 HSR

Industrial Design

- Panel or DIN mounting
- Dual DC inputs:
  - Order code 24: 10 to 36 VDC
  - Order code 48: 37 to 72 VDC
- Universal AC input:
  - Order code HI: 85-264 VAC or 88-300 VDC
- 20 AWG steel enclosure

Substation Rated

- IEC 61850-3
- IEEE 1613 Class 2
- -40 to 85 °C (-40 to 185 °F) operating (no fans)
- Zero-Packet-Loss™

Management

- SSH/SSL encryption
- Web-based, Telnet
- Alarms, Critical Relay

Section 1.2

Security Recommendations and Considerations

The following describes important security-related recommendations and suggestions that should be considered before implementing the RUGGEDCOM ROS on any network:

Section 1.2.1

Security Recommendations

To prevent unauthorized access to the device, note the following security recommendations:

- Do not connect the device directly to the Internet. Deploy the device only within a secure network perimeter.
- Replace the default passwords for all user accounts and processes (where applicable) before the device is deployed.
- Use strong passwords. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, etc. For more information about creating strong passwords, refer to the password requirements in Section 3.6, “Passwords”.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Passwords should not be re-used across different usernames and systems, or after they expire.
- When RADIUS authentication is done remotely, make sure all communications are within the security perimeter or on a secure channel.
- Create and provision custom SSL certificates and SSH keys in order to establish a chain of trust that you yourself can verify.
- SSL and SSH private keys are accessible to users who connect to the device via the serial console. Make sure to take appropriate precautions when shipping the device beyond the boundaries of the trusted environment:
  - Replace the SSH and SSL keys with *throwaway* keys prior to shipping.
  - Take the existing SSH and SSL keys out of service. When the device returns, create and program new keys for the device.
- Restrict physical access to the device to only trusted personnel. A person with malicious intent in possession of the flash card could extract critical information, such as certificates, keys, etc. (user passwords are protected by hash codes), or reprogram the card.
- Control access to the serial console to the same degree as any physical access to the device. Access to the serial console allows for potential access to the RUGGEDCOM ROS boot loader, which includes tools that may be used to gain complete access to the device.
- Only enable the services that will be used on the device.
- If SNMP is enabled, limit the number of IP addresses that can connect to the device and change the community names. Also configure SNMP to raise a trap upon authentication failures.
- Avoid using insecure services such as Telnet and TFTP, or disable them completely if possible. These services are available for historical reasons and are disabled by default.
- Limit the number of simultaneous Web Server, Telnet and SSH sessions allowed.
- Configure remote system logging to forward all logs to a central location.
- Periodically audit the device to make sure it complies with these recommendations and/or any internal security policies.
- Configuration files are provided in the CSV (comma separated values) format for ease of use. Make sure that configuration files are properly protected.
- Management of the configuration file, certificates and keys is the responsibility of the device owner. Before returning the device to Siemens' for repair, make sure encryption is disabled (to create a cleartext version of the configuration file) and replace the current certificates and keys with temporary certificates and keys that can be destroyed upon the device's return.

Section 1.2.2
Key Files

This section describes in detail the security keys used by RUGGEDCOM ROS for the establishment of secure remote login (SSH) and web access (SSL).

It is strongly recommended to create and provision your own SSL certificates and SSH keys. The default certificate and keys are only ever used when upgrading to RUGGEDCOM ROS 3.11.7 or later. New RUGGEDCOM ROS-based units from Siemens' will already have unique certificate and keys pre-configured in `ssl.crt` and `ssh.keys` flash files.

The default SSL certificate are self-signed. It is recommended to use SSL certificates that are either signed by a trusted third party Certificate Authority (CA) or by an organization's own CA. This technique is described in the Siemens' application note: *Creating/Uploading SSH Keys and SSL Certificates to ROS Using Windows*, available from www.siemens.com/ruggedcom.

The sequence of events related to Key Management during an upgrade to RUGGEDCOM ROS 3.11.7 or later is as follows:

- On first boot, RUGGEDCOM ROS 3.11.7 will start the SSH and SSL (secure web) services using the *default keys*.
- At any time, one may upload custom keys, which will take precedence over the default keys and will take effect immediately.
- On subsequent boot, if there is a valid `ssl.crt` file, the default certificate will not be used for SSL. If there is a valid `ssh.keys` file, the default SSH key will not be used.
- At any time, new keys may be uploaded.

The following sections describe SSL certificates and SSH key pairs in more details:

- Section 1.2.2.1, “SSL Certificates”
- Section 1.2.2.2, “SSH Key Pairs”

Section 1.2.2.1
SSL Certificates

RUGGEDCOM ROS supports SSL certificates that conform to the following specifications:

- X.509 v3 digital certificate format
- PEM format
- RSA key pair, 512 to 2048 bits in length

The RSA key pair used in the default certificate uses a public key of 1024 bits in length.

NOTE
RSA keys smaller than 2048 bits in length are not recommended. Support is only included here for compatibility with legacy equipment.

NOTE
The default certificate and keys are common to every instance of a given RUGGEDCOM ROS firmware version. That is why it is important to provide custom keys. In this way, one has at least unique, and at best, traceable and verifiable keys installed when establishing secure communication with the unit.

The following (bash) shell script fragment uses the `openssl` command line utility to generate a self-signed X.509 v3 SSL certificate with a 1024-bit RSA key suitable for use in RUGGEDCOM ROS. Note that two standard PEM files are required: the SSL certificate and the RSA private key file. These are concatenated into the resulting `ssl.crt` file, which may then be uploaded to RUGGEDCOM ROS:

```
# RSA key size:
BITS=1024
# 20 years validity:
DAYS=7305

# Values that will be stored in the Distinguished Name fields:

COUNTRY_NAME=CA                    # Two-letter country code
STATE_OR_PROVINCE_NAME=Ontario     # State or Province
LOCALITY_NAME=Concord              # City
ORGANIZATION=Ruggedcom.com         # Your organization's name
ORGANIZATION_CA=${ORGANIZATION}_CA # Your Certificate Authority
COMMON_NAME=RC                     # The DNS or IP address of the ROS unit
ORGANIZATIONAL_UNIT=ROS            # Organizational unit name

# Variables used in the construction of the certificate
REQ_SUBJ="/C=${COUNTRY_NAME}/ST=${STATE_OR_PROVINCE_NAME}/L=${LOCALITY_NAME}/O=${ORGANIZATION}/OU=
${ORGANIZATIONAL_UNIT}/CN=${COMMON_NAME}/"
REQ_SUBJ_CA="/C=${COUNTRY_NAME}/ST=${STATE_OR_PROVINCE_NAME}/L=${LOCALITY_NAME}/O=${ORGANIZATION_CA}/
OU=${ORGANIZATIONAL_UNIT}/"

#########################################################################
# Make the self-signed SSL certificate and RSA key pair:

openssl req -x509 -newkey rsa:${BITS} -nodes \
 -days ${DAYS} -subj ${REQ_SUBJ} \
 -keyout ros_ssl.key  \
 -out    ros_ssl.crt

# Concatenate Cert and Key into a single file suitable for upload to ROS:
# Note that cert must precede the RSA key:
cat  ros_ssl.crt  ros_ssl.key > ssl.crt
```

For information on creating SSL certificates for use with RUGGEDCOM ROS in a Microsoft Windows environment, refer to the following Siemens' application note: *Creating/Uploading SSH Keys and SSL Certificates to ROS Using Windows*.

The following listing is the disassembly of a self-signed SSL certificate generated by RUGGEDCOM ROS:

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
 ca:01:2d:c0:bf:f9:fd:f2
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=CA, ST=Ontario, L=Concord, O=RuggedCom.com, OU=RC, CN=ROS
  Validity
 Not Before: Dec  6 00:00:00 2012 GMT
 Not After : Dec  7 00:00:00 2037 GMT
  Subject: C=CA, ST=Ontario, L=Concord, O=RuggedCom.com, OU=RC, CN=ROS
  Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public Key: (1024 bit)
  Modulus (1024 bit):
    00:83:e8:1f:02:6b:cd:34:1f:01:6d:3e:b6:d3:45:
    b0:18:0a:17:ae:3d:b0:e9:c6:f2:0c:af:b1:3e:e7:
    fd:f2:0e:75:8d:6a:49:ce:47:1d:70:e1:6b:1b:e2:
    fa:5a:1b:10:ea:cc:51:41:aa:4e:85:7c:01:ea:c3:
    1e:9e:98:2a:a9:62:48:d5:27:1e:d3:18:cc:27:7e:
    a0:94:29:db:02:5a:e4:03:51:16:03:3a:be:57:7d:
    3b:d1:75:47:84:af:b9:81:43:ab:90:fd:6d:08:d3:
```

```
    e8:5b:80:c5:ca:29:d8:45:58:5f:e4:a3:ed:9f:67:
    44:0f:1a:41:c9:d7:62:7f:3f
  Exponent: 65537 (0x10001)
  X509v3 extensions:
 X509v3 Subject Key Identifier:
  EC:F3:09:E8:78:92:D6:41:5F:79:4D:4B:7A:73:AD:FD:8D:12:77:88
 X509v3 Authority Key Identifier:
  keyid:EC:F3:09:E8:78:92:D6:41:5F:79:4D:4B:7A:73:AD:FD:8D:12:77:88
  DirName:/C=CA/ST=Ontario/L=Concord/O=RuggedCom.com/OU=RC/CN=ROS
  serial:CA:01:2D:C0:BF:F9:FD:F2
 X509v3 Basic Constraints:
  CA:TRUE
Signature Algorithm: sha1WithRSAEncryption
  64:cf:68:6e:9f:19:63:0e:70:49:a6:b2:fd:09:15:6f:96:1d:
  4a:7a:52:c3:46:51:06:83:7f:02:8e:42:b2:dd:21:d2:e9:07:
  5c:c4:4c:ca:c5:a9:10:49:ba:d4:28:fd:fc:9d:a9:0b:3f:a7:
  84:81:37:ca:57:aa:0c:18:3f:c1:b2:45:2a:ed:ad:dd:7f:ad:
  00:04:76:1c:f8:d9:c9:5c:67:9e:dd:0e:4f:e5:e3:21:8b:0b:
  37:39:8b:01:aa:ca:30:0c:f1:1e:55:7c:9c:1b:43:ae:4f:cd:
  e4:69:78:25:5a:a5:f8:98:49:33:39:e3:15:79:44:37:52:da:
  28:dd
```

Section 1.2.2.2
SSH Key Pairs

Controlled versions of RUGGEDCOM ROS support SSH public/private key pairs that conform to the following specifications:

- PEM format
- DSA key pair, 512 to 2048 bits in length

The DSA key pair used in the default key pair uses a public key of 1024 bits in length.

NOTE
DSA keys smaller than 2048 bits in length are not recommended, and support is only included here for compatibility with legacy equipment.

The following is an example of an SSH key generated by RUGGEDCOM ROS:

```
Private-Key: (1024 bit)
priv:
 00:b2:d3:9d:fa:56:99:a5:7a:ba:1e:91:c5:e1:35:
 77:85:e8:c5:28:36
pub:
 6f:f3:9e:af:e6:d6:fd:51:51:b9:fa:d5:f9:0a:b7:
 ef:fc:d7:7c:14:59:52:48:52:a6:55:65:b7:cb:38:
 2e:84:76:a3:83:62:d0:83:c5:14:b2:6d:7f:cc:f4:
 b0:61:0d:12:6d:0f:5a:38:02:67:a4:b7:36:1d:49:
 0a:d2:58:e2:ff:4a:0a:54:8e:f2:f4:c3:1c:e0:1f:
 9b:1a:ee:16:e0:e9:eb:c8:fe:e8:16:99:e9:61:81:
 ed:e4:f2:58:fb:3b:cb:c3:f5:9a:fa:ed:cd:39:51:
 47:90:5d:6d:1b:27:d5:04:c5:de:57:7e:a7:a3:03:
 e8:fb:0a:d5:32:89:40:12
P:
 00:f4:81:c1:9b:5f:1f:eb:ac:43:2e:db:dd:77:51:
 6e:1c:62:8d:4e:95:c6:e7:b9:4c:fb:39:9c:9d:da:
 60:4b:0f:1f:c6:61:b0:fc:5f:94:e7:45:c3:2b:68:
 9d:11:ba:e1:8a:f9:c8:6a:40:95:b9:93:7c:d0:99:
 96:bf:05:2e:aa:f5:4e:f0:63:02:00:c7:c2:52:c7:
 1a:70:7c:f7:e5:fe:dd:3d:57:02:86:ae:d4:89:20:
 ca:4b:46:80:ea:de:a1:30:11:5c:91:e2:40:d4:a3:
 82:c5:40:3b:25:8e:d8:b2:85:cc:f5:9f:a9:1d:ea:
```

```
 0a:ac:77:95:ee:d6:f7:61:e3
Q:
 00:d5:db:48:18:bd:ec:69:99:eb:ff:5f:e1:40:af:
 20:80:6d:5c:b1:23
G:
 01:f9:a1:91:c0:82:12:74:49:8a:d5:13:88:21:3e:
 32:ea:f1:74:55:2b:de:61:6c:fd:dd:f5:e1:c5:03:
 68:b4:ad:40:48:58:62:6c:79:75:b1:5d:42:e6:a9:
 97:86:37:d8:1e:e5:65:09:28:86:2e:6a:d5:3d:62:
 50:06:b8:d3:f9:d4:9c:9c:75:84:5b:db:96:46:13:
 f0:32:f0:c5:cb:83:01:a8:ae:d1:5a:ac:68:fb:49:
 f9:b6:8b:d9:d6:0d:a7:de:ad:16:2b:23:ff:8e:f9:
 3c:41:16:04:66:cf:e8:64:9e:e6:42:9a:d5:97:60:
 c2:e8:9e:f4:bc:8f:6f:e0
```

Section 1.3

Available Services by Port

The following table lists the services available under RUGGEDCOM ROS. This table includes the following information:

- **Services**
  The service supported by the device.
- **Port Number**
  The port number associated with the service.
- **Port Open**
  The port state, whether it is always open and cannot be closed, or open only, but can be configured.

  NOTE
  In certain cases, the service might be disabled, but the port can still be open (e.g. TFTP).
- **Port Default**
  The default state of the port (i.e. open or closed).
- **Access Authorized**
  Denotes whether the ports/services are authenticated during access.

Services	Port Number	Port Open	Port Default	Access Authorized	Note
Telnet	TCP/23	Open (configurable)	Closed	Yes	Only available through two management interfaces.
HTTP	TCP/80	Open, redirects to 443	Open	—	
TFTP	UDP/69	Open (configurable)	Closed	No	Only available through two management interfaces.
SFTP	TCP/22	Open	Open	Yes	Only available through two management interfaces.

Services	Port Number	Port Open	Port Default	Access Authorized	Note
SNMP	UDP/161	Open (configurable)	Closed	Yes	Only available through two management interfaces.
SNTP	UDP/123	Open - Always might acts as server	Open	No	Only available through two management interfaces.
SSH	TCP/22	Open	Open	Yes	Only available through two management interfaces.
ICMP	—	Open	Open	No	
TACACS+	TCP/49 (configurable)	Open (configurable)	Closed	Yes	
RADIUS	UDP/1812 to send (configurable), opens random port to listen to	Open (configurable)	Closed	Yes	Only available through two management interfaces.
Remote Syslog	UDP/514 (configurable)	Open (configurable)	Closed	No	Only available through two management interfaces.

Section 1.4
Certificate and Key Requirements

Users are able to load custom and unique SSL certificates and SSL/SSH keys in RUGGEDCOM ROS.

There are two types of certificates and keys:

NOTE
Default SSH keys are not available for Non-Controlled (NC) versions of RUGGEDCOM ROS.

- **Default**
  Each RUGGEDCOM ROS device is shipped with an SSL certificate and RSA key pair, and a DSA key pair for SSH that are unique to software version. If a valid SSL certificate or SSL/SSH keys are not available on the device, the default certificate and keys are used immediately so that SSH and SSL (https) sessions can be served.
- **User-Generated (Recommended)**
  Custom certificates and keys are the most secure option. They give the user complete control over certificate and key management, allow for certificates signed by a public or local certificate authority, controlled distribution of public SSH keys to network hosts that need them, and more.

NOTE
The RSA key pair must be added to the `ssl.crt` *file after the SSL certificate.*

For SSL, RUGGEDCOM ROS requires an X.509 certificate in standard PEM format and an RSA key pair. The certificate may be self-signed or signed by a separate authoriy. The RSA key must be between 512 and 1048 bits in length. The certificate and keys must be combined in a single `ssl.crt` file and uploaded to the device.

The following is an example of a combined SSL certificate and key:

```
-----BEGIN CERTIFICATE-----
MIIC9jCCAl+gAwIBAgIJAJh6rrehMt3iMA0GCSqGSIb3DQEBBQUAMIGuMQswCQYD
VQQGEwJDQTEQMA4GA1UECBMHT250YXJpbzEQMA4GA1UEBxMHQ29uY29yZDESMBAG
A1UEChMJUnVnZ2VkY29tMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MSYwJAYD
VQQDEx1XUy1NSUxBTkdPVkFOLlJVR0dFRENPTS5MT0NBTDEkMCIGCSqGSIb3DQEJ
ARYVc3VwcG9ydEBydWdnZWRjb20uY29tMB4XDTEyMTAyMzIxMTA1M1oXDTE3MTAy
MjIxMTA1M1owgZwxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdPbnRhcmlvMRAwDgYD
VQQHEwdDb25jb3JkMRIwEAYDVQQKEwlSdWdnZWRDb20xGTAXBgNVBAsTEEN1c3Rv
bWVyIFN1cHBvcnQxFDASBgNVBAMTCzE5Mi4xNjguMS4yMSQwIgYJKoZIhvcNAQkB
FhVTdXBwb3J0QHJ1Z2dlZGNvbS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALfE4eh2aY+CE3W5a4Wz1Z1RGRP02COHt153wFFrU8/fFQXNhKlQirlAHbNT
RSwcTR8ZFapivwYDivn0ogOGFXknYP90gv2oIaSVY08FqZkJW77g3kzkv/8Zrw3m
W/cBsZJ8SyKLIDfy401HkHpDOle5NsQFSrziGUPjAOIvvx4rAgMBAAGjLDAqMAkG
A1UdEwQCMAAwHQYDVR0OBBYEFER0utgQOifnrflnDtsqNcnvRB0XMA0GCSqGSIb3
DQEBBQUAA4GBAHtBsNZuh8tB3kdqR7Pn+XidCsD70YnI7w0tiy9yiRRhARmVXH8h
5Q1rOeHceri3JFFIOxIxQt4KgCUYJLu+c9Esk/nXQQar3zR7IQCt0qOABPkviiY8
c3ibVbhJjLpR2vNW4xRAJ+HkNNtBOg1xUlp4vOmJ2syYZR+7XAy/OP/S
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC3xOHodmmPghN1uWuFs9WdURkT9Ngjh7ded8BRa1PP3xUFzYSp
UIq5QB2zU0UsHE0fGRWqYr8GA4r59KIDhhV5J2D/dIL9qCGklWNPBamZCVu+4N5M
5L//Ga8N5lv3AbGSfEsiiyA38uNNR5B6QzpXuTbEBUq84hlD4wDiL78eKwIDAQAB
AoGBAI2CXHuHg23wuk9zAusoOhw0MN1/M1jYz0k9aajIvvdZT3Tyd29yCADy8GwA
eUmoWXLS/C4CcBqPa9til8ei3rDn/w8dveVHsi9FXjtVSYqN+ilKw+moMAjZy4kN
/kpdpHMohwv/909VWR1AZbr+YTxaG/++tKl5bqXnZl4wHF8xAkEA5vwut8USRg2/
TndOt1e8ILEQNHvHQdQr2et/xNH4ZEo7mqot6skkCD1xmxA6XG64hR3BfxFSZcew
Wr4SOFGCtQJBAMurr5FYPJRFGzPM3HwcpAaaMIUtPwNyTtTjywlYcUI7iZVVfbdx
4B7qOadPybTg7wqUrGVkPSzzQelz9YCSSV8CQFqpIsEYhbqfTLZEl83YjsuaE801
xBivaWLIT0b2TvM2O7zSDOG5fv4I990v+mgrQRtmeXshVmEChtKnBcm7HH0CQE6B
2WUfLArDMJ8hAoRczeU1nipXrIh5kWWCgQsTKmUrafdEQvdpT8ja5GpX2Rp98eaU
NHfI0cP36JpCdome2eUCQDZN9OrTgPfeDIXzyOiUUwFlzS1idkUGL9nH86iuPnd7
WVF3rV9Dse30sVEk63Yky8uKUy7yPUNWldG4U5vRKmY=
-----END RSA PRIVATE KEY-----
```

For SSH, RUGGEDCOM ROS requires a DSA key pair in PEM format. The DSA key must be between 512 and 2048 bits in length for Controlled versions. The key file is uploaded to the `ssh.keys` flash file on the device.

The following is an example of a PEM formatted SSH key:

```
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQD0gcGbXx/rrEMu2913UW4cYo1OlcbnuUz7OZyd2mBLDx/GYbD8
X5TnRcMraJ0RuuGK+chqQJW5k3zQmZa/BS6q9U7wYwIAx8JSxxpwfPfl/t09VwKG
rtSJIMpLRoDq3qEwEVyR4kDUo4LFQDsljtiyhcz1n6kd6gqsd5Xu1vdh4wIVANXb
SBi97GmZ6/9f4UCvIIBtXLEjAoGAAfmhkcCCEnRJitUTiCE+MurxdFUr3mFs/d31
4cUDaLStQEhYYmx5dbFdQuapl4Y32B7lZQkohi5q1T1iUAa40/nUnJx1hFvblkYT
8DLwxcuDAaiu0VqsaPtJ+baL2dYNp96tFisj/475PEEWBGbP6GSe5kKa1Zdgwuie
9LyPb+ACgYBv856v5tb9UVG5+tX5Crfv/Nd8FFlSSFKmVWW3yzguhHajg2LQg8UU
sm1/zPSwYQ0SbQ9aOAJnpLc2HUkK0lji/0oKVI7y9MMc4B+bGu4W4OnryP7oFpnp
YYHt5PJY+zvLw/Wa+u3NOVFHkF1tGyfVBMXeV36nowPo+wrVMolAEgIVALLTnfpW
maV6uh6RxeE1d4XoxSg2
-----END DSA PRIVATE KEY-----
```

Certificates and keys are uploaded using the same file transfer mechanisms discussed in previous sections.

Please refer to Section 1.2, “Security Recommendations and Considerations” for a detailed discussion of encryption key management.

2 Using ROS

This chapter describes how to use the RUGGEDCOM ROS interface. It describes the following tasks:

Section 2.1
Connecting to ROS

The following describes the various methods for connecting the device:

Section 2.1.1
Connecting Directly

RUGGEDCOM ROS can be accessed through a direct RS-232 serial console connection for management and troubleshooting purposes. A console connection provides access to the console interface and CLI.

To establish a console connection to the device, do the following:

Section 2.1.2
Connecting via the Network

RUGGEDCOM ROS can be accessed over the network either through a Web browser, terminal or a workstation running terminal emulation software.

Using a Web Browser

Web browsers provide a secure connection to the Web interface for RUGGEDCOM ROS using the SSL (Secure Socket Layer) communication method. SSL encrypts traffic exchanged with its clients.

The RUGGEDCOM ROS Web server guarantees that all communications with the client are private. If a client requests access through an insecure HTTP port, the client is automatically rerouted to the secure port. Access to the Web server through SSL will only be granted to clients that provide a valid user name and password.

To establish a connection through a Web browser, do the following:

1. On the workstation being used to access the device, configure an Ethernet port to use an IP address falling within the subnet of the device. The default IP address is 192.168.0.1/24.

   For example, to configure the device to connect to one of the available Ethernet ports, assign an IP address to the Ethernet port on the workstation in the range of 192.168.0.3 to 192.168.0.254.

2. Open a Web browser. For a list of recommended Web browsers, refer to the section called "System Requirements".

   IMPORTANT!
   Upon connecting to the device, some Web browsers may report the Web server's certificate cannot be verified against any known certificates. This is expected behavior, and it is safe to instruct the browser to accept the certificate. Once the certificate is accepted, all communications with the Web server through that browser will be secure.

3. In the address bar, type the IP address for the port that is connected to the network. For example, to access the device using its factory default IP address, type **`https://192.168.0.1`** and press **Enter**. Once the connection is established, the login screen for the Web interface appears.

   For more information about logging in to the device, refer to Section 2.2, "Logging In". For more information about the Web interface, refer to Section 2.4, "Using the Web Interface".

Using a Terminal or Terminal Emulation Software

A terminal or computer running terminal emulation software provides access to the console interface for RUGGEDCOM ROS through a Telnet, RSH (Remote Shell) or SSH (Secure Shell) service.

NOTE
IP services can be restricted to control access to the device. For more information, refer to Section 3.3, "IP Services".

To establish a connection through a terminal or terminal emulation software, do the following:

1. Select the service (i.e. Telnet, RSH or SSH).
2. Enter the IP address for the port that is connected to the network.
3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to Section 2.2, "Logging In".

Section 2.2

Logging In

To log in to the device, do the following:

1. Connect to the device either directly or through a Web browser. For more information about how to connect to the device, refer to Section 2.1, "Connecting to ROS".

   Once the connection is established, the login form appears.

Figure 1: SSH Login Screen (Console Interface)

1. User Name Box **2.** Password Box

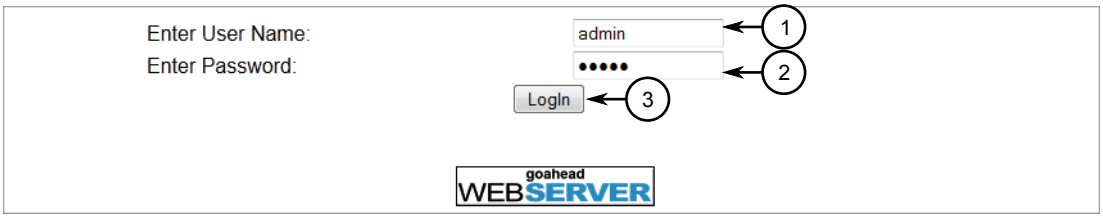


Figure 2: Login Screen (Web Interface)

1. Username Box **2.** Password Box **3.** Login Button

NOTE

The following default usernames and passwords are set on the device for each user type:

Guest	***Operator***	***Admin***
Username: guest	*Username: operator*	*Username: admin*
Password: guest	*Password: operator*	*Password: admin*

CAUTION!

To prevent unauthorized access to the device, make sure to change the default guest, operator, and admin passwords before commissioning the device.

For more information about changing passwords, refer to Section 3.6, "Passwords".

2. In the **User Name** field, type the username for an account setup on the device.
3. In the **Password** field, typ the password for the account.
4. Click **Enter** or click **Login** (Web interface only).

Section 2.3

Logging Out

To log out of the device, navigate to the main screen and do the following:

- To log out of the Console or secure shell interfaces, press **CTRL** + **X**.
- To log out of the Web interface, click **Logout**.

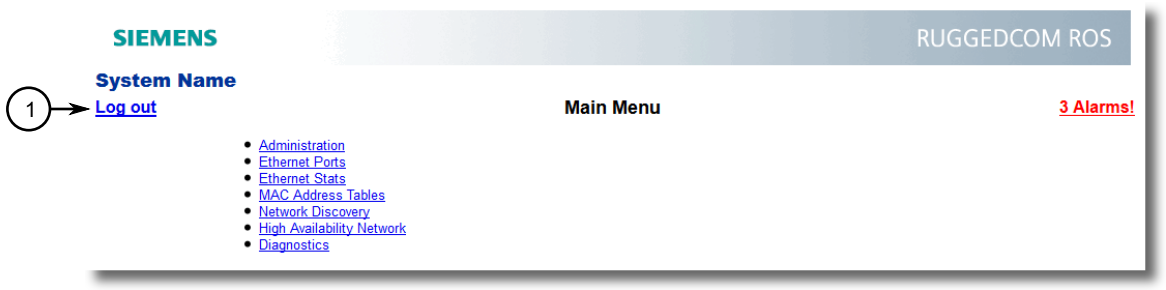


Figure 3: Web Interface

1. Logout

NOTE

If any pending configuration changes have not been committed, RUGGEDCOM ROS will request confirmation before discarding the changes and logging out of the device.

Section 2.4

Using the Web Interface

The user interface is organized as a series of linked web pages. The main menu provides the links at the top level of the menu hierarchy and allows them to be expanded to display lower-level links for each configuration subsystem.

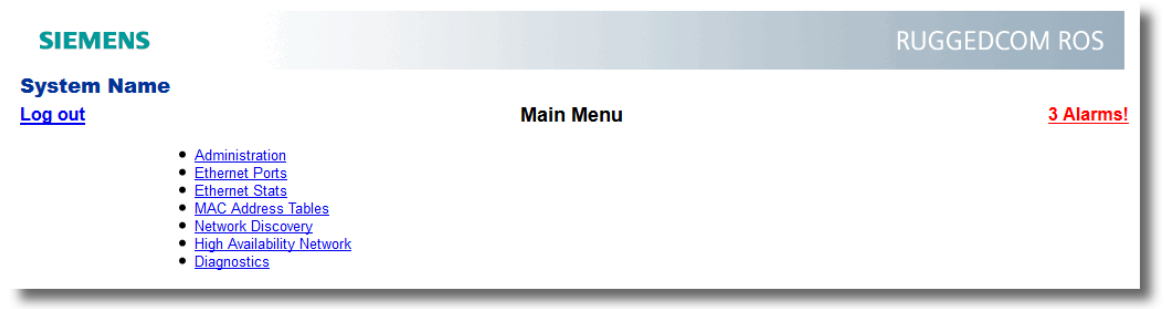


Figure 4: Main Menu via Web Server Interface

Every web page in the menu system has a common header section which contains:

- The System Name, as configured in the System Identification menu, is displayed below the top banner.
- A "Log out" link at left and immediately below the System Name, terminates the current web session.
- A "Back" link at left and below "Log out" links back to the previously viewed page.
- The menu title, in the center of the page and below the banner, is a link to a context-sensitive help page.
- The access level, e.g. "access admin", is displayed by default at the right of the page and below the banner. If, however, any alarms are pending, the text will be replaced with a link which displays the number of pending alarms. Following this link displays a table of pending alarms.

Figure 5: Web Page Header Showing Alarms Link

Section 2.5

Using the Console Interface

The Console interface is a Graphical User Interface (GUI) organized as a series of menus. It is primarily accessible through a serial console connection, but can also be accessed through IP services, such as a Telnet, RSH (Remote Shell), or SSH (Secure Shell) session.

NOTE
IP services can be restricted to control access to the device. For more information, refer to Section 3.3, "IP Services".

Each screen consists of a system identifier, the name of the current menu, and a command bar. Alarms are also indicated on each screen in the upper right corner.

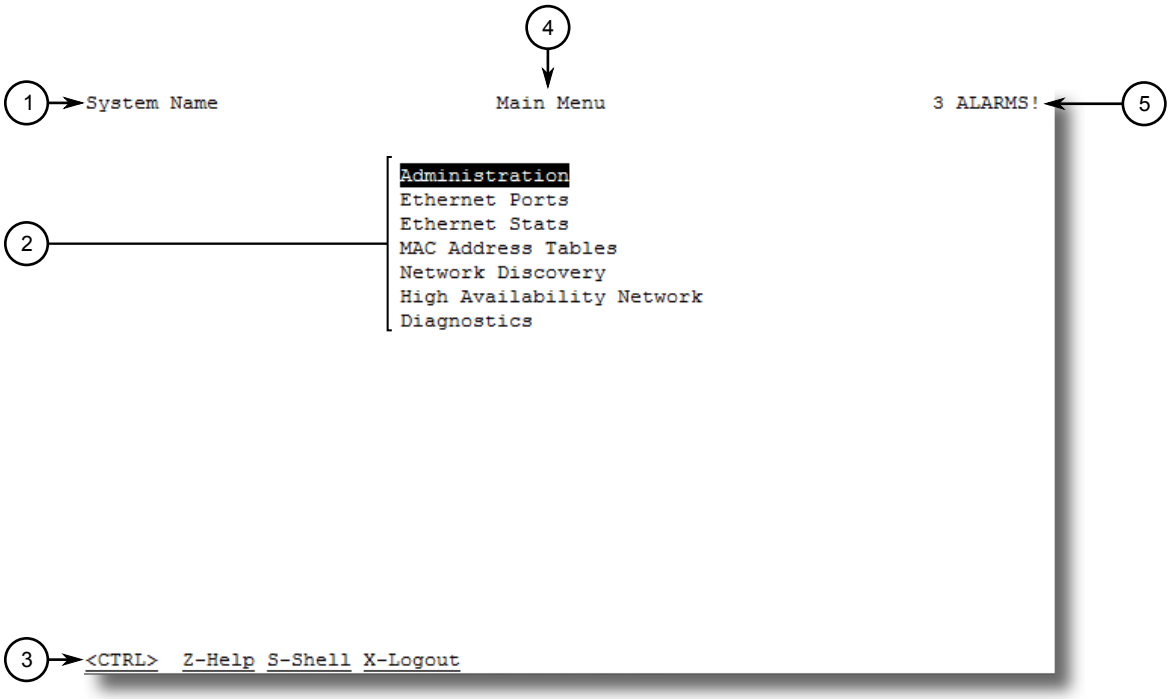


Figure 6: Console Interface (Example)

1. System Identification **2.** Menus **3.** Command Bar **4.** Menu Name **5.** Alarms Indicator

NOTE

They system identifier is user configurable. For more information about setting the system name, refer to Section 3.5, "System Identification".

Navigating the Interface

Use the following controls to navigate between screens in the Console interface:

Enter	Select a menu item and press this **Enter** to enter the sub-menu or screen beneath.
Esc	Press **Esc** to return to the previous screen.

Configuring Parameters

Use the following controls to select and configure parameters in the Console interface:

Up/Down Arrow Keys	Use the up and down arrow keys to select parameters.
Enter	Select a parameter and press **Enter** to start editing a parameter. Press **Enter** again to commit the change.
Esc	When editing a parameter, press **Esc** to abort all changes.

Commands

The command bar lists the various commands that can be issued in the Console interface. Some commands are specific to select screens. The standard commands include the following:

Ctrl + A	Commits configuration changes made on the current screen. **NOTE** *Before exiting a screen, RUGGEDCOM ROS will automatically prompt the user to save any changes that have not been committed.*
Ctrl + I	Inserts a new record.
Ctrl + S	Opens the CLI interface.
Ctrl + X	Terminates the current session. This command is only available from the main menu.
Ctrl + Z	Displays important information about the current screen or selected parameter.

Section 2.6
Using the Command Line Interface

The following sections describe how to use the Command Line Interface (CLI):

- Section 2.6.1, “Available CLI Commands”
- Section 2.6.2, “Tracing Events”
- Section 2.6.3, “Executing Commands Remotely via RSH”
- Section 2.6.4, “Using SQL Commands”

Section 2.6.1
Available CLI Commands

The following commands are available at the command line:

Command	Description
alarms `all`	Displays a list of available alarms. Optional and/or required parameters include: • `all` displays all available alarms
arp	Displays the IP to MAC address resolution table.
clearalarms	Clears all alarms.
clearethstats `[ all | port ]`	Clears Ethernet statistics for one or more ports. Optional and/or required parameters include: • `all` clears statistics for all ports • *port* is a comma separated list of port numbers (e.g. 1,3-5,7)
clearlogs	Clears the system and crash logs.
clrcblstats `[ all | port ]`	Clears cable diagnostics statistics for one or more ports. Optional and/or required parameters include:

Command	Description
	• `all` clears statistics for all ports • *`port`* is a comma separated list of port numbers (e.g. 1,3-5,7)
`clrstpstats`	Clears all spanning tree statistics.
`cls`	Clears the screen.
`dir`	Prints the directory listing.
`exit`	Terminates the session.
`factory`	Enables factory mode, which includes several factory-level commands used for testing and troubleshooting. Only available to admin users. **CAUTION!** *Misuse of the factory commands may corrupt the operational state of device and/or may permanently damage the ability to recover the device without manufacturer intervention.*
`flashfiles` { `info` *`filename`* | `defrag` }	A set of diagnostic commands to display information about the Flash filesystem and to defragment Flash memory. Optional and/or required parameters include: • `info` *`filename`* displays information about the specified file in the Flash file system • `defrag` defragments files in the Flash file system For more information about the **`flashfiles`** command, refer to Section 2.7, "Managing the Flash File System".
`flashleds` *`timeout`*	Flashes the LED indicators on the device for a specified number of seconds. Optional and/or required parameters include: • *`timeout`* is the number of seconds to flash the LED indicators. To stop the LEDs from flashing, set the timeout period to 0 (zero).
`help` *`command`*	Displays a brief description of the specified command. If no command is specified, it displays a list of all available commands, including a description for each. Optional and/or required parameters include: • *`command`* is the command
`ipconfig`	Displays the current IP address, subnet mask and default gateway. This command provides the only way of determining these values when DHCP is used.
`loaddflts`	Loads the factory default configuration.
`login`	Logs in to the shell.
`logout`	Logs out of the shell.
`ping` *`address`* { *`count`* | *`timeout`* }	Sends an ICMP echo request to a remotely connected device. For each reply received, the round trip time is displayed. Use this command to verify connectivity to the next connected device. It is a useful tool for testing commissioned links. This command also includes the ability to send a specific number of pings with a specified time for which to wait for a response. Optional and/or required parameters include: • *`address`* is the target IP address. • *`count`* is the number of echo requests to send. The default is 4. • *`timeout`* is the time in milliseconds to wait for each reply. The range is 2 to 5000 seconds. The default is 300 milliseconds. **NOTE** *The device to be pinged must support ICMP echo. Upon commencing the ping, an ARP request for the MAC address of the device is issued. If the device to be*

Command	Description
	pinged is not on the same network as the device pinging the other device, the default gateway must be programmed.
purgemac	Purges the MAC Addrtess table.
reset	Perform a hard reset of the switch.
resetport { all | *ports* }	Resets one or more Ethernet ports, which may be useful for forcing re-negotiation of speed and duplex, or in situations where the link partner has latched into an inappropriate state. Optional and/or required parameters include: • all resets all ports • *ports* is a comma separated list of port numbers (e.g. 1,3-5,7)
route	Displays the gateway configuration.
sql { default | delete | help | info | insert | save | select | update }	Provides an SQL-like interface for manipulating all system configuration and status parameters. All commands, clauses, table, and column names are case insensitive. Optional and/or required parameters include: • default sets all records in a table(s) to factory defaults • delete allows for records to be deleted from a table • help provides a brief description for any SQL command or clause • info displays a variety of information about the tables in the database • insert enables new records to be inserted into a table • save saves the database to non-volatile memory storage • select queries the dtabase and displays selected records • update enable existing records in a table to be updated For more information about the **sql** command, refer to Section 2.6.4, "Using SQL Commands".
telnet *dest*	Opens a telnet session. Press **Ctrl-C** to close the session. Optional and/or required parameters include: • *dest* is the server's IP address
tftp { *dest* | *cmd* | *fsource* | *fdest* }	Opens a TFTP session. Press **Ctrl-C** to close the session. Optional and/or required parameters include: • *dest* is the remote TFTP server's IP address • *cmd* is either **put** (upload) or **get** (download) • *fsource* is the source filename • *fdest* is the destination filename
trace	Starts event tracing. Run **trace ?** for more help.
type *filename*	Displays the contents of a text file. Optional and/or required parameters include: • *filename* is the name of the file to be read
version	Prints the software version.
xmodem { send | receive } *filename*	Opens an XModem session. Optional and/or required parameters include: • send sends the file to the client. • receive receives the file from the client. • *filename* is the name of the file to be read.

Section 2.6.2

Tracing Events

The CLI trace command provides a means to trace the operation of various protocols supported by the device. Trace provides detailed information, including STP packet decodes, IGMP activity and MAC address displays.

NOTE
Tracing has been designed to provide detailed information to expert users. Note that all tracing is disabled upon device startup.

To display the current trace settings and discover the systems that are being traced, enter the CLI command **`trace`** `?`.

```
>trace ?
Supported commands:
noclear          Starts the log without clearing it first
alloff           Disables all trace subsystems from tracing
allon            Enables all flags in all trace subsystems
transport        Traces IP Transport for Serial Protocols
secconn          Traces SSL and SSH connections
snmp             Traces SNMP communications
ip               Traces IP communications
ipassign         Traces IP assignement
tacplus          Traces TACACS+ client-server communication
radius           Traces RADIUS client-server communication
Iec62439         Traces IEC62439 protocols

Enter "trace command ?" for more information on a particular command.
TRANSPORT: Logging is disabled
SECCONN : Logging is disabled
SNMP : Logging is disabled
IP   : Logging is disabled
IPASSIGN : Logging is disabled
TacPlus : Logging is disabled
Radius : Logging is disabled
Iec62439 : Logging is disabled
```

The following sections describe how to enable and run traces:

- Section 2.6.2.1, “Enabling a Trace”
- Section 2.6.2.2, “Starting a Trace”

Section 2.6.2.1

Enabling a Trace

Tracing can be enabled on a per subsystem basis. However, some subsystems can only trace events on certain ports.

To enable a trace, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.
2. Determine the options available for a trace event by typing:

   ```
   trace protocol ?
   ```

   Where:

   - *`protocol`* is the protocol to trace

Example:

```
>trace stp ?
trace stp syntax:
  stp [-|+] [all] [verbose] [packets] [timers] [actions]
            [decodes] [ports[port_number|all]]
STP  : Logging is disabled
```

3. Choose the option to use and type:

```
trace protocol option
```

Where:

- *protocol* is the protocol to trace
- *option* is the option to use durign the trace

Example:

```
>trace ip ?
trace ip syntax
   ip decodes | raw_data | allon | alloff
or ip ports [port_number|all] on|off

IP   : Logging is disabled
```

4. Start the trace. For more information, refer to Section 2.6.2.2, “Starting a Trace”.

Section 2.6.2.2
Starting a Trace

To start a trace, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.
2. Start the trace by typing:

```
trace { noclear | clear }
```

Where:

- noclear displays all historical trace messages
- clear automatically clears the trace buffer

Example:

```
>trace ip allon
IP   : decodes, raw_data on no ports

>trace

Log has been cleared
01/13 00:05:58.010 IP  RX 00:13:3b:0c:80:1c ff:ff:ff:ff:ff:ff ARP 60b:
      arp who-has 192.168.0.191 tell 192.168.0.100
       0001 0800 0604 0001 0013 3b0c 801c c0a8
       0064 0000 0000 0000 c0a8 00bf 0000 0000
       0000 0000 0000 0000 0000 0000 0000
00:05:58.012 IP  TX 00:0a:dc:01:01:13 00:13:3b:0c:80:1c ARP 60b:
      arp reply 192.168.0.191 is-at 00:0a:dc:01:01:13
       0001 0800 0604 0002 000a dc01 0113 c0a8
       00bf 0013 3b0c 801c c0a8 0064 0000 0000
```

```
       0000 0000 0000 0000 0000 0000 0000
00:05:58.015 IP  RX 00:13:3b:0c:80:1c 00:0a:dc:01:01:13 IP 74b:
      192.168.0.100 > 192.168.0.191: ICMP
       4500 003c 68f8 0000 4001 8f55 c0a8 0064
       c0a8 00bf 0800 465c 0600 0100 6162 6364
       6566 6768 696a 6b6c 6d6e 6f70 7172 7374
       7576 7761 6263 6465 6667 6869
00:05:58.018 IP  TX 00:0a:dc:01:01:13 00:13:3b:0c:80:1c IP 74b:
      192.168.0.191 > 192.168.0.100: ICMP
       4500 003c 0004 0000 3c01 fc49 c0a8 00bf
       c0a8 0064 0000 4e5c 0600 0100 6162 6364
       6566 6768 696a 6b6c 6d6e 6f70 7172 7374
       7576 7761 6263 6465 6667 6869
```

Section 2.6.3

Executing Commands Remotely via RSH

The Remote Shell (RSH) facility can be used from a workstation to cause the product to act upon commands as if they were entered at the CLI prompt. The syntax of the RSH command is usually of the form:

```
rsh ipaddr -l auth_token command_string
```

Where:

- *ipaddr* is the address or resolved name of the device.
- *auth_token* is the is the user name (i.e. guest, operator or admin) and corresponding password separated by a comma. For example, *admin,secret*.
- *command_string* is the RUGGEDCOM ROS CLI command to execute.

NOTE
The access level (corresponding to the user name) selected must support the given command.

NOTE
Any output from the command will be returned to the workstation submitting the command. Commands that start interactive dialogs (such as **trace***) cannot be used.*

Section 2.6.4

Using SQL Commands

RUGGEDCOM ROS provides an *SQL-like* command facility that allows expert users to perform several operations not possible under the traditional Web or CLI interface. For instance:

- Restoring the contents of a specific table, but not the whole configuration, to their factory defaults.
- Search tables in the database for specific configurations.
- Make changes to tables predicated upon existing configurations.

When combined with RSH, SQL commands provide a means to query and configure large numbers of devices from a central location.

NOTE
For a list of parameters available under the **sql** *command, refer to Section 2.6.1, "Available CLI Commands".*

The following sections describe in more detail how to use SQL commands:

- Section 2.6.4.1, "Finding the Correct Table"
- Section 2.6.4.2, "Retrieving Information"
- Section 2.6.4.3, "Changing Values in a Table"
- Section 2.6.4.4, "Resetting a Table"
- Section 2.6.4.5, "Using RSH and SQL"

Section 2.6.4.1
Finding the Correct Table

Many SQL commands operate upon specific tables in the database, and require the table name to be specified. Navigating the menu system in the console interface to the desired menu and pressing **Ctrl-Z** displays the name of the table. The menu name and the corresponding database table name will be cited.

Another way to find a table name is to type the following in the CLI:

```
sql info tables
```

This command also displays menu names and their corresponding database table names depending upon the features supported by the device. For example:

```
Table Description
--------------------------------------------------------------------------------
alarms Alarms
cpuDiags CPU Diagnostics
ethPortCfg Port Parameters
ethPortStats Ethernet Statistics
ethPortStatus Port Status
ipCfg IP Services
```

Section 2.6.4.2
Retrieving Information

The following describes various methods for retrieving information about tables and parameters.

Retrieving Information from a Table

Use the following command to display a summary of the parameters within a table, as well as their values:

```
sql select from table
```

Where:

- *table* is the name of the table

Example:

```
>sql select from ipAddrtable
```

```
IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
172.30.146.88   255.255.224.0   1001       17007888   2994       default
192.168.0.1     255.255.255.0   1002       17007672   3195       vlan1

2 records selected
```

Retrieving Information About a Parameter from a Table

Use the following command to retrieve information about a specific parameter from a table:

NOTE
The parameter name must be the same as it is displayed in the menu system, unless the name contains spaces (e.g. ip address). Spaces must be replaced with underscores (e.g. ip_address) or the parameter name must be wrapped in double quotes (e.g. "ip address").

```
sql select parameter from table
```

Where:

- *parameter* is the name of the parameter
- *table* is the name of the table

Example:

```
>sql select "ip address" from ipSwitchIfCfg

IP Address
192.168.0.1

1 records selected
```

Retrieving Information from a Table Using the *Where* Clause

Use the following command to display specific parameters from a table that have a specific value:

```
sql select from table where parameter = value
```

Where:

- *table* is the name of the table
- *parameter* is the name of the parameter
- *value* is the value of the parameter

Example:

```
>sql select from ethportcfg where media = 1000T

Port Name            ifName          Media       State    AutoN Speed Dupx  FlowCtrl LFI Alarm
1/1  Port 1          1/1             1000T       Enabled  On    Auto  Auto  Off      Off On
1/2  Port 2          1/2             1000T       Enabled  On    Auto  Auto  Off      Off On
1/3  Port 3          1/3             1000T       Enabled  On    Auto  Auto  Off      Off On
1/4  Port 4          1/4             1000T       Enabled  On    Auto  Auto  Off      Off On

4 records selected
```

Further refine the results by using `and` or `or` operators:

```
sql select from table where parameter = value [ { and | or } | parameter | = | value ...]
```

Where:

- *table* is the name of the table
- *parameter* is the name of the parameter

- *value* is the value of the parameter

Example:

```
>sql select from ethportcfg where media = 1000T and State = enabled

Port Name            ifName          Media       State    AutoN Speed Dupx  FlowCtrl LFI Alarm
1/1  Port 1          1/1             1000T       Enabled  On    Auto  Auto  Off      Off on
1/2  Port 2          1/2             1000T       Enabled  On    Auto  Auto  Off      Off On
1/3  Port 3          1/3             1000T       Enabled  On    Auto  Auto  Off      Off On
1/4  Port 4          1/4             1000T       Enabled  On    Auto  Auto  Off      Off On

4 records selected
```

Section 2.6.4.3
Changing Values in a Table

Use the following command to change the value of parameters in a table:

```
sql update table set parameter = value
```

Where:

- *table* is the name of the table
- *parameter* is the name of the parameter
- *value* is the value of the parameter

Example:

```
>sql update vlanportcfg set pvid = 2
8 records updated
```

Conditions can also be included in the command to apply changes only to parameters that meet specific criteria. In the following example, flow control is enabled on ports that are operating in 100 Mbps full-duplex mode with flow control disabled:

Conditions can also be included in the command to apply changes only to parameters that meet specific criteria. In the following example, the **PVID** is changed to 2 on port 1/2.

```
>sql update vlanportcfg set pvid = 2 where port = 1/2
1 records updated
```

Section 2.6.4.4
Resetting a Table

Use the following command to reset a table back to its factory defaults:

```
sql default into table
```

Where:

- *table* is the name of the table

Section 2.6.4.5
Using RSH and SQL

The combination of remote shell scripting and SQL commands offers a means to interrogate and maintain a large number of devices. Consistency of configuration across sites may be verified by this method. The following presents a simple example where the devices to interrogate are drawn from the file `Devices`:

```
C:> type Devices
10.0.1.1
10.0.1.2
10.0.1.3

c:\> for /F %i in (devices) do rsh %i -l admin,admin sql select from vlanportcfg where pvid = 2

C:\>rsh 10.0.1.1 -l admin,admin sql select from vlanportcfg where pvid = 2
Port   Trnk       Port(s) Type     PVID   PVID Format   GVRP        GVRPStatus
1/2    0                    1/2     Edge     2      Untagged      Disabled    Disabled

1 records selected

C:\>rsh 10.0.1.2 -l admin,admin sql select from vlanportcfg where pvid = 2
0 records selected

C:\>rsh 10.0.1.3 -l admin,admin sql select from vlanportcfg where pvid = 2

Port   Trnk Port(s) Type     PVID   PVID Format   GVRP GVRPStatus
1/1    0          1/1     Edge     2      Untagged      Disabled    Disabled
1/2    0          1/2     Edge     2      Untagged      Disabled    Disabled
1/3    0          1/3     Edge     2      Untagged      Disabled    Disabled
1/4    0          1/4     Edge     2      Untagged      Disabled    Disabled
5/1    0          5/1     Edge     2      Untagged      Disabled    Disabled
5/2    0          5/2     Edge     2      Untagged      Disabled    Disabled
5/3    0          5/3     Edge     2      Untagged      Disabled    Disabled
5/4    0          5/4     Edge     2      Untagged      Disabled    Disabled

8 records selected
C:\
```

Section 2.7
Managing the Flash File System

The following sections describe how to manage the flash file system:

- Section 2.7.1, “Viewing a List of Flash Files”
- Section 2.7.2, “Viewing a List of Flash File Details”
- Section 2.7.3, “Defragmenting the Flash File System”

Section 2.7.1
Viewing a List of Flash Files

To view a list of files currently stored in Flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.

2. Type **`flashfiles`**. A list of files currently in Flash memory is displayed, along with their locations and the amount of memory they consume. For example:

```
>flashfiles
------------------------------------------------------------------
Filename             Base   Size  Sectors     Used
------------------------------------------------------------------
main.bin         00810000 490000  129-201  4741611
system.bin       00CA0000 010000  202-202      256
syslog.txt       00CB0000 2E0000  203-248  2261328
ssh.keys         00F90000 010000  249-249      256
ssl.crt          00FA0000 010000  250-250      256
banner.txt       00FB0000 010000  251-251      256
crashlog.txt     00FC0000 010000  252-252      256
config.bak       00FD0000 010000  253-253     9441
config.csv       00FE0000 010000  254-254     9441
factory.txt      00FF0000 010000  255-255      890
------------------------------------------------------------------
```

Section 2.7.2

Viewing a List of Flash File Details

To view the details of a file currently stored in Flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.
2. Display information about a file by typing:

```
flashfiles info filename
```

Where:

- *`filename`* is the name of the file stored in Flash memory

Details, similar to the following, are displayed.

```
>flashfiles info main.bin

Flash file information for main.bin:
Header version   : 4
Platform         : ROS-CF52
File name        : main.bin
Firmware version : v3.8.0.QA3
Build date       : Oct 23 2009 13:32
File length      : 2726770
Board IDs        :  ff   1   9   b   8   a  19  17
                     4   5  11  15  13  14   f  18
                     2   7   3  10   c   d  12  16
Header CRC       : 0827
Header CRC Calc  : 0827
Body CRC         : a270
Body CRC Calc    : a270
```

Section 2.7.3

Defragmenting the Flash File System

The flash memory is defragmented automatically whenever there is not enough memory available for a binary upgrade. However, fragmentation can occur whenever a new file is uploaded to the unit. Fragmentation causes

sectors of available memory to become separated by ones allocated to files. In some cases, the total available memory might be sufficient for a binary upgrade, but that memory may not be available in one contiguous region.

To defragment the flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to Section 2.6, “Using the Command Line Interface”.
2. Defragment the flash memory by typing:

```
flashfiles defrag
```

3 Administration

The Administration menu covers the configuration of administrative parameters of both device and network (local services availability, security methods employed, system identification and functionality related to the IP network). The following sections describe the Administration menu in greater details:

Figure 7: Administration Menu

Section 3.1
IP Interface

These parameters provide the ability to configure IP connection parameters such as address, network and mask.

The user can configure one IP interface that multiplexes both management and control traffic.

The following IP services are available: TFTP server, SNMP server, Telnet server, SSH server, RSH server, Web server, authentication using a RADIUS server, DHCP client, and BOOTP client.

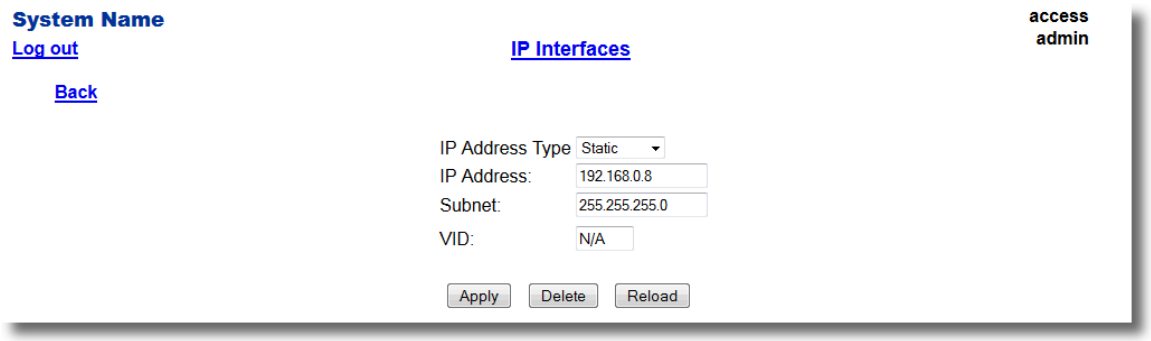


Figure 8: IP Interfaces Form

NOTE
Changes to the IP address take effect immediately. All IP connections in place at the time of an IP address change will be lost.

NOTE
*You can use the RUGGEDCOM ROS web interface to change the **IP Address Type** of the management interface from **Static** to **DHCP**. However, after doing so, you cannot use the web interface to change the **IP Address Type** back to **Static** and set an IP address. If you need to change the **IP Address Type** of the management interface from **DHCP** to **Static**, configure the setting through a telnet, SSH, RSH, or serial port connection, or upload a new configuration file to the device.*

Parameter	Description
IP Address Type	**Synopsis:** { Static, Dynamic, DHCP, BOOTP } **Default:** Static Specifies whether the IP address is static or dynamically assigned via DHCP or BOOTP. Options include: • `Static` – Must be used for a non-management interface. • `Dynamic` – Switches between DHCP and BOOTP until a response is received from the relevant server. • `DHCP` – Widely used in LAN environments to dynamically assign IP addresses from a centralized server, which reduces the overhead of administrating IP addresses. • `BOOTP` – A subset of the DHCP protocol. RUGGEDCOM ROS supports the transfer of a BOOTFILE via BOOTP. The BOOTFILE represents any valid RUGGEDCOM ROS file such as `config.csv`. The name of BOOTFILE on the BOOTP server must match the corresponding RUGGEDCOM ROS file.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 192.168.0.1

Parameter	Description
	Specifies the IP address of this device. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Only a unicast IP address is allowed, which ranges from 1.0.0.0 to 233.255.255.255.
Subnet	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 255.255.255.0 Specifies the IP subnet mask of this device. An IP subnet mask is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, subnet mask numbers use either 0 or 255 as values (e.g. 255.255.255.0) but other numbers can appear.
VID	**Synopsis:** 0 to 4094 or { N/A } **Default:** N/A Specifies the VLAN ID associated with the IP interface. N/A means no VLAN is associated the IP interface. RS950G is, by default, VLAN unaware. All VLAN tagged and non-VLAN tagged frames are accepted, and only non-VLAN tagged frames are returned. However, once a specific VLAN is specified, only frames tagged with the same VLAN are accepted and all other frames (tagged or not tagged) are dropped.

Section 3.2

IP Gateways

These parameters provide the ability to configure gateways. A maximum of 10 gateways can be configured. When both the Destination and Subnet fields are both 0.0.0.0 (displayed as blank space), the gateway is a default gateway.

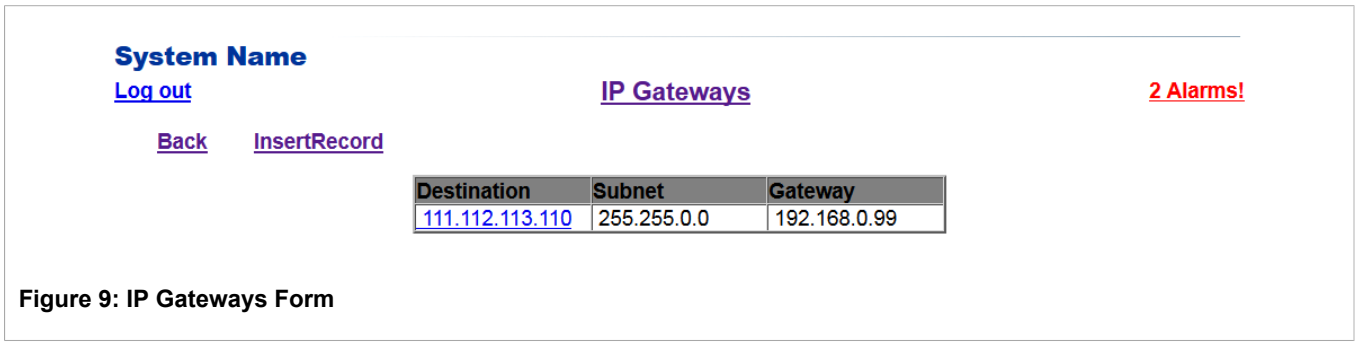


Figure 9: IP Gateways Form

Parameter	Description
Destination	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 0.0.0.0 Specifies the IP address of the destination device. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods.
Subnet	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 0.0.0.0 Specifies the IP subnet mask of the destination. An IP subnet mask is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, subnet mask numbers use either 0 or 255 as values (e.g. 255.255.255.0) but

Parameter	Description
	other numbers can appear. For the default gateway, both the destination and subnet are 0.
Gateway	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 0.0.0.0 Specifies the gateway IP address. The gateway address must be on the same IP subnet as this device.

NOTE
The default gateway configuration will not be changed when resetting all configuration parameters to defaults.

Section 3.3
IP Services

These parameters provide the ability to configure properties for IP services provided by the device.

Figure 10: IP Services Form

Parameter	Description
Inactivity Timeout	**Synopsis:** 1 to 60 or { Disabled } **Default:** 5 min Specifies when the console will timeout and display the login screen if there is no user activity. A value of zero disables timeouts for console and Telnet users. For Web Server users, the maximum timeout value is limited to 30 minutes.
Telnet Sessions Allowed	**Synopsis:** 0 to 4 **Default:** 0 (controlled version) **Default:** 4 (non-controlled version) Limits the number of Telnet sessions. A value of zero prevents any Telnet access.
Web Server Users Allowed	**Synopsis:** 1 to 16 **Default:** 16 Limits the number of simultaneous web server users.

Parameter	Description
TFTP Server	**Synopsis:** { Disabled, Get Only, Enabled } **Default:** Disabled As TFTP is a very insecure protocol, this parameter allows the user to limit or disable TFTP Server access. DISABLED - disables read and write access to a TFTP Server GET ONLY - only allows reading of files via a TFTP Server ENABLED - allows reading and writing of files via a TFTP Server
SSH Sessions Allowed (Controlled Version Only)	**Synopsis:** 1 to 4 **Default:** 4 Limits the number of SSH sessions.
RSH Server	**Synopsis:** { Disabled, Enabled } **Default:** Disabled (controlled version) **Default:** Enabled (non-controlled version) Disables/enables Remote Shell access.

Section 3.4
Data Storage

These parameters provide the ability to encrypt and password protect data in the CSV configuration file.

NOTE
Data encryption is not available in Non-Controlled (NC) versions of RUGGEDCOM ROS.

When switching between Controlled and Non-Controlled (NC) versions of RUGGEDCOM ROS, make sure data encryption is disabled. Otherwise, the NC version of RUGGEDCOM ROS will ignore the encrypted configuration file and load the factory defaults.

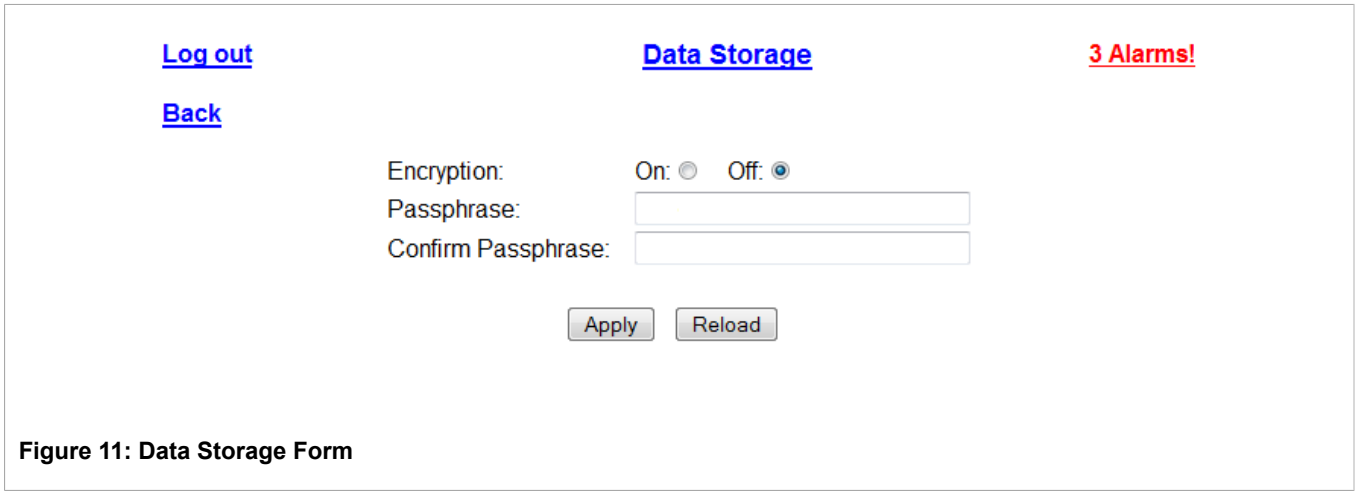


Figure 11: Data Storage Form

Parameter	Description
Encryption	**Synopsis:** { On, Off } **Default:** Off Enable/disable encryption of data in configuration file.
Passphrase	**Synopsis:** 31 character ascii string

Parameter	Description
	This passphrase is used as a secret key to encrypt the configuration data. Encrypted data can be decrypted by any device configured with the same passphrase.
Confirm Passphrase	**Synopsis:** 31 character ascii string This passphrase is used as a secret key to encrypt the configuration data. Encrypted data can be decrypted by any device configured with the same passphrase.

NOTE
Only configuration data is encrypted. All comments and table names in the configuration file are saved as clear text.

NOTE
When sharing a configuration file between devices, make sure both devices have the same passphrase configured. Otherwise, the configuration file will be rejected.

NOTE
Encryption must be disabled before the device is returned to Siemens or the configuration file is shared with Customer Support.

IMPORTANT!
Never downgrade the RUGGEDCOM ROS software version beyond RUGGEDCOM ROS 3.11.7 when encryption is enabled. Make sure the device has been restored to factory defaults before downgrading.

Section 3.5
System Identification

The system identification is displayed in the sign-on screen and in the upper left hand corner of all RUGGEDCOM ROS screens.

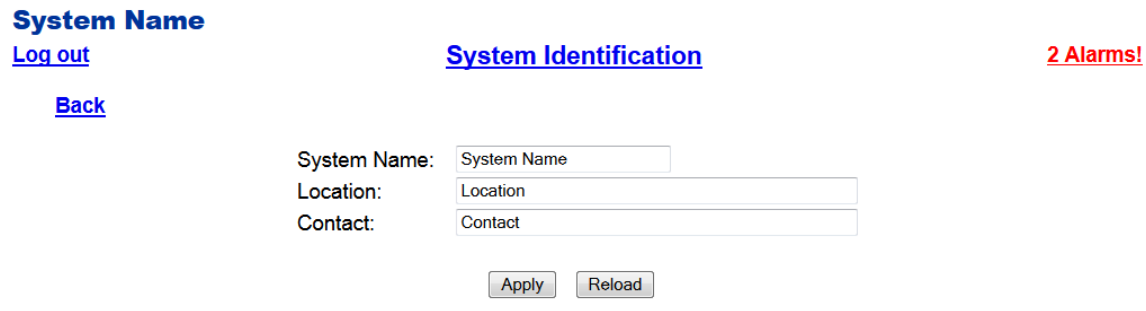


Figure 12: System Identification Form

Parameter	Description
System Name	**Synopsis:** Any 24 characters **Default:** System Name

Parameter	Description
	The system name is displayed in all RUGGEDCOM ROS menu screens. This can make it easier to identify the switches within your network, provided that all switches are given a unique name.
Location	**Synopsis:** Any 49 characters **Default:** Location The location can be used to indicate the physical location of the switch. It is displayed in the login screen as another means to ensure you are dealing with the desired switch.
Contact	**Synopsis:** Any 49 characters **Default:** Contact The contact can be used to help identify the person responsible for managing the switch. You can enter name, phone number, email, etc. It is displayed in the login screen so that this person may be contacted, should help be required.

Section 3.6

Passwords

These parameters provide the ability to configure parameters for authorized and authenticated access to the device's services (HMI via Serial Console, Telnet, SSH, RSH, Web Server). Access to the switch can be authorized and authenticated via RADIUS or TACACS+ servers, or using locally configured passwords that are configured per user name and access level.

Note that access via the Serial Console is authorized first using local settings. If a local match is not found, RADIUS/TACACS+ will be used if enabled. For all other services, if RADIUS or TACACS+ is enabled for authentication and authorization, but is unreachable, the local settings will be used if configured.

To access the unit, the user name and password must be provided.

Three user names and passwords can be configured. They correspond to three access levels, which provide or restrict access to change settings and execute various commands within the device.

- *guest* users can view most settings, but may not change settings or run commands
- *operator* cannot change settings, but can reset alarms, clear statistics and logs
- *admin* user can change all the settings and run commands

CAUTION!
To prevent unauthorized access to the device, make sure to change the default user, admin and guest passwords before commissioning the device.

When creating a new password, it should adhere to the following rules:

- Must not be less than 6 characters in length.
- Must not include the username or any 4 continous alphanumeric characters found in the username. For example, if the username is Subnet25, the password may not be subnet25admin or subnetadmin. However, net25admin or Sub25admin is permitted.
- Must have at least one alphabetic character and one number. Special characters are permitted.
- Must not have more than 3 continuously incrementing or decrementing numbers. For example, Sub123 and Sub19826 are permitted, but Sub12345 is not.

An alarm will generate if a weak password is configured. The weak password alarm can be disabled by user. For more information about disabling alarms, refer to Section 9.1.4, “Configuring Alarms”.

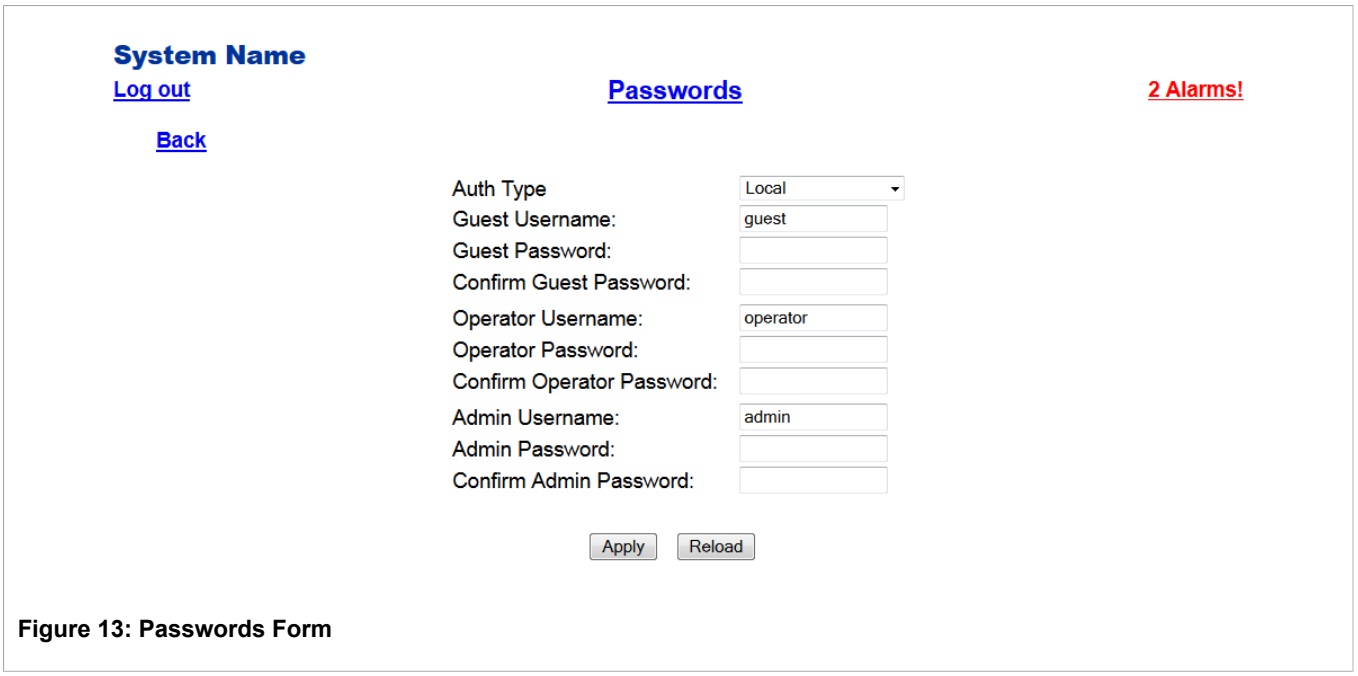


Figure 13: Passwords Form

Parameter	Description
Auth Type	**Synopsis:** { Local, RADIUS, TACACS+, RADIUSorLocal, TACACS+orLocal } **Default:** Local Password authentication can be performed using locally configured values, a remote RADIUS server, or a remote TACACS+ server. Setting this value to one of the combinations that includes RADIUS or TACACS+ requires that the Security Server Table be configured. • Local - authentication from the local Password Table • RADIUS - authentication using a RADIUS server • TACACS+ - authentication using a TACACS+ server • RADIUSOrLocal - authentication using RADIUS. If the server cannot be reached, authenticate from the local Password Table. • TACACS+OrLocal - authentication using TACACS+. If the server cannot be reached, authenticate from the local Password Table
Guest Username	**Synopsis:** Any 15 characters **Default:** guest Related password is in the Guest Password field; view only, cannot change settings or run any commands.
Guest Password	**Synopsis:** 15 character ASCII string **Default:** guest Related user name is in the Guest Username field; view only, cannot change settings or run any commands. Rules to generate strong password or secret key: 1. Should be no less than 6 characters in length. 2. Shall not have the username or the continuous 'alpha' part contained of 4 (four) characters of the username as part of itself. Eg. If username is Subnet25, password cannot be subnet25admin, it cannot be subnetadmin but it can be net25admin or Sub25admin. 3. Should have at least one alphabet and one number. Special characters can be there.

Parameter	Description
	4. Shall not have more than 3 continuously incrementing or decrementing numbers. Eg. Sub123 and Sub19826 is ok but Sub12345 is not. Alarm will be generated if weak password is configured! Weak password alarm can be disabled by user.
Confirm Guest Password	**Synopsis:** 15 character ASCII string **Default:** None Rules to generate strong password or secret key: Related username is in field Guest Username; view only, cannot change settings or run any commands. Rules to generate strong password or secret key: • Should be no less than 6 characters in length. • Shall not have the username or the continuous 'alpha' part contained of 4 (four) characters of the username as part of itself. Eg. If username is Subnet25, password cannot be subnet25admin, it cannot be subnetadmin but it can be net25admin or Sub25admin. • Should have at least one alphabet and one number. Special characters can be there. • Shall not have more than 3 continuously incrementing or decrementing numbers. Eg. Sub123 and Sub19826 is ok but Sub12345 is not. Alarm will be generated if weak password is configured! Weak password alarm can be disabled by user.
Operator Username	**Synopsis:** Any 15 characters **Default:** operator Related password is in the Oper Password field; cannot change settings; can reset alarms, statistics, logs, etc.
Operator Password	**Synopsis:** 15 character ASCII string **Default:** operator Related user name is in the Oper Username field; cannot change settings; can reset alarms, statistics, logs, etc. Rules to generate strong password or secret key: 1. Should be no less than 6 characters in length. 2. Shall not have the username or the continuous 'alpha' part contained of 4 (four) characters of the username as part of itself. Eg. If username is Subnet25, password cannot be subnet25admin, it cannot be subnetadmin but it can be net25admin or Sub25admin. 3. Should have at least one alphabet and one number. Special characters can be there. 4. Shall not have more than 3 continuously incrementing or decrementing numbers. Eg. Sub123 and Sub19826 is ok but Sub12345 is not. Alarm will be generated if weak password is configured! Weak password alarm can be disabled by user.
Confirm Operator Password	**Synopsis:** 15 character ASCII string **Default:** None Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc. Rules to generate strong password or secret key: 1. Should be no less than 6 characters in length. 2. Shall not have the username or the continuous 'alpha' part contained of 4 (four) characters of the username as part of itself. Eg. If username is Subnet25, password cannot be subnet25admin, it cannot be subnetadmin but it can be net25admin or Sub25admin.

Parameter	Description
	3. Should have at least one alphabet and one number. Special characters can be there. 4. Shall not have more than 3 continuously incrementing or decrementing numbers. Eg. Sub123 and Sub19826 is ok but Sub12345 is not. Alarm will be generated if weak password is configured! Weak password alarm can be disabled by user.
Admin Username	**Synopsis:** Any 15 characters **Default:** admin Related password is in the Admin Password field; full read/write access to all settings and commands.
Admin Password	**Synopsis:** 15 character ASCII string **Default:** admin Related user name is in the Admin Username field; full read/write access to all settings and commands. Rules to generate strong password or secret key: 1. Should be no less than 6 characters in length. 2. Shall not have the username or the continuous 'alpha' part contained of 4 (four) characters of the username as part of itself. Eg. If username is Subnet25, password cannot be subnet25admin, it cannot be subnetadmin but it can be net25admin or Sub25admin. 3. Should have at least one alphabet and one number. Special characters can be there. 4. Shall not have more than 3 continuously incrementing or decrementing numbers. Eg. Sub123 and Sub19826 is ok but Sub12345 is not. Alarm will be generated if weak password is configured! Weak password alarm can be disabled by user.
Confirm Admin Password	**Synopsis:** 15 character ASCII string **Default:** None Related username is in field Admin Username; full read/write access to all settings and commands. Rules to generate strong password or secret key: 1. Should be no less than 6 characters in length. 2. Shall not have the username or the continuous 'alpha' part contained of 4 (four) characters of the username as part of itself. Eg. If username is Subnet25, password cannot be subnet25admin, it cannot be subnetadmin but it can be net25admin or Sub25admin. 3. Should have at least one alphabet and one number. Special characters can be there. 4. Shall not have more than 3 continuously incrementing or decrementing numbers. Eg. Sub123 and Sub19826 is ok but Sub12345 is not. Alarm will be generated if weak password is configured! Weak password alarm can be disabled by user.

Section 3.7

System Time Management

RUGGEDCOM ROS running on the RS950G offers the following time-keeping and time synchronization features:

- Local hardware time keeping and time zone management
- Precision Time Protocol configuration

- SNTP time synchronization

The *System Time Manager* option within the RUGGEDCOM ROS Administration menu fully configures time keeping functions on a RUGGEDCOM ROS-based device:

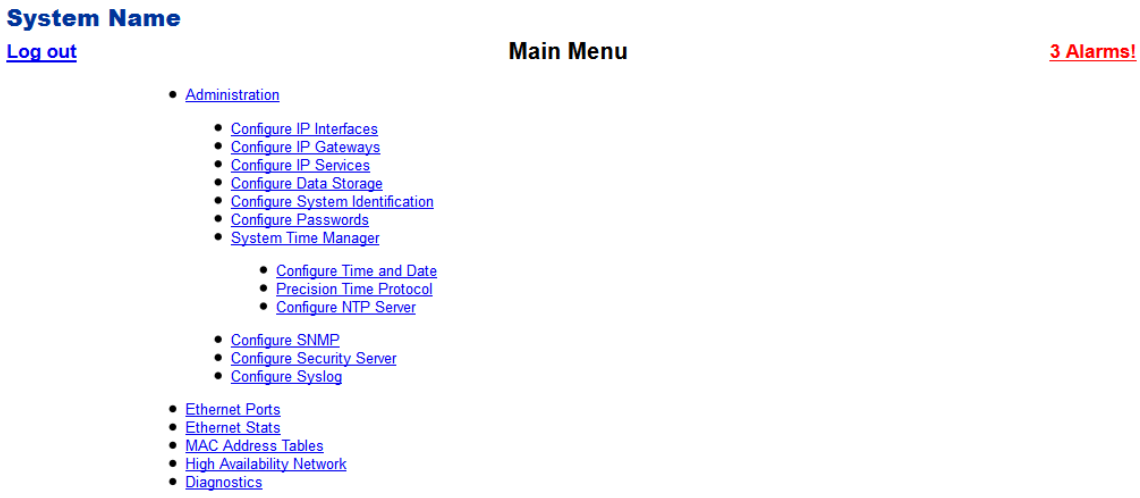


Figure 14: System Time Manager Menu

To configure system time management, refer to the following sections:

- Section 3.7.1, “Configuring Time and Date”
- Section 3.7.2, “Configuring Precision Time Protocol”
- Section 3.7.3, “Configuring NTP Service”

Section 3.7.1

Configuring Time and Date

This menu configures the current time, date, time zone, and DST (Daylight Savings Time) settings.

Figure 15: Time and Date Form

Parameter	Description
Time	**Synopsis:** HH:MM:SS This parameter enables both the viewing and setting of the local time.
Date	**Synopsis:** MMM DD, YYYY This parameter enables both the viewing and setting of the local date.
Time Zone	**Synopsis:** { UTC-12:00 (Eniwetok, Kwajalein), UTC-11:00 (Midway Island, Samoa), UTC-10:00 (Hawaii), UTC-9:00 (Alaska), UTC-8:00 (Los Angeles, Vancouver), UTC-7:00 (Calgary, Denver), UTC-6:00 (Chicago, Mexico City), UTC-5:00 (New York, Toronto), UTC-4:30 (Caracas), UTC-4:00 (Santiago), UTC-3:30 (Newfoundland), UTC-3:00 (Brasilia, Buenos Aires), UTC-2:00 (Mid Atlantic), UTC-1:00 (Azores), UTC-0:00 (Lisbon, London), UTC+1:00 (Berlin, Paris, Rome), ...} UTC+2:00 (Athens, Cairo, Helsinki), UTC+3:00 (Baghdad, Moscow), UTC+3:30 (Teheran), UTC+4:00 (Abu Dhabi, Kazan, Muscat), UTC+4:30 (Kabul), UTC+5:00 (Islamabad, Karachi), UTC+5:30 (Calcutta, New Delhi), UTC+5:45 (Kathmandu), UTC+6:00 (Almaty, Dhaka), UTC+6:30 (Rangoon), UTC+7:00 (Bangkok, Hanoi), UTC+8:00 (Beijing, Hong Kong) UTC+9:00 (Seoul, Tokyo), UTC+9:30 (Adelaide, Darwin), UTC+10:00 (Melbourne, Sydney), UTC+11:00 (Magadan, New Caledonia), UTC+12:00 (Auckland, Fiji) } **Default:** UTC-0:00 (Lisbon, London) This setting enables the conversion of UTC (Universal Coordinated Time) to local time.
DST Offset	**Synopsis:** HH:MM:SS **Default:** 00:00:00 This parameter specifies the amount of time to be shifted forward/backward when DST begins and ends. For example, for most of the USA and Canada, DST time shift is 1 hour (01:00:00) forward when DST begins and 1 hour backward when DST ends.
DST Rule	**Synopsis:** mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS **Default:** This parameter specifies a rule for time and date when the transition between Standard and Daylight Saving Time occurs. • mm - Month of the year (01 - January, 12 - December) • n - week of the month (1 - 1st week, 5 - 5th/last week) • d - day of the week (0 - Sunday, 6 - Saturday) • HH - hour of the day (0 - 24) • MM - minute of the hour (0 - 59) • SS - second of the minute (0 - 59) Example: The following rule applies in most of the USA and Canada: 03.2.0/02:00:00 11.1.0/02:00:00 In the example, DST begins on the second Sunday in March at 2:00am, and ends on the first Sunday in November at 2:00am.
Current UTC Offset	**Synopsis:** 0 s to 1000 s **Default:** 34 s Coordinated Universal Time (UTC) is a time standard based on International Atomic Time (TAI) with leap seconds added at

Parameter	Description
	irregular intervals to compensate for the Earth's slowing rotation. The Current UTC Offset parameter allows the user to adjust the difference between UTC and TAI. The International Earth Rotation and Reference System Service (IERS) observes the Earth's rotation and nearly six months in advance (January and July) a Bulletin-C message is sent out, which reports whether or not to add a leap second in the end of June and December. Please note that change in the Current UTC Offset parameter will result in a temporary disruption in the timing network.
Leap Second Pending	**Synopsis:** { No , Yes } **Default:** No This parameter allows user to manage the leap second event. A leap second is a second added to Coordinated Universal Time (UTC) in order to keep it synchronized with astronomical time. The International Earth Rotation and Reference System Service (IERS) observes the Earth's rotation and nearly six months in advance (January and July) a Bulletin-C message is sent out, which reports whether or not to add a leap second in the end of June and December. This parameter must set at least 5 minutes in advance before the occurrence of leap second event.

Section 3.7.2

Configuring Precision Time Protocol

The *Precision Time Protocol* (PTP) link on the main web menu leads to three sub-menus that configure the operation of Transparent Clock (TC) functionality on the RS950G.

Figure 16: Precision Time Protocol Menu

To configure precision time protocol, refer to the following sections:

- Section 3.7.2.1, “Global Parameters”

- Section 3.7.2.2, “Path Delay Settings”
- Section 3.7.2.3, “Viewing PTP Statistics”

Section 3.7.2.1
Global Parameters

This menu configures system PTP parameters.

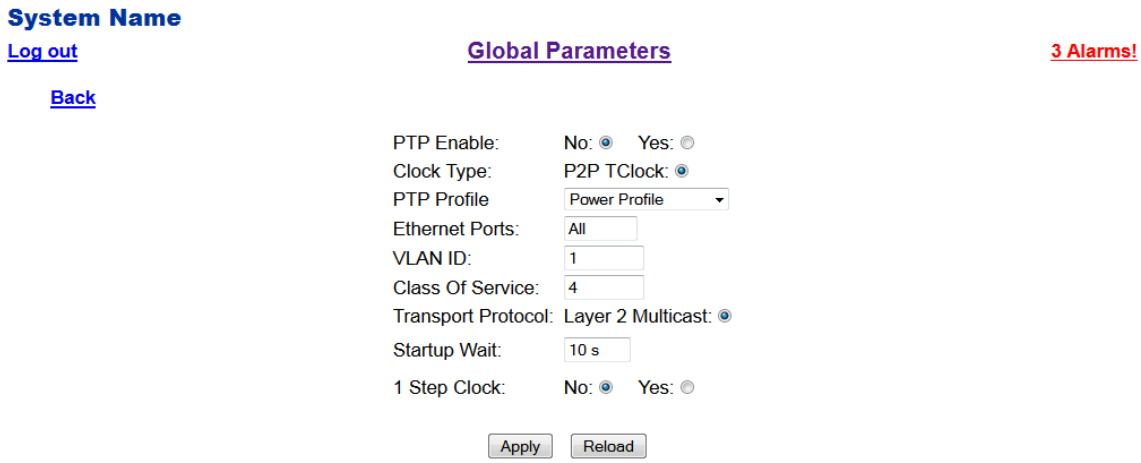


Figure 17: Global Parameters Form

Parameter	Description
PTP Enable	**Synopsis:** { No, Yes } **Default:** No **NOTE** *PTP messages are only sent and forwarded when PTP is enabled.* Enables PTP (Precision Time Protocol) protocol.
Clock Type	**Synopsis:** { P2P TClock } **Default:** P2P TClock Selects PTP (Precision Time Protocol) clock type.
PTP Profile	**Synopsis:** { Power Profile, Default P2P Profile, Custom Profile } **Default:** Power Profile Selects PTP (Precision Time Protocol) clock profile. PTP profile is the set of allowed PTP features applicable to a device. Supported profiles are Power Profile (IEEE C37.238), Default P2P (Peer-to-Peer) Profile as defined in IEEE 1588-2008 standard with layer 2 transport, and user defined Custom Profile.
Ethernet Ports	**Synopsis:** Any combination of numbers valid for this parameter **Default:** All Selects Ethernet port(s) which take part in PTP (Precision Time Protocol) message exchanges.
VLAN ID	**Synopsis:** 1 to 4095 or { Disable }

Parameter	Description
	Default: 1 The VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag. Frames tagged with a zero VLAN ID will always be associated with the VLAN ID 1 unless this parameter is configured.
Class Of Service	**Synopsis:** 1 to 7 or { Disable } **Default:** 4 Selects PTP (Precision Time Protocol) message priority based on IEEE 802.1p specification. IEEE 802.1p defines eight different classes of service which are available, usually expressed through the 3-bit priority field in an IEEE 802.1Q header added to the Ethernet frame. If VLAN option is enabled and Class Of Service option is 'Disable' then it represents priority '0' in terms of IEEE 802.1p specification.
Transport Protocol	**Synopsis:** { Layer 2 Multicast } **Default:** Layer 2 Multicast Selects layer 2 (Ethernet) multicast transport for PTP (Precision Time Protocol) messages.
Startup Wait	**Synopsis:** 0 to 3600 s **Default:** 10 s This parameter provides ability to bootstrap the PTP network in more orderly fashion.
1 Step Clock	**Synopsis:** { No, Yes } **Default:** Yes Selects 1-step or 2-step clock functionality.

Section 3.7.2.2
Path Delay Settings

This menu configures PTP (Precision Time Protocol) path delay attributes.

Figure 18: Path Delay Form

Parameter	Description
P2P Request Interval	**Synopsis:** { 1 s, 2 s, 4 s, 8 s, 16 s, 32 s } **Default:** 1 s Selects the PTP delay request interval (mean time interval between successive delay request messages), in seconds. The peer delay mechanism measures the port-to-port propagation time, such as the

Parameter	Description
	link delay, between two communicating ports supporting the peer delay mechanism.

Section 3.7.2.3
Viewing PTP Statistics

The View PTP Statistics menu provides links to forms where you can view PTP Clock and Peer Delay statistics.

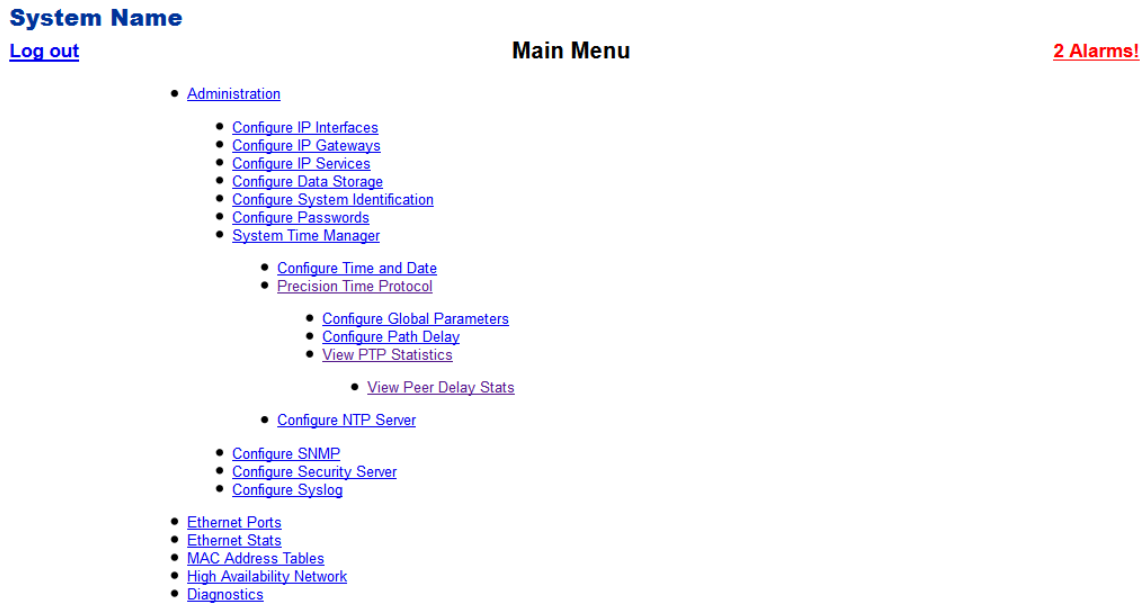


Figure 19: View PTP Statistics Menu

The Peer Delay Statistics form displays P2P (Peer To Peer) clock statistics for all ports. These statistics are updated every few seconds.

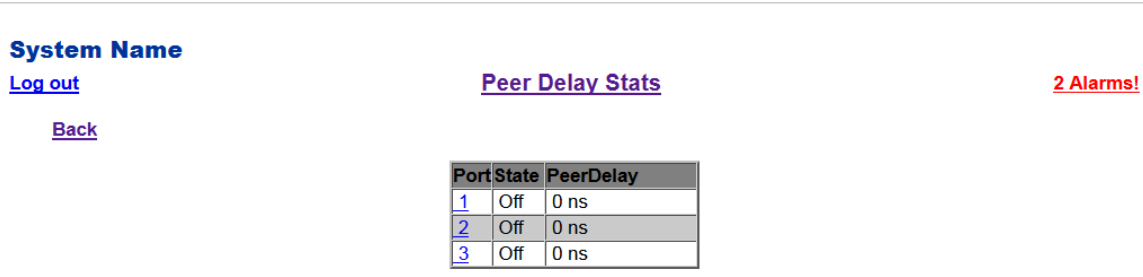


Figure 20: Peer Delay Statistics Form

Parameter	Description
Port	**Synopsis:** 1 to 3 The port number as seen on the front plate silkscreen.

Parameter	Description
State	**Synopsis:** { On, Off } The status of the PTP port with respect to the P2P (Peer To Peer) delay mechanism.
PeerDelay	**Synopsis:** 0 ns to 2147483647 ns Peer delay in nanoseconds. The peer delay mechanism measures the port-to-port propagation time, such as the link delay, between two communicating ports supporting the peer delay mechanism.

Section 3.7.3
Configuring NTP Service

RUGGEDCOM ROS may optionally be configured to refer periodically to a specified NTP server to correct any accumulated drift in the on-board clock. RUGGEDCOM ROS will also serve time via SNTP to hosts that request it.

Two NTP servers (primary and backup) may be configured for the device. The primary server is contacted first upon each attempt to update the system time. If the primary server fails to respond, the backup server is contacted. If either the primary or backup server fails to respond, an alarm is raised.

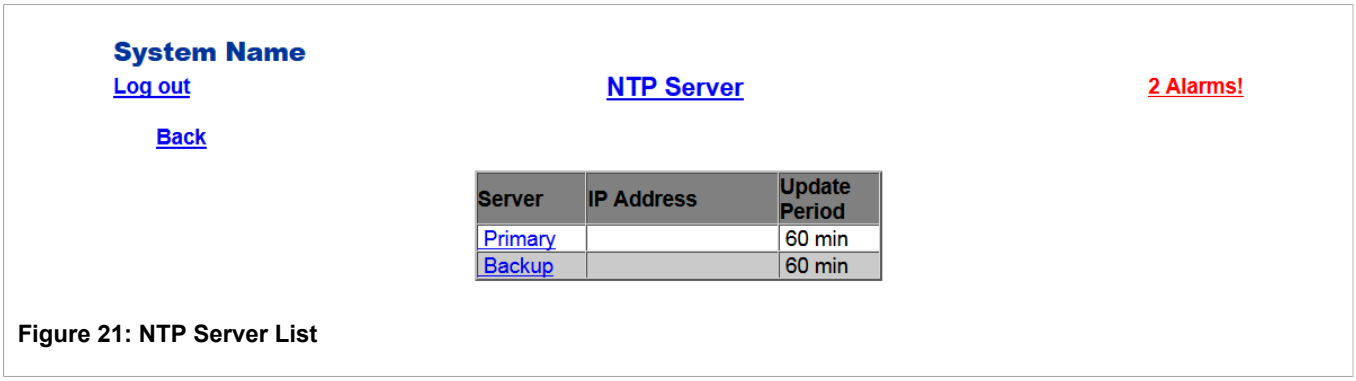


Figure 21: NTP Server List

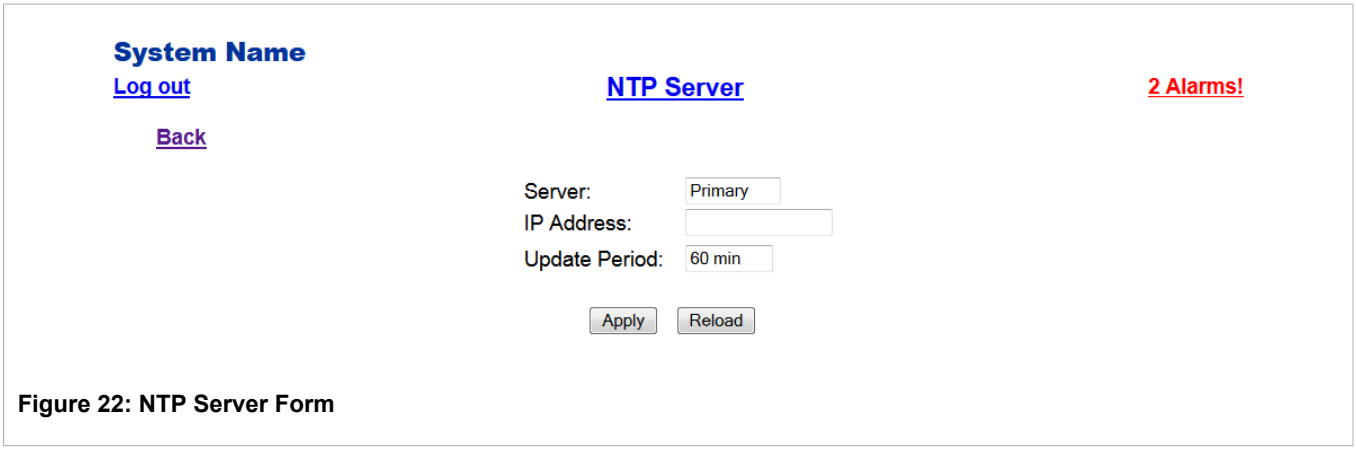


Figure 22: NTP Server Form

Parameter	Description
Server	**Synopsis:** Primary, Backup

Parameter	Description
	This field displays the chosen NTP server, which is either a primary or a backup server. The remaining fields on this form correspond to the chosen server.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** This parameter specifies the IP address of an (S)NTP server ((Simple) Network Time Protocol); programming an address of '0.0.0.0' disables SNTP requests. This device is an SNTP client which may connect to only one server. If a server address is programmed then a manual setting of the time will be overwritten at the next update period.
Update Period	**Synopsis:** 1 min to 1440 min **Default:** 60 min This setting determines how frequently the (S)NTP server is polled for a time update. If the server cannot be reached, three attempts are made at one-minute intervals and then an alarm is generated, at which point the programmed rate is resumed.

Section 3.8

SNMP Management

RUGGEDCOM ROS supports Simple Network Management Protocol Versions 1 (SNMPv1), 2 (SNMPv2c), and 3 (SNMPv3). SNMPv3 protocol provides secure access to devices by a combination of authentication and packet encryption over the network. SNMPv3 security features include the following:

- message integrity – ensures that a packet has not been tampered with in-transit.
- authentication – determines the message is from a valid source.
- encryption – scrambles the contents of a packet to prevent it from being seen by an unauthorized source.

SNMPv3 provides security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is a permitted level of security within a security model. A combination of a security model and security level will determine which security mechanism is employed when handling an SNMP packet.

Note the following about the SNMPv3 protocol:

- each user belongs to a group.
- a group defines the access policy for a set of users.
- an access policy defines what SNMP objects can be accessed for: reading, writing and creating notifications.
- a group determines the list of notifications its users can receive.
- a group also defines the security model and security level for its users.

Community is configured for protocols v1 and v2c. Community is mapped to the group and access level with security name (which is configured as User name).

To configure SNMP, refer to the following sections:

- Section 3.8.1, “SNMP Users”
- Section 3.8.2, “SNMP Security to Group Maps”
- Section 3.8.3, “SNMP Access”

Section 3.8.1
SNMP Users

These parameters provide the ability to configure users for the local SNMPv3 engine, along with the community for SNMPv1 and SNMPv2c. Note that when employing the SNMPv1 or SNMPv2c security level, the User Name maps the community name with the security group and access level. Up to 32 entries can be configured.

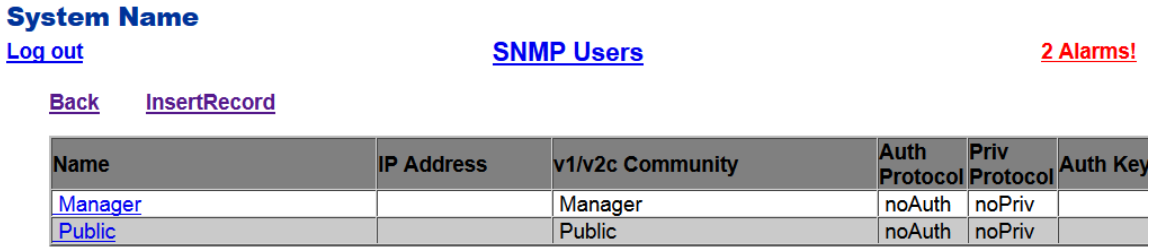


Figure 23: SNMP User Table

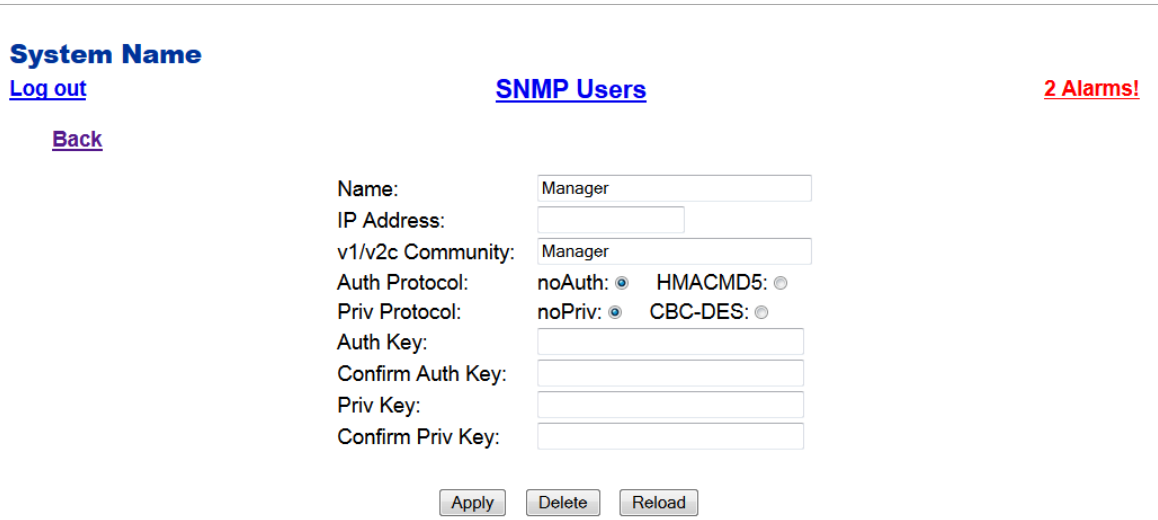


Figure 24: SNMP User Form

Parameter	Description
Name	**Synopsis:** Any 32 characters **Default:** initial The name of the user. This user name also represents the security name that maps this user to the security group.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** The IP address of the user's SNMP management station. If IP address is configured, SNMP requests from that user will be verified by IP address as well. SNMP Authentication trap will be generated to trap receivers if request was received from this user, but from any other IP address. If IP address is empty, traps can not be generated to this user, but SNMP requests will be served for this user from any IP address.

Parameter	Description
v1/v2c Community	**Synopsis:** Any 32 characters **Default:** The community string which is mapped by this user/security name to the security group if security model is SNMPv1 or SNMPv2c. If this string is left empty, it will be assumed to be equal to the same as user name.
Auth Protocol	**Synopsis:** { noAuth, HMACMD5 } **Default:** noAuth An indication of whether messages sent on behalf of this user to/from SNMP engine, can be authenticated, and if so, the type of authentication protocol which is used.
Priv Protocol	**Synopsis:** { noPriv, CBC-DES } **Default:** noPriv An indication of whether messages sent on behalf of this user to/from SNMP engine can be protected from disclosure, and if so, the type of privacy protocol which is used.
Auth Key	**Synopsis:** 31 character ASCII string **Default:** The secret authentication key (password) that must be shared with SNMP client. if the key is not an emtpy string, it must be at least 6 characters long.
Confirm Auth Key	**Synopsis:** 31 character ASCII string **Default:** The secret authentication key (password) that must be shared with SNMP client. if the key is not an emtpy string, it must be at least 6 characters long.
Priv Key	**Synopsis:** 31 character ASCII string **Default:** The secret encription key (password) that must be shared with SNMP client. if the ke is not an emtpy string, it must be at least 6 characters long.
Confirm Priv Key	**Synopsis:** 31 character ASCII string **Default:** The secret encription key (password) that must be shared with SNMP client. if the ke is not an emtpy string, it must be at least 6 characters long.

Section 3.8.2

SNMP Security to Group Maps

Entries in this table map configuration of security model and security name (user) into a group name, which is used to define an access control policy. Up to 32 entries can be configured.

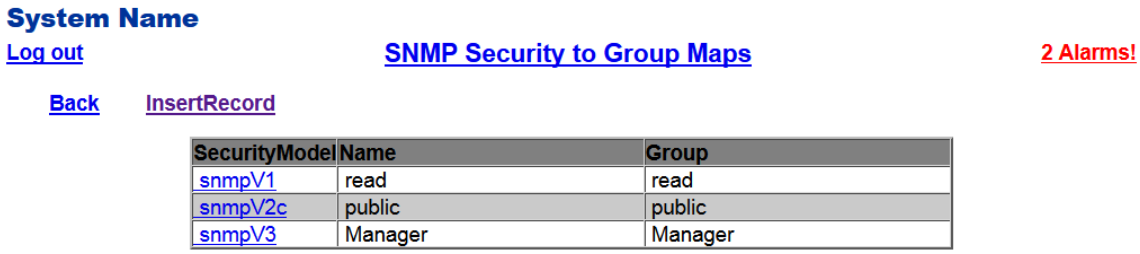


Figure 25: SNMP Security to Group Maps Table

Figure 26: SNMP Security to Group Maps Form

Parameter	Description
SecurityModel	**Synopsis:** { snmpV1, snmpV2c, snmpV3 } **Default:** snmpV3 The Security Model that provides the name referenced in this table.
Name	**Synopsis:** Any 32 characters **Default:** The user name which is mapped by this entry to the specified group name.
Group	**Synopsis:** Any 32 characters **Default:** The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.

Section 3.8.3

SNMP Access

These parameters provide the ability to configure access rights for groups.To determine whether access is allowed, one entry from this table needs to be selected and the proper view name from that entry must be used for access control checking. View names are predefined:

- noView - access is not allowed
- V1Mib - SNMPv3 MIBs excluded
- allOfMibs - all supported MIBs are included.

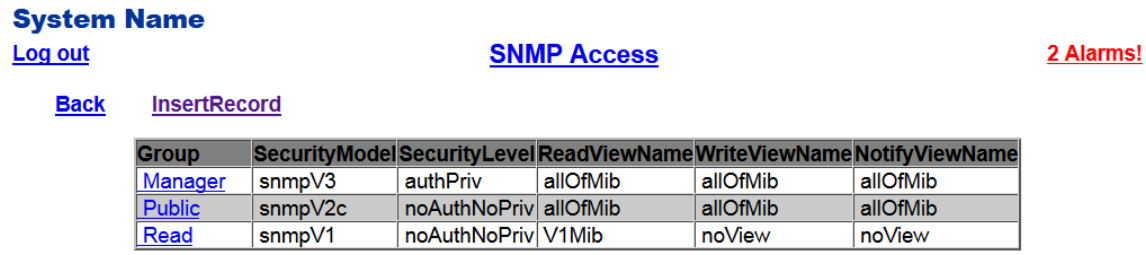


Figure 27: SNMP Access Table

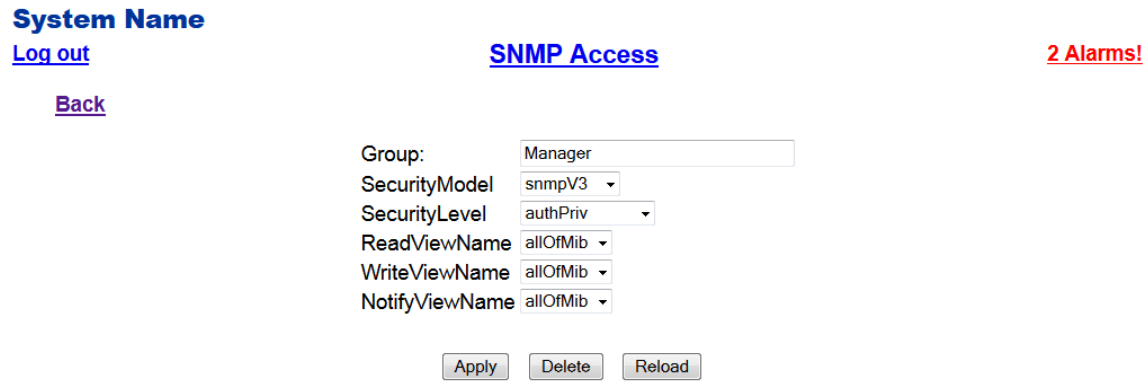


Figure 28: SNMP Access Form

Parameter	Description
Group	**Synopsis:** Any 32 characters **Default:** The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.
SecurityModel	**Synopsis:** { snmpV1, snmpV2c, snmpV3 } **Default:** snmpV3 In order to gain the access rights allowed by this entry, the configured security model must be in use.
SecurityLevel	**Synopsis:** { noAuthNoPriv, authNoPriv, authPriv } **Default:** noAuthNoPriv The minimum level of security required in order to gain the access rights allowed by this entry. A security level of noAuthNoPriv is less than authNoPriv, which is less than authPriv.
ReadViewName	**Synopsis:** { noView, V1Mib, allOfMib } **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes read access. If the value is noView, then read access will not be granted.
WriteViewName	**Synopsis:** { noView, V1Mib, allOfMib } **Default:** noView

Parameter	Description
	This parameter identifies the MIB tree(s) to which this entry authorizes write access. If the value is noView, then write access will not be granted.
NotifyViewName	**Synopsis:** { noView, V1Mib, allOfMib } **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes access for notifications. If the value is noView, then access for notifications will not be granted.

Section 3.9
RADIUS

RADIUS (Remote Authentication Dial In User Service) is used to provide centralized authentication and authorization for network access. RUGGEDCOM ROS assigns a privilege level of Admin, Operator or Guest to a user who presents a valid user name and password. The number of users who can access the RUGGEDCOM ROS server is ordinarily dependent on the number of user records which can be configured on the server itself. RUGGEDCOM ROS can also, however, be configured to pass along the credentials provided by the user to be remotely authenticated by a RADIUS server. In this way, a single RADIUS server can centrally store user data and provide authentication and authorization service to multiple RUGGEDCOM ROS servers needing to authenticate connection attempts.

Section 3.9.1
RADIUS Overview

RADIUS (described in RFC 2865 [http://tools.ietf.org/html/rfc2865]) is a UDP-based protocol used for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.

A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

Unlike TACACS+, authorization and authentication functionality is supported by RADIUS in the same packet frame. TACACS+ actually separates authentication from authorization into separate packets.

On receiving an authentication-authorization request from a client in an "Access-Request" packet, the RADIUS server checks the conditions configured for received username-password combination in the user database. If all the conditions are met, the list of configuration values for the user is placed into an "Access-Accept" packet. These values include the type of service (e.g. SLIP, PPP, Login User) and all the necessary values to deliver the desired service.

Section 3.9.2
User Login Authentication and Authorization

A RADIUS server can be used to authenticate and authorize access to the device's services, such as HMI via Serial Console, Telnet, SSH, RSH, Web Server (see Password Configuration). RUGGEDCOM ROS implements a RADIUS client which uses the Password Authentication Protocol (PAP) to verify access. Attributes sent to a RADIUS server are:

- user name

- user password
- service type: Login
- vendor specific, currently defined as the following:

  vendor ID: RuggedCom Inc. enterprise number (15004) assigned by the Internet Assigned Numbers Authority (IANA)

  string, sub-attribute containing specific values:

  subtype: 1 (vendor's name subtype)

  length: 11 (total length of sub-attribute of subtype 1)

  ASCII string "RuggedCom"

Two RADIUS servers (Primary and Secondary) are configurable per device. If the Primary Server is not reachable, the device will automatically fall back to the Secondary server to complete the authorization process.

The vendor specific attribute is used to determine the access level from the server, which may be configured at the RADIUS server with the following information:

- Vendor ID: RuggedCom Inc. enterprise number (15004) assigned by Internet Assigned Numbers Authority (IANA)
- Sub-attribute Format: String
- Vendor Assigned Sub-Attribute Number: 2
- Attribute value – any one of: admin, operator, guest

NOTE
If no access level is received in the response packet from the server then no access will be granted to the user

An Example of a RuggedCom Dictionary for a FreeRADIUS server:

VENDOR	RuggedCom 15004
BEGIN-VENDOR	RuggedCom
ATTRIBUTE	RuggedCom-Privilege-level 2 string
END-VENDOR	RuggedCom

Sample entry for user "admin" Adding Users:

admin Auth-Type := Local, User-Password == "admin"

RuggedCom-Privilege-level = "admin"

Section 3.9.3
RADIUS Server Configuration

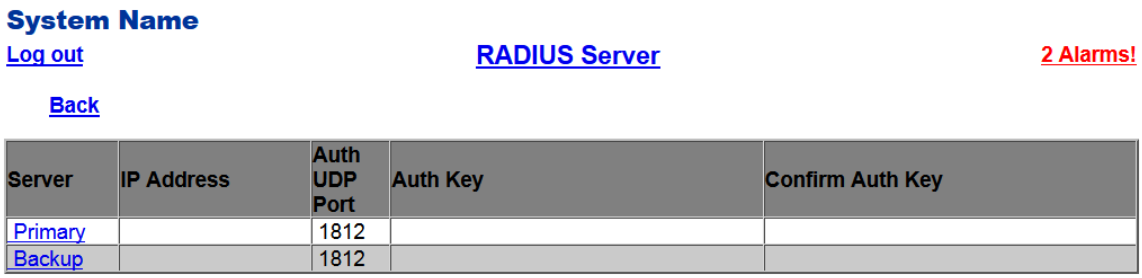


Figure 29: RADIUS Server Summary

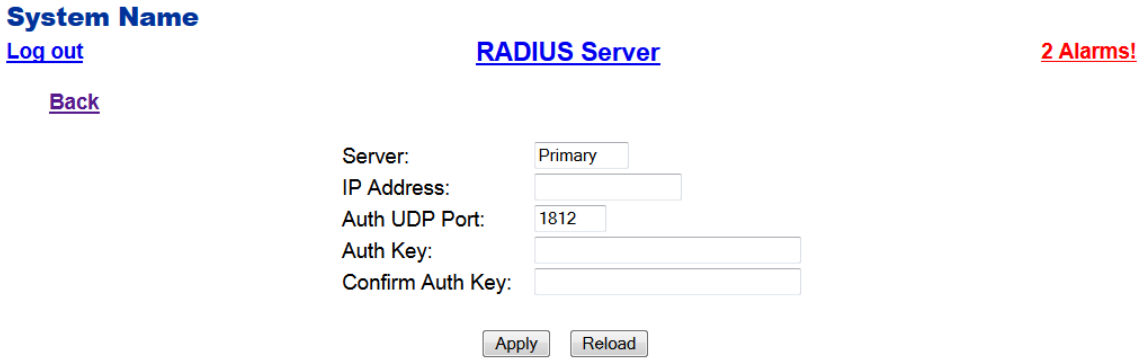


Figure 30: RADIUS Server Form

Parameter	Description
Server	**Synopsis:** Any 8 characters **Default:** Primary This field tells whether this configuration is for a primary or a backup server
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** The RADIUS server IP Address.
Auth UDP Port	**Synopsis:** 1 to 65535 **Default:** 1812 The authentication UDP Port on the RADIUS server.
Auth Key	**Synopsis:** 31 character ASCII string **Default:** None The authentication key shared with the RADIUS server. It is used to encrypt any passwords that are sent between the switch and the RADIUS server.
Confirm Auth Key	**Synopsis:** 31 character ASCII string **Default:** None

Parameter	Description
	Confirm input of the above authentication key.

Section 3.10
TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) is a TCP-based access control protocol that provides authentication, authorization and accounting services to routers, network access servers and other networked computing devices via one or more centralized servers. It is based on, but is not compatible with, the older TACACS protocol. TACACS+ has generally replaced its predecessor in more recently built or updated networks, although TACACS and XTACACS are still used on many older networks. Note that RuggedCom's TACACS+ client implementation always has encryption enabled.

Section 3.10.1
User Login Authentication and Authorization

A TACACS+ server can be used to authenticate and authorize access to the device's services, such as HMI via Serial Console, Telnet, SSH, RSH, Web Server (see Password Configuration). User name and Password are sent to the configured TACACS+ Server.

Two TACACS+ servers (Primary and Secondary) are configurable per device. If the primary server is not reachable, the device will automatically fall back to the secondary server to complete the authorization process.

Section 3.10.2
TACACS+ Server Configuration

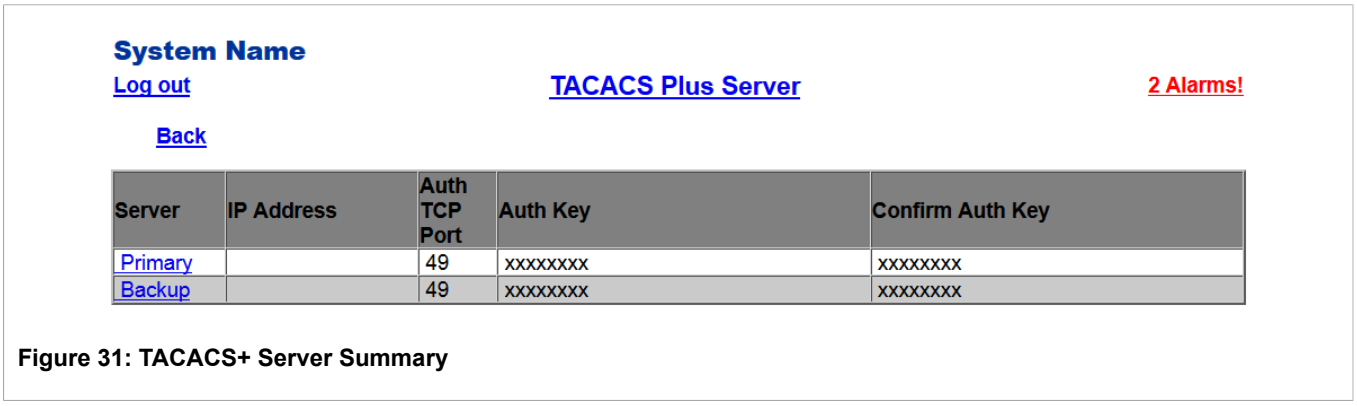


Figure 31: TACACS+ Server Summary

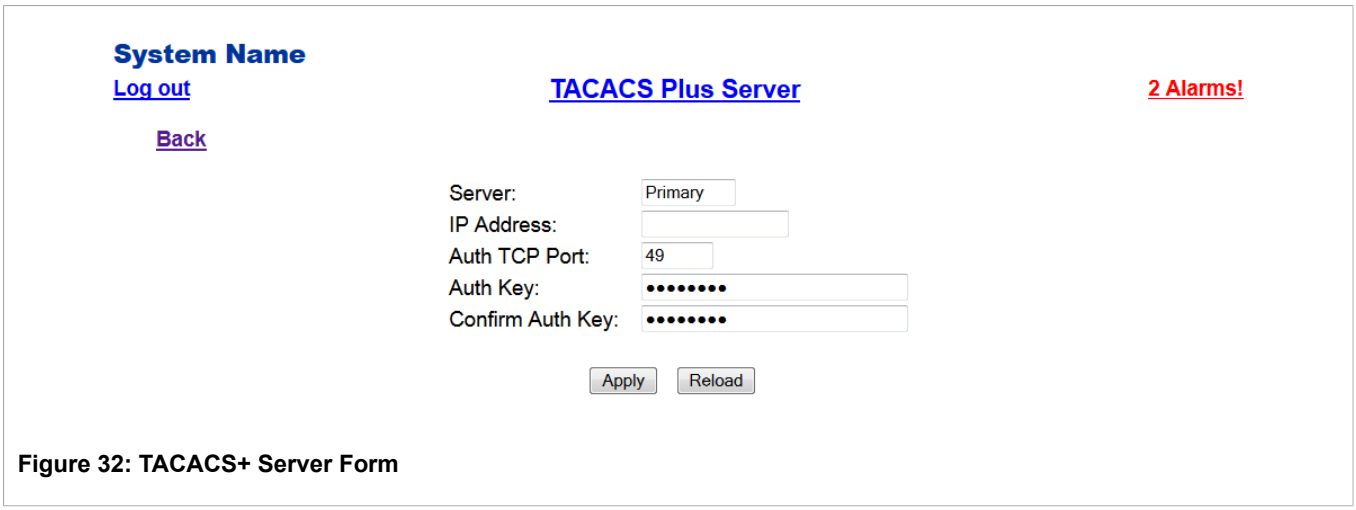


Figure 32: TACACS+ Server Form

Parameter	Description
Server	**Synopsis:** Any 8 characters **Default:** Primary This field indicates whether this configuration is for a primary or a backup server.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** The TACACS+ server IP Address.
Auth TCP Port	**Synopsis:** 1 to 65535 **Default:** 49 The authentication TCP Port on the TACACS+ server.
Auth Key	**Synopsis:** 31 character ASCII string **Default:** The authentication key shared with the TACACS+ server. It is used to encrypt any passwords that are sent from the switch to the TACACS+ server.
Confirm Auth Key	**Synopsis:** 31 character ASCII string **Default:** None Confirm input of the above authentication key.

Section 3.11

Syslog

The syslog provides users with the ability to configure local and remote syslog connections. The remote syslog protocol, defined in RFC 3164, is a UDP/IP-based transport that enables a device to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is simply designed to transport these event messages from the generating device to the collector.

The syslog client resides in RUGGEDCOM ROS and supports up to 5 collectors (syslog servers). RUGGEDCOM ROS Remote Syslog provides the ability to configure:

- IP address(es) of collector(s).
- Source UDP port.

- Destination UDP port per collector.
- Syslog source facility ID per collector (same value for all RUGGEDCOM ROS modules).
- Filtering severity level per collector (in case different collectors are interested in syslog reports with different severity levels).

Configuring syslog is described in the following sections:

- Section 3.11.1, “Configuring Local Syslog”
- Section 3.11.2, “Configuring Remote Syslog Client”
- Section 3.11.3, “Configuring the Remote Syslog Server”

Section 3.11.1

Configuring Local Syslog

The local syslog configuration enables users to control what level of syslog information will be logged. Only messages of a severity level equal to or greater than the configured severity level are written to the syslog.txt file in the unit.

Figure 33: Local Syslog Form

Parameter	Description
Local Syslog Level	**Synopsis:** { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING } **Default:** INFORMATIONAL The severity of the message that has been generated. Note that the severity level selected is considered the minimum severity level for the system. For example, if ERROR is selected, the system sends any syslog messages generated by Error, Critical, Alert and Emergency.

Section 3.11.2
Configuring Remote Syslog Client

Figure 34: Remote Syslog Client Form

Parameter	Description
UDP Port	**Synopsis:** 1025 to 65535 or { 514 } **Default:** 514 The local UDP port through which the client sends information to the server(s).

Section 3.11.3
Configuring the Remote Syslog Server

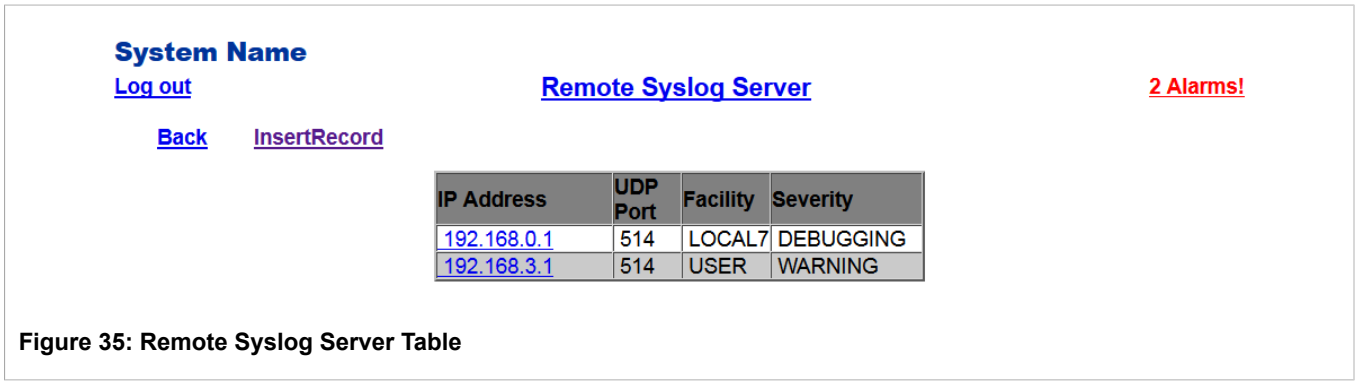


Figure 35: Remote Syslog Server Table

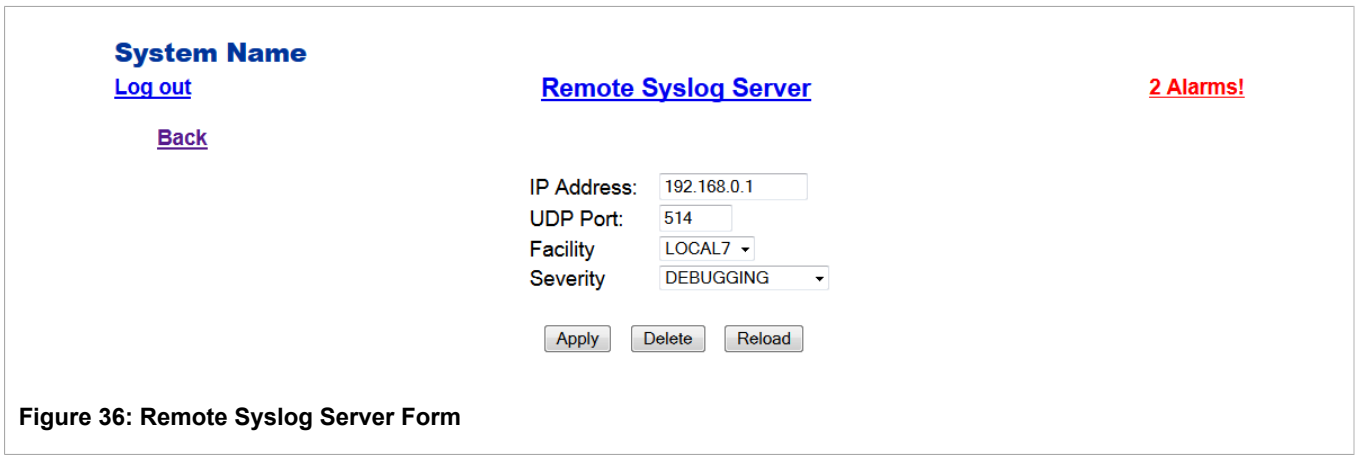


Figure 36: Remote Syslog Server Form

Parameter	Description
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** Syslog server IP Address.
UDP Port	**Synopsis:** 1025 to 65535 or { 514 } **Default:** 514 The UDP port number on which the remote server listens.
Facility	**Synopsis:** { USER, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 } **Default:** LOCAL7 Syslog facility name - { USER, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7 }. Syslog Facility is an information field associated with a syslog message. The syslog facility is the application or operating system component that generates a log message. RUGGEDCOM ROS maps all syslog logging information onto a single facility, which is configurable to facilitate a remote syslog server.
Severity	**Synopsis:** { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING } **Default:** DEBUGGING Syslog severity level - {EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING}. The severity level is the severity of the generated message. Note that the selected severity level is accepted as the minimum severity level for the system. For example, if the severity level is set as "Error", then the system sends any syslog message generated by Error, Critical, Alert and Emergency events.

Section 3.12

Troubleshooting

Problem One

I have configured the IP address and a gateway. I am pinging the switch but it is not responding. I am sure the switch is receiving the ping because its port LEDs are flashing and the statistics menu shows the pings. What is going on?

Is the switch being pinged through a router? If so, the switch gateway address must be configured. The following figure illustrates the problem.

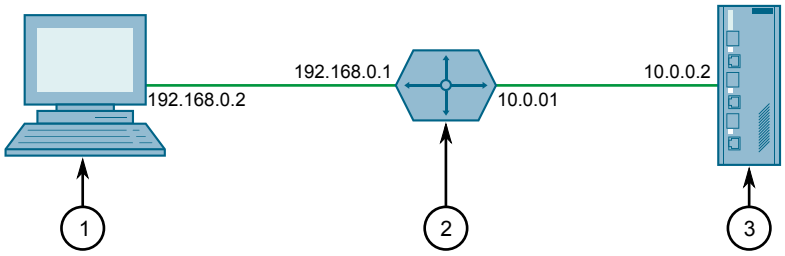


Figure 37: Using A Router As A Gateway

1. Workstation **2.** Router **3.** Switch (RUGGEDCOM RS950G)

The router is configured with the appropriate IP subnets and will forward the ping from the workstation to the switch. When the switch responds, however, it will not know which of its interfaces to use in order to reach the workstation and will drop the response. Programming a gateway of 10.0.0.1 will cause the switch to forward unresolvable frames to the router.

4 Ethernet Ports

RUGGEDCOM ROS Ethernet port control provides the following features:

- Configuring port physical parameters
- Configuring link alarms for the port
- Configuring port rate limiting
- Cable Diagnostics
- Viewing port status
- Resetting all or some ports
- Using Link-Fault-Indication (LFI)

Section 4.1

Ethernet Ports Configuration and Status

The Ethernet Ports menu is accessible from the main menu.

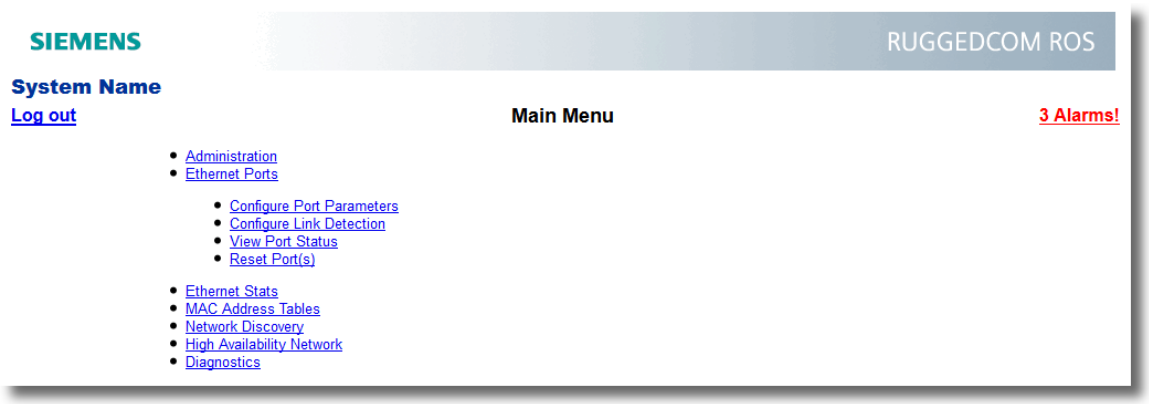
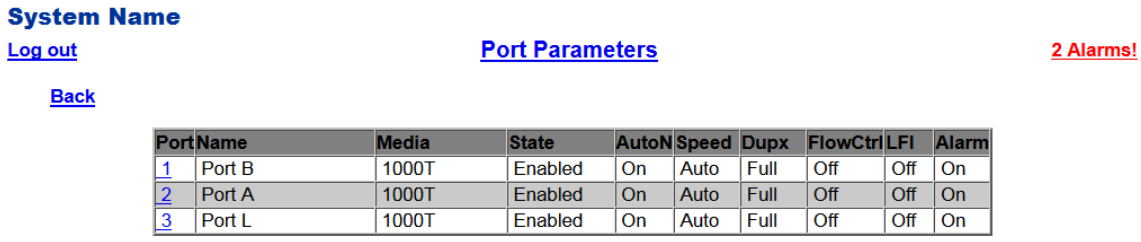


Figure 38: Ethernet Ports Menu

Section 4.1.1
Port Parameters



Port	Name	Media	State	AutoN	Speed	Dupx	FlowCtrl	LFI	Alarm
1	Port B	1000T	Enabled	On	Auto	Full	Off	Off	On
2	Port A	1000T	Enabled	On	Auto	Full	Off	Off	On
3	Port L	1000T	Enabled	On	Auto	Full	Off	Off	On

Figure 39: Port Parameters Table

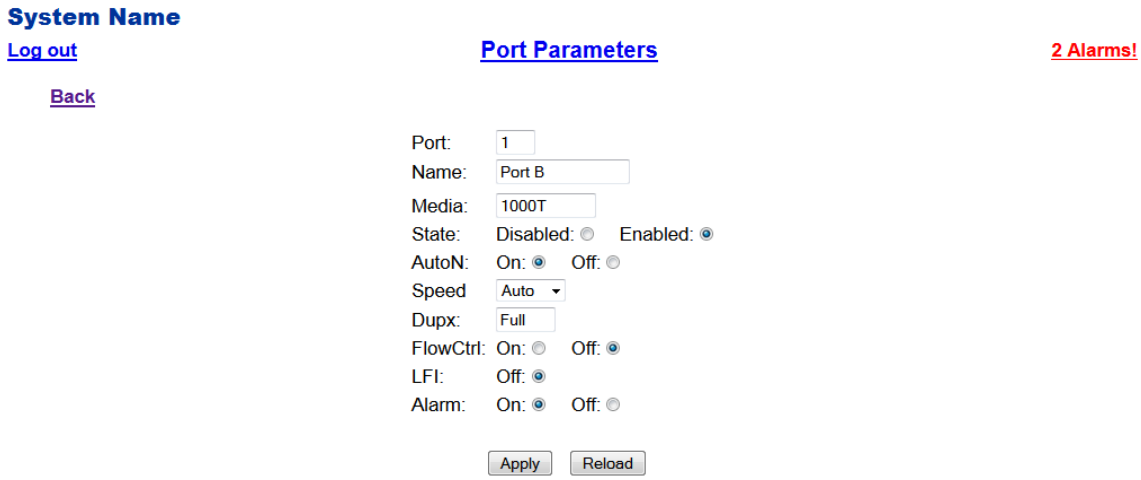


Figure 40: Port Parameters Form

Parameter	Description
Port	Synopsis: 1 to 3 Default: 1 The port number as seen on the front plate silkscreen of the switch.
Name	Synopsis: Any 15 characters Default: Port x A descriptive name that may be used to identify the device connected to that port.
Media	Synopsis: { 100TX, 100FX, 1000X, 1000T } Default: 100TX The type of the port's media.
State	Synopsis: { Disabled, Enabled } Default: Enabled Disabling a port will prevent all frames from being sent and received on that port. Also, when disabled, link integrity pulses are not sent so that the link/activity LED will never be lit. You may want to

Parameter	Description
	disable a port for troubleshooting or to secure it from unauthorized connections.
AutoN	Synopsis: { On, Off } Default: On Enable or disable IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex mode being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results. 100Mbps fiber optic media do not support auto-negotiation so these media must be explicitly configured to full-duplex mode. Full-duplex operation requires both ends to be configured as such or else severe frame loss will occur during heavy network traffic.
Speed	Synopsis: { Auto, 100M, 1G } Default: Auto Speed (in Megabit-per-second or Gigabit-per-second). If auto-negotiation is enabled, this is the speed capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is set to this speed mode. AUTO means advertise all supported speed modes.
Dupx	Synopsis: { Auto, Full } Default: Full Duplex mode. If auto-negotiation is enabled, this is the duplex capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is set to this duplex mode. AUTO means advertise all supported duplex modes.
Flow Control	Synopsis: { Off, On } Default: Off Flow Control is useful for preventing frame loss during times of severe network traffic. Examples of this include multiple source ports sending to a single destination port or a higher-speed port bursting to a lower-speed port. When the port is in half-duplex mode, this is accomplished using 'backpressure' whereby the switch simulates collisions, causing the sending device to retry transmissions according to the Ethernet back-off algorithm. When the port is in full-duplex mode, this is accomplished using PAUSE frames, which cause the sending device to stop transmitting for a certain period of time.
LFI	Synopsis: { Off } Default: Off Enabling Link-Fault-Indication (LFI) inhibits transmission of the link integrity signal when the receiving link has failed. This enables the device at the far end to detect link failure under all circumstances. **NOTE** *This feature must not be enabled at both ends of a link.*
Alarm	Synopsis: { On, Off } Default: On Disabling link state alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that port.

NOTE
If one end of the link is fixed to a specific speed and duplex type and the peer auto-negotiates, there is a strong possibility that the link will either fail to raise, or raise with the wrong settings on the auto-

negotiating side. The auto-negotiating peer will fall back to half-duplex operation, even when the fixed side is full duplex. Full-duplex operation requires that both ends are configured as such or else severe frame loss will occur during heavy network traffic. At lower traffic volumes the link may display few if any errors As the traffic volume rises the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience excessive collisions. Ultimately, as traffic load approaches 100% the link will become entirely unusable. These problems can be avoided by always configuring ports to the appropriate fixed values.

Section 4.1.2
Link Detection Options

Figure 41: Link Detection Form

Parameter	Description
Fast Link Detection	Synopsis: { Off, On, On_withPortGuard } Default: Off This parameter provides system protection against a faulty end device generating an improper link integrity signal. When a faulty end device or a mismatched fiber port is connected to the unit, a large number of continuous link state changes can be reported in a short period of time. This high rate of link state changes can render the system unresponsive. **Three different settings are available for this parameter:** • *ON_withPortGuard* - This is the recommended setting. With this setting, an extended period (> two minutes) of excessive link state changes reported by a port prompts the Port Guard feature to permanently disable Fast Link Detection on the and raises an alarm. By disabling Fast Link Detection on the port, excessive link state changes can no longer consume a substantial amount of system resources. However, note that if Fast Link Detection is disabled, the port will need a longer time to detect a link failure. If the port is part of a spanning tree, this could result in a longer network recovery time, of up to two seconds. After Port Guard disables Fast Link Detection on a particular port, you can re-enable it by clearing the alarm. • *ON* - In special cases where prolonged and frequent link state change constitutes legitimate link operation, this setting prevents the system from disabling Fast Link Detection on the port. If excessive link state changes persist for more than two minutes on a particular port, an alarm is generated to warn about the observed bouncing link. If the condition of excessive link state changes is resolved later on, the alarm is cleared automatically. Because this option does not disable Fast Link Detection, a

Parameter	Description
	persistent bouncing link could affect the response time of the system. This setting should be used with caution. • *OFF* - Turning this parameter OFF completely disables Fast Link Detection. The switch will need a longer time to detect a link failure. This will result in a longer network recovery time of up to two seconds. Only use this option if if fast link failure detection is not needed.
Link Detection Time	Synopsis: 100 ms to 1000 ms Default: 100 ms Determines the time that the link has to continuously stay up before the “link up” decision is made by the device. The device performs Ethernet link detection de-bouncing to avoid multiple responses to an occasional link bouncing event (for example, when a cable makes intermittent contact while being plugged in or unplugged).

NOTE
When Fast Link Detection is enabled, the system prevents link state change processing from consuming all available CPU resources. However, if Port Guard is not used, it is possible for almost all available CPU time to be consumed by frequent link state changes, which could have a negative impact on overall system responsiveness.

Section 4.1.3
Port Status

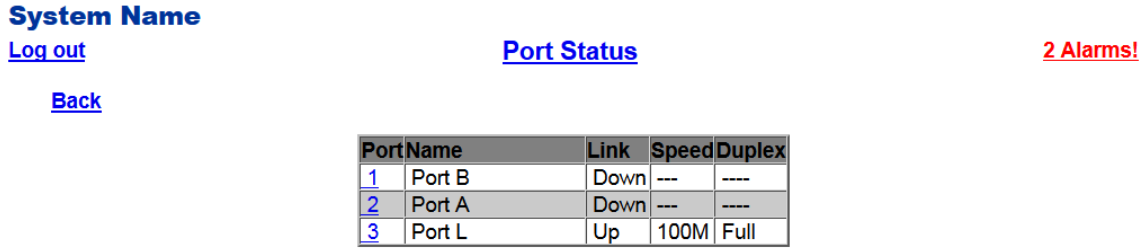


Figure 42: Port Status Table

Parameter	Description
Port	Synopsis: 1 to 3 The port number as seen on the front plate silkscreen of the switch.
Name	Synopsis: Any 15 characters A descriptive name that may be used to identify the device connected to that port.
Link	Synopsis: { ----, ----, Down, Up } The port's link status.
Speed	Synopsis: { ---, 100M, 1G } The port's current speed.
Duplex	Synopsis: { ----, Full }

Parameter	Description
	The port's current duplex status.

Section 4.1.4
Resetting Ports

This command performs a reset of the specified Ethernet ports. This action is useful for forcing re-negotiation of speed and duplex mode or in situations where the link partner has latched into an inappropriate state.

Section 4.2
Troubleshooting

Problem One

One of my links seems to be fine at low traffic levels, but starts to fail as traffic rates increase.

One of my links pings OK but has problems with FTP/SQL/HTTP/…

A possible cause of intermittent operation is that of a ‘duplex mismatch’. If one end of the link is fixed to full-duplex and the peer auto-negotiates, the auto-negotiating end falls back to half-duplex operation. At lower traffic volumes, the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable.

NOTE
The ping command with flood options is a useful tool for testing commissioned links. The command “ping 192.168.0.1 500 2” can be used to issue 500 pings each separated by two milliseconds to the next switch. If the link used is of high quality, then no pings should be lost and the average round trip time should be small.

Problem Two

I am trying to use the LFI protection feature but my links won’t even come up.

Is it possible that the peer also has LFI enabled? If both sides of the link have LFI enabled, then both sides will withhold link signal generation from each other.

5 Ethernet Statistics

RUGGEDCOM ROS Ethernet Statistics provide you with the following abilities:

- Viewing basic Ethernet statistics.
- Viewing and clearing detailed Ethernet statistics.

The Ethernet Statistics menu is accessible from the main menu.

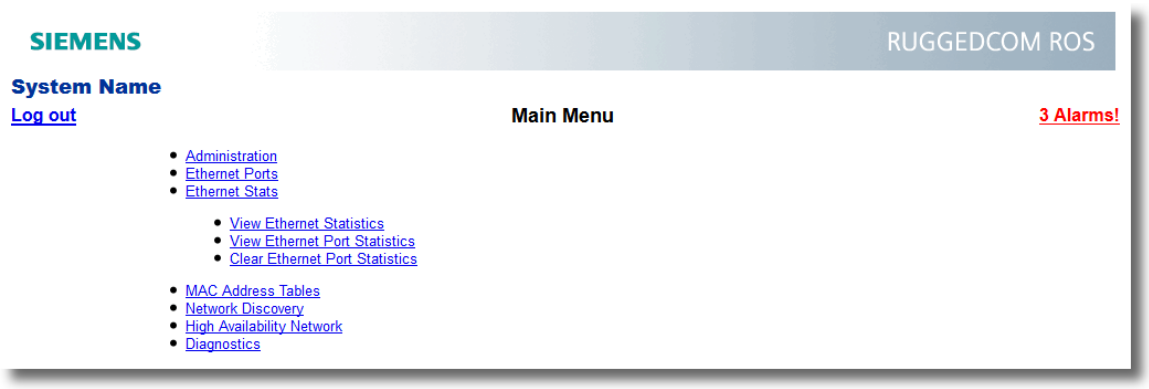
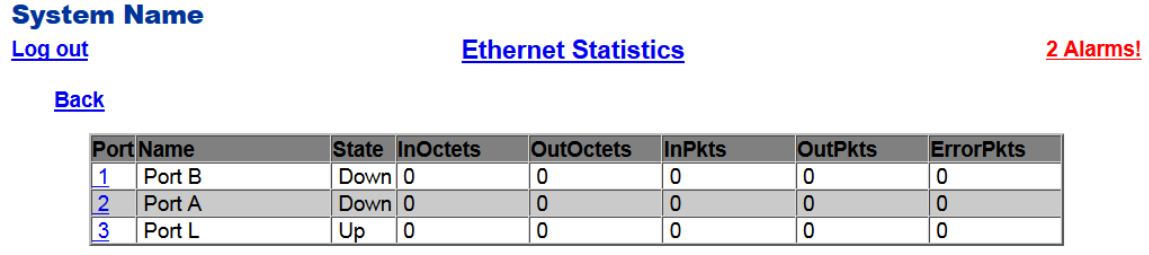


Figure 43: Ethernet Port Statistics Menu

Section 5.1

Viewing Ethernet Statistics

This table provides basic Ethernet statistics information which is reset periodically, every few seconds. This traffic view is useful when the origin and destination of a traffic flow need to be determined.



Port	Name	State	InOctets	OutOctets	InPkts	OutPkts	ErrorPkts
1	Port B	Down	0	0	0	0	0
2	Port A	Down	0	0	0	0	0
3	Port L	Up	0	0	0	0	0

Figure 44: Ethernet Statistics Table

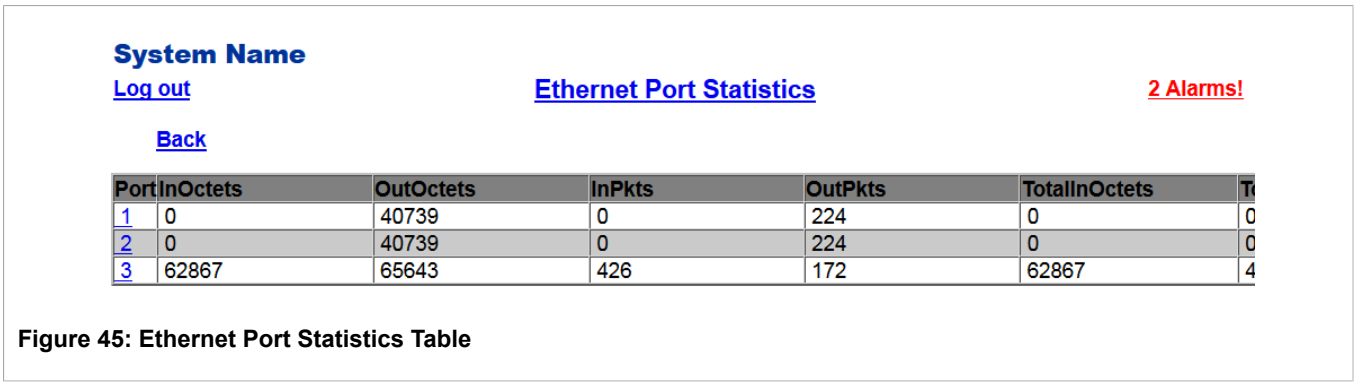
Parameter	Description
Port	Synopsis: 1 to 3 The port number as seen on the front plate silkscreen of the switch.

Parameter	Description
Name	Synopsis: Any 15 characters A descriptive name that may be used to identify the device connected on that port.
State	Synopsis: { ----, ----, Down, Up } The port link status.
InOctets	Synopsis: 0 to 4294967295 The number of octets in received good packets (Unicast+Multicast +Broadcast) and dropped packets.
OutOctets	Synopsis: 0 to 4294967295 The number of octets in transmitted good packets.
InPkts	Synopsis: 0 to 4294967295 The number of received good packets (Unicast+Multicast +Broadcast) and dropped packets.
OutPkts	Synopsis: 0 to 4294967295 The number of transmitted good packets.
ErrorPkts	Synopsis: 0 to 4294967295 The number of any type of erroneous packet.

Section 5.2

Viewing Ethernet Port Statistics

Ethernet port statistics provide a detailed view of the traffic. This is useful when the exact source of error or traffic mix needs to be determined.



Port	InOctets	OutOctets	InPkts	OutPkts	TotalInOctets	T
1	0	40739	0	224	0	0
2	0	40739	0	224	0	0
3	62867	65643	426	172	62867	4

Figure 45: Ethernet Port Statistics Table

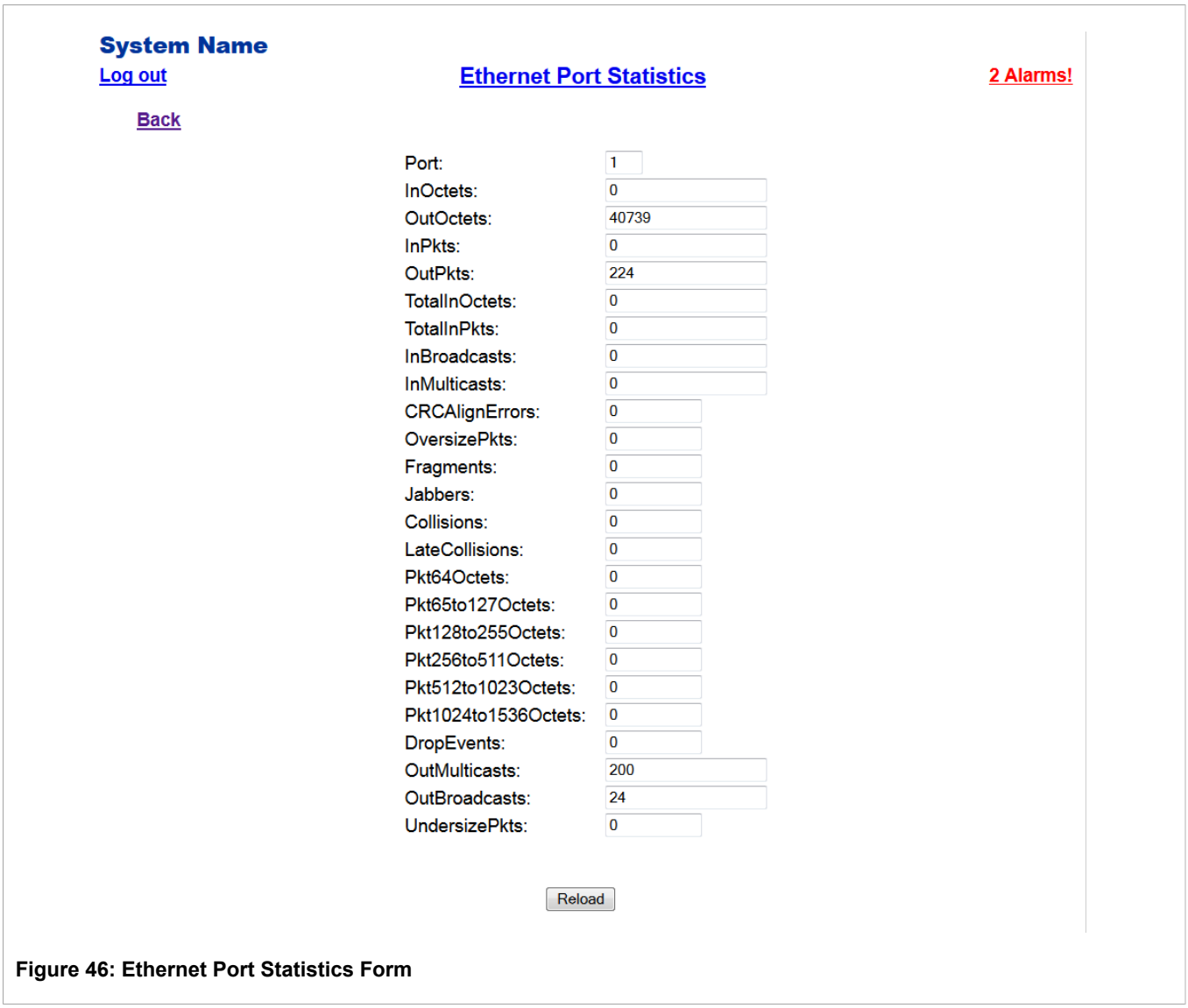


Figure 46: Ethernet Port Statistics Form

Parameter	Description
Port	Synopsis: 1 to 3 The port number as seen on the front plate silkscreen of the switch.
InOctets	Synopsis: 0 to 18446744073709551615 The number of octets in both received packets (Unicast+Multicast +Broadcast) and dropped packets.
OutOctets	Synopsis: 0 to 18446744073709551615 The number of octets in transmitted packets.
InPkts	Synopsis: 0 to 18446744073709551615 The number of received good packets (Unicast+Multicast +Broadcast) and dropped packets.
OutPkts	Synopsis: 0 to 18446744073709551615 The number of transmitted good packets.
TotalInOctets	Synopsis: 0 to 18446744073709551615

Parameter	Description
	The total number of octets of all received packets. This includes data octets of rejected and local packets which are not forwarded to the switching core for transmission. It should reflect all the data octets received on the line.
TotalInPkts	Synopsis: 0 to 18446744073709551615 The number of received packets. This includes rejected, dropped local, and packets which are not forwarded to the switching core for transmission. It should reflect all packets received on the line.
InBroadcasts	Synopsis: 0 to 18446744073709551615 The number of good Broadcast packets received.
InMulticasts	Synopsis: 0 to 18446744073709551615 The number of good Multicast packets received.
CRCAlignErrors	Synopsis: 0 to 4294967295 The number of packets received which meet all the following conditions: 1. Packet data length is between 64 and 1536 octets inclusive. 2. Packet has invalid CRC. 3. Collision Event has not been detected. 4. Late Collision Event has not been detected.
OversizePkts	Synopsis: 0 to 4294967295 The number of packets received with data length greater than 1536 octets and valid CRC.
Fragments	Synopsis: 0 to 4294967295 The number of packets received which meet all the following conditions: 1. Packet data length is less than 64 octets, or packet without SFD and is less than 64 octets in length. 2. Collision Event has not been detected. 3. Late Collision Event has not been detected. 4. Packet has invalid CRC.
Jabbers	Synopsis: 0 to 4294967295 The number of packets which meet all the following conditions: 1. Packet data length is greater that 1536 octets. 2. Packet has invalid CRC.
Collisions	Synopsis: 0 to 4294967295 The number of received packets for which Collision Event has been detected.
LateCollisions	Synopsis: 0 to 4294967295 The number of received packets for which Late Collision Event has been detected.
Pkt64Octets	Synopsis: 0 to 4294967295 The number of received and transmitted packets with size of 64 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkt65to127Octets	Synopsis: 0 to 4294967295 The number of received and transmitted packets with a size of 65 to 127 octets. This includes received and transmitted packets as

Parameter	Description
	well as dropped and local received packets. This does not include rejected received packets.
Pkt128to255Octets	Synopsis: 0 to 4294967295 The number of received and transmitted packets with a size of 128 to 257 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkt256to511Octets	Synopsis: 0 to 4294967295 The number of received and transmitted packets with a size of 256 to 511 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkt512to1023Octets	Synopsis: 0 to 4294967295 The number of received and transmitted packets with a size of 512 to 1023 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkt1024to1536Octets	Synopsis: 0 to 4294967295 The number of received and transmitted packets with a size of 1024 to 1536 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
DropEvents	Synopsis: 0 to 4294967295 The number of received packets that are dropped due to lack of receive buffers.
OutMulticasts	Synopsis: 0 to 18446744073709551615 The number of transmitted multicast packets. This does not include broadcast packets.
OutBroadcasts	Synopsis: 0 to 18446744073709551615 The number of transmitted broadcast packets.
UndersizePkts	Synopsis: 0 to 18446744073709551615 The number of received packets which meet all the following conditions: 1. Packet data length is less than 64 octets. 2. Collision Event has not been detected. 3. Late Collision Event has not been detected. 4. Packet has valid CRC.

Section 5.3
Clearing Ethernet Port Statistics

Figure 47: Clear Ethernet Port Statistics Form

This command clears Ethernet ports statistics for one or more Ethernet ports. Ports are chosen by checking the corresponding boxes.

6 MAC Address Tables

RUGGEDCOM ROS MAC address table management provides you with the following features:

- Configuring static MAC addresses
- Purging MAC Address Entries

The MAC Address Tables menu is accessible from the main menu.

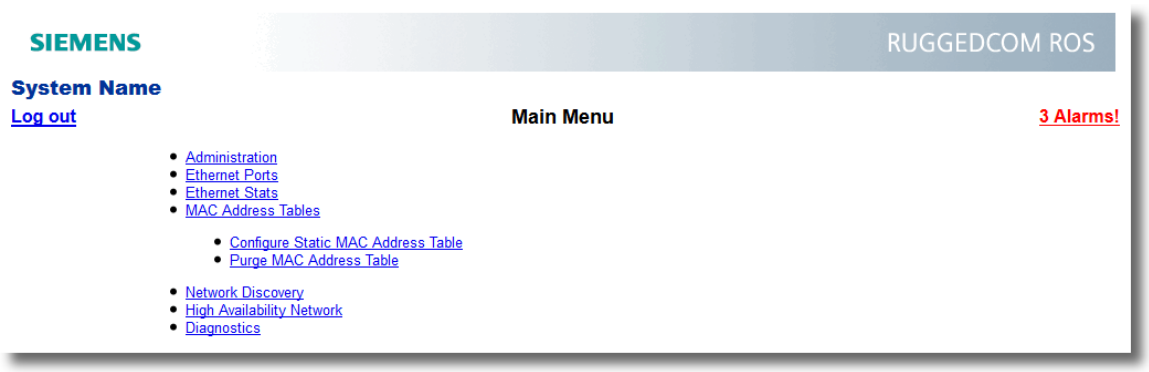


Figure 48: MAC Address Tables Menu

Section 6.1

Configuring Static MAC Address Table

Static MAC addresses are usually configured when the user wishes to enforce port security (if supported).

Static MAC addresses are also configured when a device can receive but cannot transmit frames.

Prioritized MAC addresses are configured when traffic to or from a specific device on a LAN segment is to be assigned a higher CoS priority than other devices on that LAN segment.

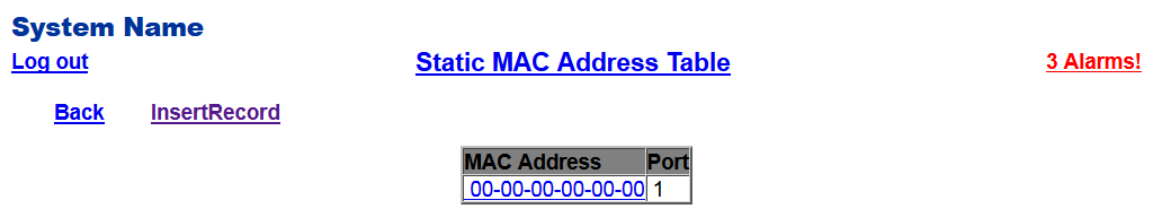


Figure 49: Static MAC Address Table

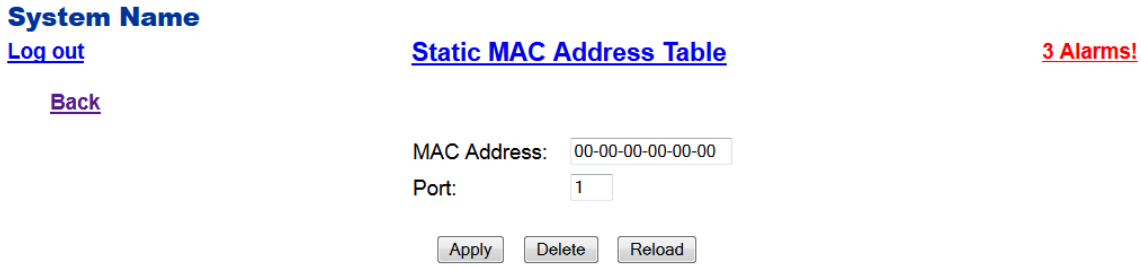


Figure 50: Static MAC Address Form

Parameter	Description
MAC Address	**Synopsis:** ##-##-##-XX-XX-XX, where ## is 0 to FF, XX is 0 to FF or * wildcard **Default:** 00-00-00-00-00-00 A MAC address that is to be statically configured. A maximum of 6 wildcard characters may be used to specify a range of MAC addresses allowed to be learned by the Port Security module (when Port Security is set to 'Static MAC' mode). Wildcards must start from the end of the MAC address and all wildcards must be contiguous. Examples: • 00-0A-DC-**-**-** means the range beginning with 00-0A-DC-00-00-00 and ending with 00-0A-DC-FF-FF-FF. • 00-0A-DC-12-3*-** means the range beginning with 00-0A-DC-12-30-00 and ending with 00-0A-DC-12-3F-FF
Port	Synopsis: 1 to 3 Default: 1 Enter the port number upon which the device with this address is located.

Section 6.2

Purging MAC Address Table

This command removes all dynamic entries from the MAC address table. The only negative impact of this operation is that it causes flooding while addresses are relearned.

7 High Availability Network

Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) are two mechanisms defined by the IEC 62439-3 standard to provide hitless network recovery. Unlike Spanning Tree Protocol (STP), which requires reconfiguration of the active network topology over redundant physical links, HSR and PRP provide hitless network recovery through the use of information replication.

NOTE
The Siemens PRP and HSR implementation is based on IEC 62439-3:2012.

The following sections explain high availability networks in greater details:

- Section 7.1, “Parallel Redundancy Protocol (PRP)”
- Section 7.2, “High-Availability Seamless Redundancy (HSR)”
- Section 7.3, “Configuring the High Availability Network”
- Section 7.4, “Viewing HAN Statistics”

Section 7.1

Parallel Redundancy Protocol (PRP)

Parallel Redundancy Protocol (PRP) provides hitless network recovery by replicating information over two physically independent Ethernet networks.

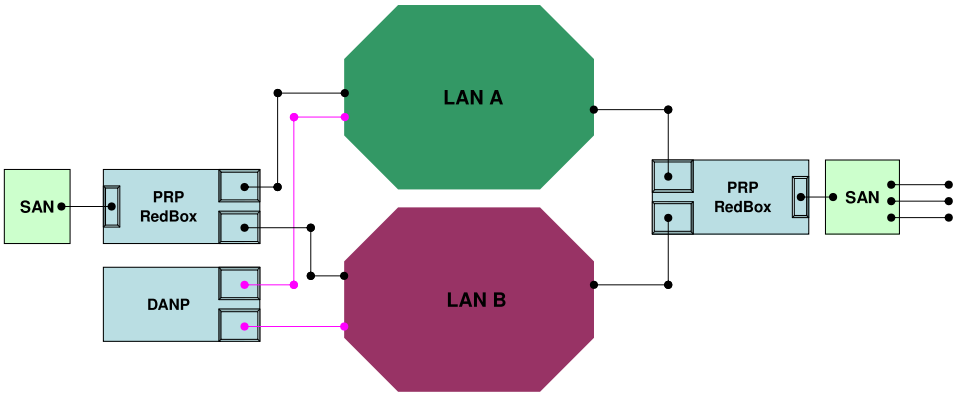


Figure 51: PRP Schematic

Acronyms in Figure 51:

- **DANP:** Doubly Attached Node implementing PRP
- **PRP RedBox:** PRP Redundancy Box
- **SAN:** Singly Attached Node (PRP-unaware)

PRP-aware devices are referred to as Doubly Attached Node implementing PRP (DANP) devices. You can connect legacy devices to a PRP network through a PRP Redundant Box (RedBox) to take advantage of network redundancy.

Periodic PRP supervision frames are sent out by a PRP-aware device to assist network nodes in monitoring network integrity and the presence of nodes. These supervision frames help other nodes to determine which devices are on the network, the type of each device (such as DANP, SANA, SANB), the MAC addresses of each device, and the operating mode.

NOTE
PRP expands the Ethernet frame by 6 octets due to RCT (Redundancy Check Trailer). Generation of PRP supervision frames also consumes bandwidth. As a result the network designer should keep in mind the overhead introduced by the PRP network during network capacity calculations.

IMPORTANT!
When accessing the device through one of the available PRP ports, make sure the client network interface supports jumbo frames (more than 1522 bytes), as PRP expands standard frames by 6 octets.

Section 7.2
High-Availability Seamless Redundancy (HSR)

HSR was officially integrated into the IEC 62439-3 standard in February 2010. A ring network, or a ring of rings, implementing HSR technology, supports zero switchover time in the case of a single link failure. Compared to PRP (Section 7.1, “Parallel Redundancy Protocol (PRP)”), HSR only demands about half of the network infrastructure. However, network bandwidth on an HSR ring is roughly halved compared with a network ring based on RSTP, MRP or DRP technology. All of the network nodes inside an HSR ring must be HSR-capable (i.e. DANH or Doubly-Attached HSR Node). HSR-unaware nodes can be attached to the HSR ring through the use of a *RedBox* (Redundancy Box).

Unlike STP (Spanning Tree Protocol), which requires the reconfiguration of an active network topology over redundant physical links, HHSR provides *hitless* network recovery in a ring topology. In other words, HSR network convergence time from single link failure is zero. The basic principle behind HSR is the replication of frames over both sides of the HSR ring as shown in Figure 52.

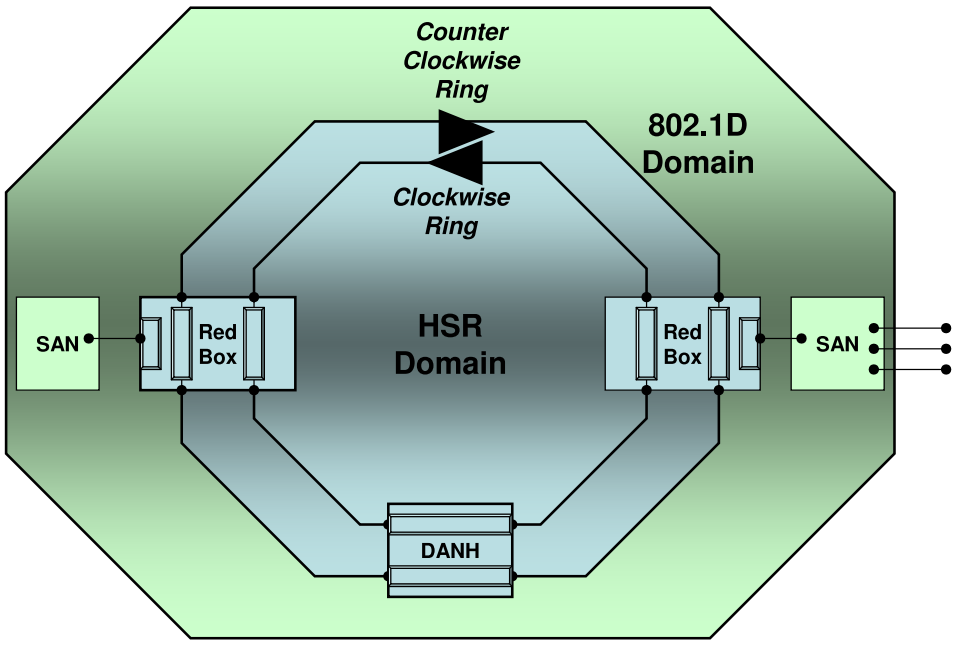


Figure 52: Encapsulation of HSR Ring In IEEE802.1D domain

Nodes within the ring are restricted to be HSR-capable switching nodes. General-purpose nodes (HSR unaware nodes or SAN - Singly Attached Node) cannot be attached directly to the HSR ring, but require a RedBox. A RedBox is a device with at least three ports, two of them being ring ports for the HSR protocol, and the third port being connected to an interlink.

HSR treats two physical Ethernet ports as a single aggregate port. An HSR node uses a single MAC address on both HSR ports. This makes redundancy transparent to layers above MAC. HSR therefore provides Layer 2 redundancy according to the OSI networking model.

The RS950G supports full HSR RedBox functionality as described in IEC62439-3, including generation of HSR supervision frames on behalf of SANs.

When a network link fails inside an HSR ring, one of the two frames sent out from the source DANH will never reach the destination DANH. The destination DANH may report the missing duplicate; but even so, the communication path between the source and destination DANH remains fully operational.

NOTE
Current HSR implementation limits link utilization at 74% when using multicast traffic.

Section 7.3
Configuring the High Availability Network

The High-Availability network menu is accessible from the main menu.

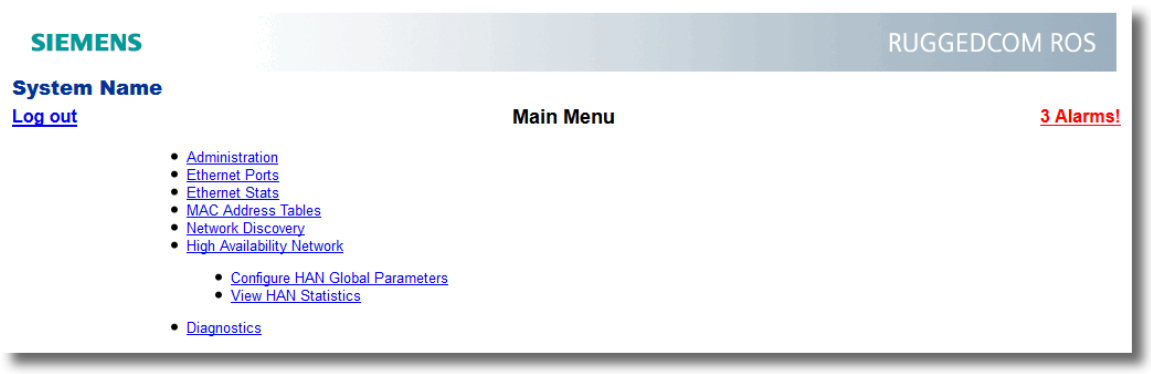


Figure 53: High-Availability Network Menu

Section 7.3.1

Configuring High-Availability Network Global Parameters

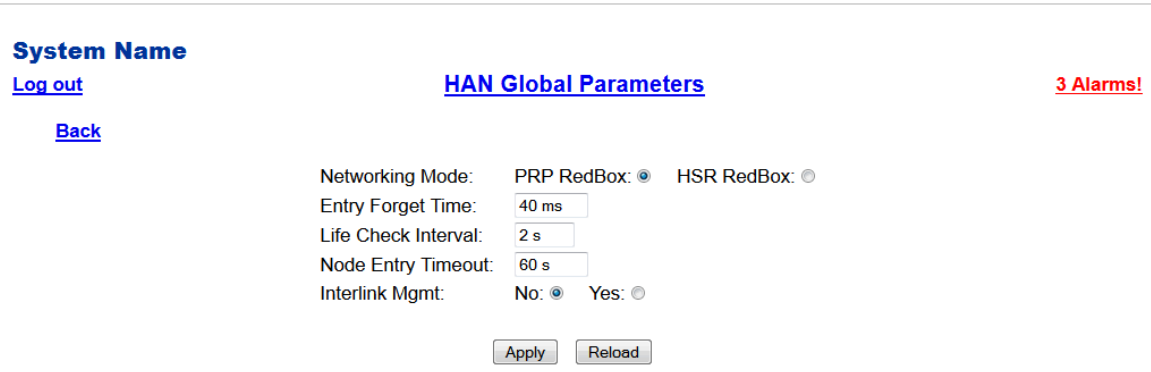


Figure 54: High-Availability Network Global Parameters Menu

Parameter	Description
Networking Mode	**Synopsis:** { PRP RedBox, HSR RedBox } **Default:** PRP RedBox Select the operational mode for a device.
Entry Forget Time	**Synopsis:** { 10 ms to 2560 ms } **Default:** 40 ms Selects timeout value after which a duplicate removal entry is cleared. Please note that the recommended value for a 100 Mbps link is 400 ms.
Life Check Interval	**Synopsis:** 0 s to 300 s **Default:** 2 s Selects how often a RedBox sends a supervision frame.
Node Entry Timeout	Synopsis: 1 s to 86400 s **Default:** 60 s Selects a timeout value after which a node entry is cleared. A timeout of 0 represents a static entry. The node table keeps

Parameter	Description
	track of peer PRP nodes. The key attribute of the Nodes table is MacAddressA (the MAC address of the source node) as received in the PRP supervision frame sent by a PRP node.
Interlink Mgmt	**Synopsis:** { No, Yes } **Default:** No This parameter allows user to manage the interlink port based on the status of PRP/HSR ports. If both PRP/HSR ports are down then system will disable the interlink port.

Section 7.4

Viewing HAN Statistics

From the View HAN Statistics menu, you can view the following High Availability Network statistics.

Figure 55: View HAN Statistics Menu

Section 7.4.1

Viewing the CPU Table

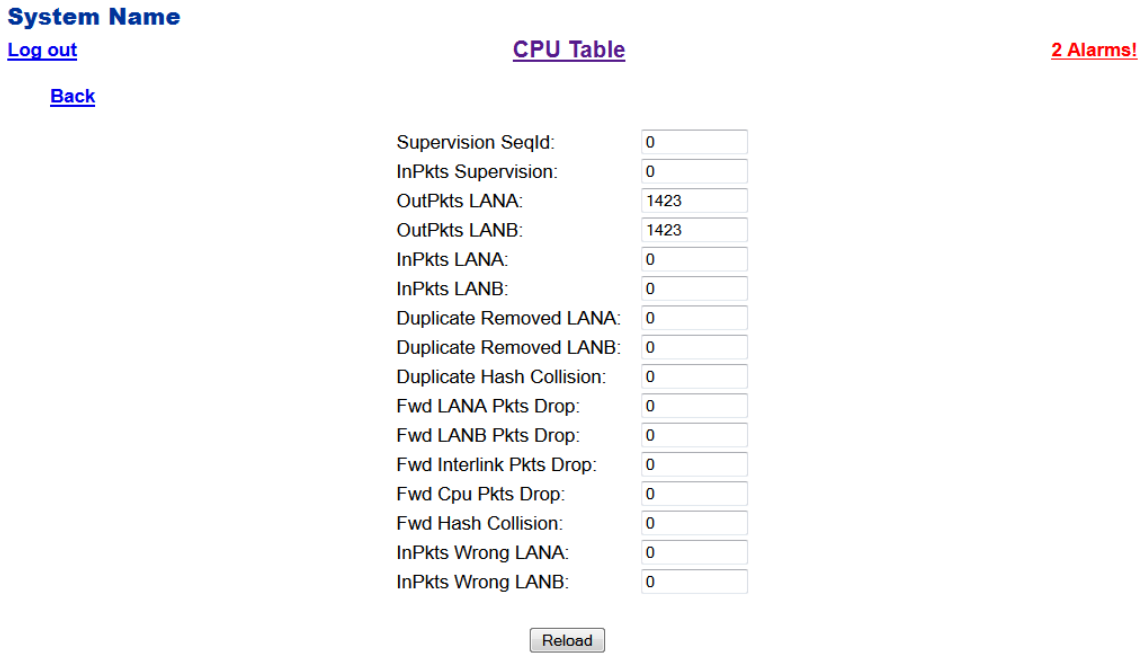


Figure 56: HAN Statistics CPU Table

The CPU Table displays the following CPU information:

Parameter	Description
Supervision SeqId	**Synopsis:** { 0 to 4294967295 } The sequence number of the supervision frame. The supervision frame allows the user to check the integrity of the network and the presence of the DANP nodes.
InPkts Supervision	**Synopsis:** { 0 to 4294967295 } Represents the number of supervision frames received.
OutPkts LANA	**Synopsis:** 0 to 4294967295 LANA ingress frame count.
OutPkts LANB	**Synopsis:** 0 to 4294967295 LANB ingress frame count.
InPkts LANA	**Synopsis:** 0 to 4294967295 LANA ingress frame count.
InPkts LANB	**Synopsis:** 0 to 4294967295 LANB ingress frame count.
Duplicate Removed LANA	**Synopsis:** { 0 to 4294967295 } Represents the number of duplicate frames detected and removed.
Duplicate Removed LANB	**Synopsis:** { 0 to 4294967295 }

Parameter	Description
	Represents the number of duplicate frames detected and removed.
Duplicate Hash Collision	**Synopsis:** { 0 to 4294967295 } Represents the number of hash collisions in duplicate removal logic.
Fwd LANA Pkts Drop	**Synopsis:** { 0 to 4294967295 } Forwarding engine LANA frame drop count.
Fwd LANB Pkts Drop	**Synopsis:** { 0 to 4294967295 } Forwarding engine LANB frame drop count.
Fwd Interlink Pkts Drop	**Synopsis:** { 0 to 4294967295 } Forwarding engine interlink frame drop count
Fwd Cpu Pkts Drop	**Synopsis:** { 0 to 4294967295 } Forwarding engine CPU frame drop count.
Fwd Hash Collision	**Synopsis:** { 0 to 4294967295 } Forwarding engine hash collision count.
InPkts Wrong LANA	**Synopsis:** { 0 to 4294967295 } The error counter CntErrWrongLanA represents a possible configuration error (LanA and LanB are cross-connected).
InPkts Wrong LANB	**Synopsis:** { 0 to 4294967295 } The error counter CntErrWrongLanB represents a possible configuration error (LanA and LanB are cross-connected).

Section 7.4.2
Viewing the VDAN Table

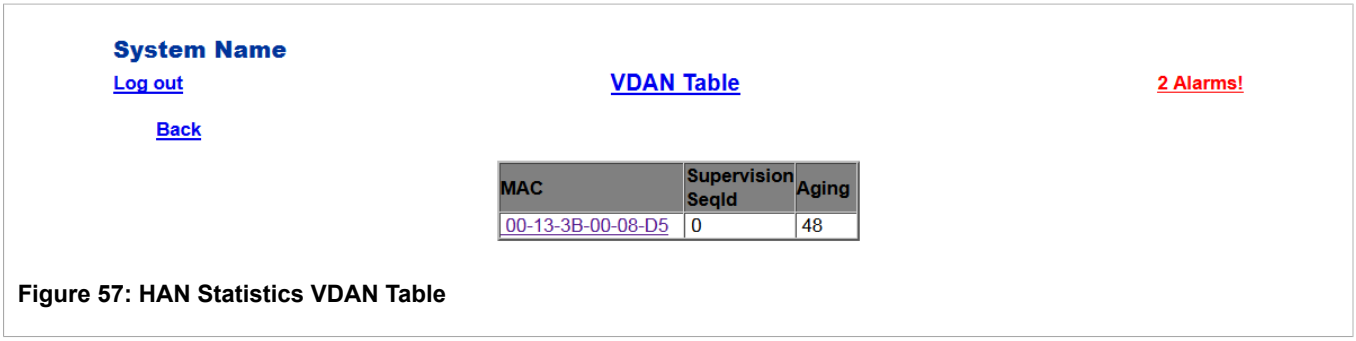


Figure 57: HAN Statistics VDAN Table

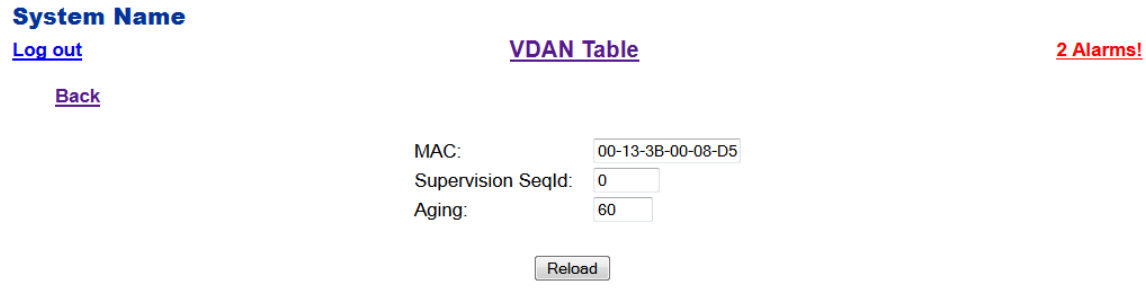


Figure 58: HAN Statistics VDAN Form

The VDAN Table displays the following VDAN (Virtual Doubly Attached Node) information:

Parameter	Description
MAC	**Synopsis:** ##-##-##-##-##-## where ## ranges from 0 to FF MAC address of a source node.
Supervision SeqId	**Synopsis:** 0 to 65535 The sequence number of the supervision frame. The supervision frame allows the user to check the integrity of the network and the presence of the DANP nodes.
Aging	**Synopsis:** 0 to 4096 Node ForgetTime in seconds.

Section 7.4.3
Viewing the Node Table

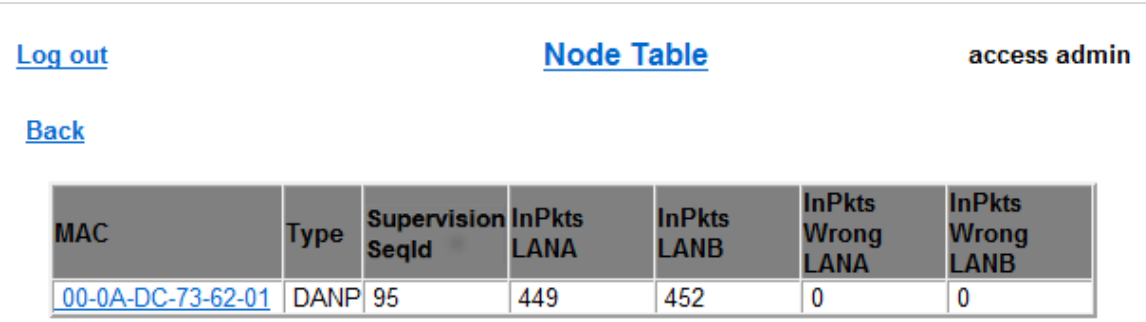


Figure 59: HAN Statistics Node Table

The Node Table displays the following Node information.

Parameter	Description
MAC	**Synopsis:** ##-##-##-##-##-## where ## ranges from 0 to FF MAC address of a source node. For more information on a node, click on its MAC address; see Figure 60.

Parameter	Description
Type	**Synopsis:** { SAN | DANP } Represents SAN (Singly Attached Node) or DANP (Double attached node implementing PRP).
Supervision SeqId	**Synopsis:** { 0 to 65535 } Represents the number of supervision frames received.
InPkts LANA	**Synopsis:** 0 to 4294967295 LANA ingress frame count.
InPkts LANB	**Synopsis:** 0 to 4294967295 LANB ingress frame count.
InPkts Wrong LANA	**Synopsis:** 0 to 4294967295 The error counter CntErrWrongLanA represents a possible configuration error (LanA and LanB are cross-connected).
InPkts Wrong LANB	**Synopsis:** 0 to 4294967295 The error counter CntErrWrongLanB represents a possible configuration error (LanA and LanB are cross-connected).

For more information about a specific node, click on its MAC address. The following information appears:

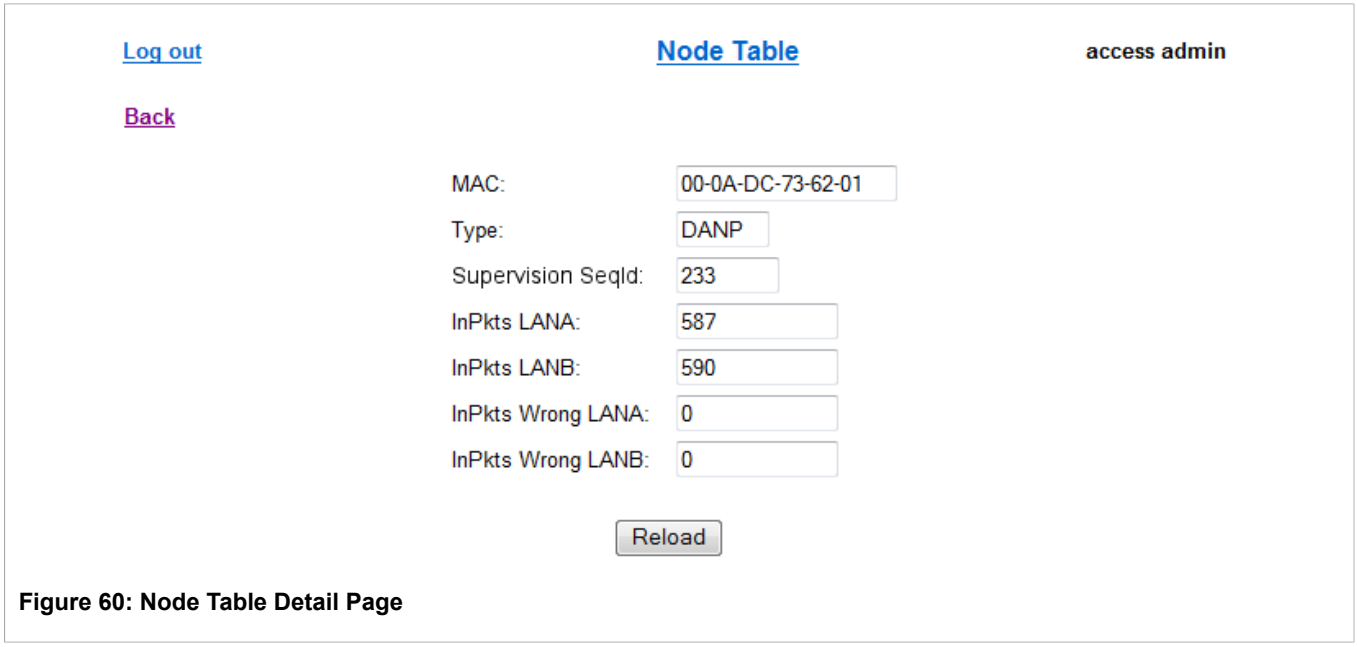


Figure 60: Node Table Detail Page

8 Network Discovery

RUGGEDCOM ROS supports the Link Layer Discovery Protocol (LLDP). LLDP is an IEEE standard protocol, IEEE 802.11AB, that allows a networked device to advertise its own basic networking capabilities and configuration.

LLDP allows a networked device to discover its neighbors across connected network links using a standard mechanism. Devices that support LLDP are able to advertise information about themselves, including their capabilities, configuration, interconnections, and identifying information.

LLDP agent operation is typically implemented as two modules: the LLDP transmit module and LLDP receive module. The LLDP transmit module, when enabled, sends the local device's information at regular intervals, in IEEE 802.1AB standard format. Whenever the transmit module is disabled, it transmits an LLDPDU (LLDP data unit) with a time-to-live (TTL) type-length-value (TLV) containing 0 in the information field. This enables remote devices to remove the information associated with the local device in their databases. The LLDP receive module, when enabled, receives a remote devices' information and updates its LLDP database of remote systems. When new or updated information is received, the receive module initiates a timer for the valid duration indicated by the TTL TLV in the received LLDPDU. A remote system's information is removed from the database when an LLDPDU is received from it with TTL TLV containing 0 in its information field.

NOTE
LLDP is implemented to keep a record of only one device per Ethernet port. Therefore, if there are multiple devices sending LLDP information to a switch port on which LLDP is enabled, information about the neighbor on that port will change constantly.

The following sections describe how to configure and manage network discovery:

Section 8.1

Configuring LLDP Globally

To configure the global settings for LLDP, do the following:

1. Navigate to ***Network Discovery » Link Layer Discovery Protocol » Configure Global LLDP Parameters***. The **Global LLDP Parameters** form appears.

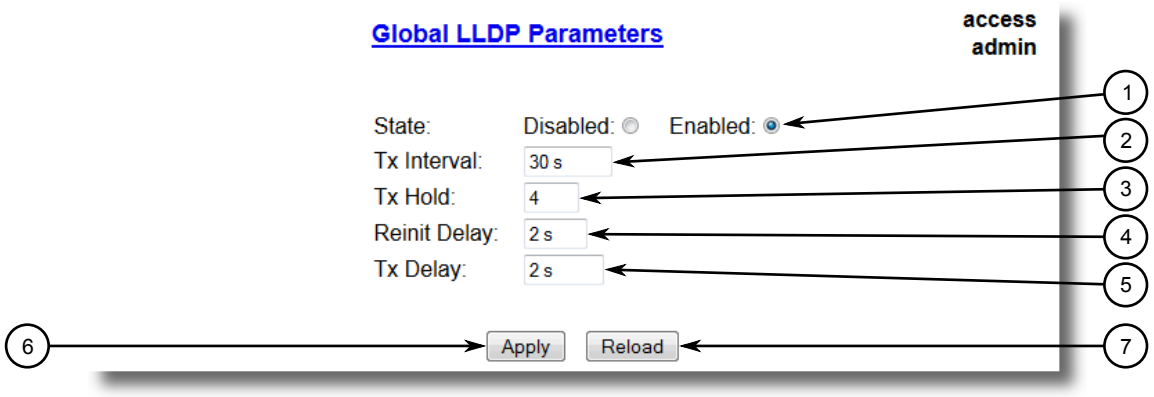


Figure 61: Global LLDP Parameters Form

1. State Options **2.** Tx Interval Box **3.** Tx Hold Box **4.** Reinit Delay Box **5.** Tx Delay Box **6.** Apply Button **7.** Reload Button

2. Configure the following parameter(s) as required:

Parameter	Description
State	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables LLDP protocol. Note that LLDP is enabled on a port when LLDP is enabled globally and along with enabling per port setting in Port LLDP Parameters menu.
Tx Interval	**Synopsis:** 5 to 32768 s **Default:** 30 s The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
Tx Hold	**Synopsis:** 2 to 10 **Default:** 4 The multiplier of the Tx Interval parameter that determines the actual time-to-live (TTL) value used in a LLDPDU. The actual TTL value can be expressed by the following formula: `TTL = MIN(65535, (Tx Interval * Tx Hold))`
Reinit Delay	**Synopsis:** 1 to 10 s **Default:** 2 s The delay in seconds from when the value of Admin Status parameter of a particular port becomes 'Disabled' until re-initialization will be attempted.
Tx Delay	**Synopsis:** 1 to 8192 s **Default:** 2 s The delay in seconds between successive LLDP frame transmissions initiated by value or status changed. The recommended value is set by the following formula: `1 <= txDelay <= (0.25 * Tx Interval)`

3. Click **Apply**.

Section 8.2

Configuring LLDP for an Ethernet Port

To configure LLDP for a specific Ethernet Port, do the following:

1. Navigate to ***Network Discovery » Link Layer Discovery Protocol » Configure Port LLDP Parameters***. The **Port LLDP Parameters** table appears.

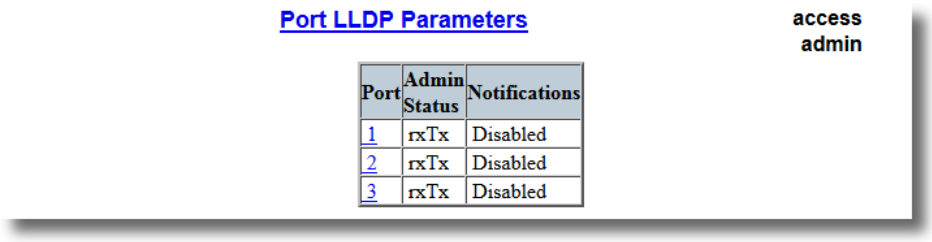


Figure 62: Port LLDP Parameters Table

2. Select a port. The **Port LLDP Parameters** form appears.

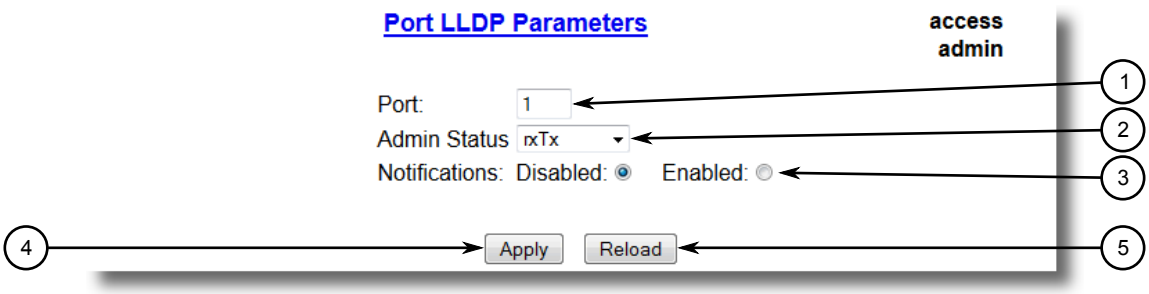


Figure 63: Port LLDP Parameters Form

1. Port Box **2.** Admin Status List **3.** Notifications Options **4.** Apply Button **5.** Reload Button

3. Configure the following parameter(s) as required:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Admin Status	**Synopsis:** { rxTx, txOnly, rxOnly, Disabled } **Default:** rxTx rxTx: the local LLDP agent can both transmit and receive LLDP frames through the port. txOnly: the local LLDP agent can only transmit LLDP frames. rxOnly: the local LLDP agent can only receive LLDP frames. disabled: the local LLDP agent can neither transmit or receive LLDP frames.

Parameter	Description
Notifications	**Synopsis:** { Disabled, Enabled } **Default:** Disabled Disabling notifications will prevent sending notifications and generating alarms for particular port from the LLDP agent.

4. Click **Apply**.

Section 8.3

Viewing Global Statistics and Advertised System Information

To view global statistics for LLDP and the system information that is advertised to neighbors, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Global Remote Statistics***. The **LLDP Global Remote Statistics** form appears.

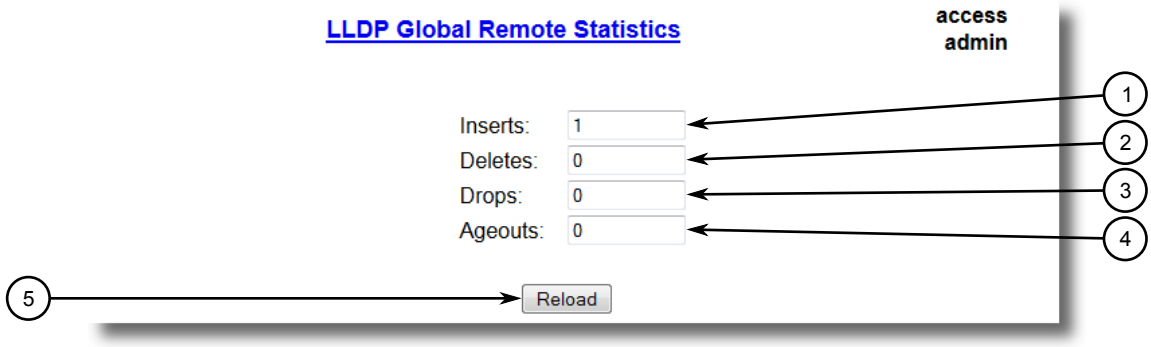


Figure 64: LLDP Global Remote Statistics Form

1. Inserts Box **2.** Deletes Box **3.** Drops Box **4.** Ageouts Box **5.** Reload Button

This form displays the following information:

Parameter	Description
Inserts	**Synopsis:** 0 to 4294967295 A number of times the entry in LLDP Neighbor Information Table was inserted.
Deletes	**Synopsis:** 0 to 4294967295 A number of times the entry in LLDP Neighbor Information Table was deleted.
Drops	**Synopsis:** 0 to 4294967295 A number of times an entry was deleted from LLDP Neighbor Information Table because the information timeliness interval has expired.
Ageouts	**Synopsis:** 0 to 4294967295

Parameter	Description
	A counter of all TLVs discarded.

Section 8.4

Viewing Statistics for LLDP Neighbors

To view statistics for LLDP neighbors, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Neighbor Information***. The **LLDP Neighbor Information** table appears.

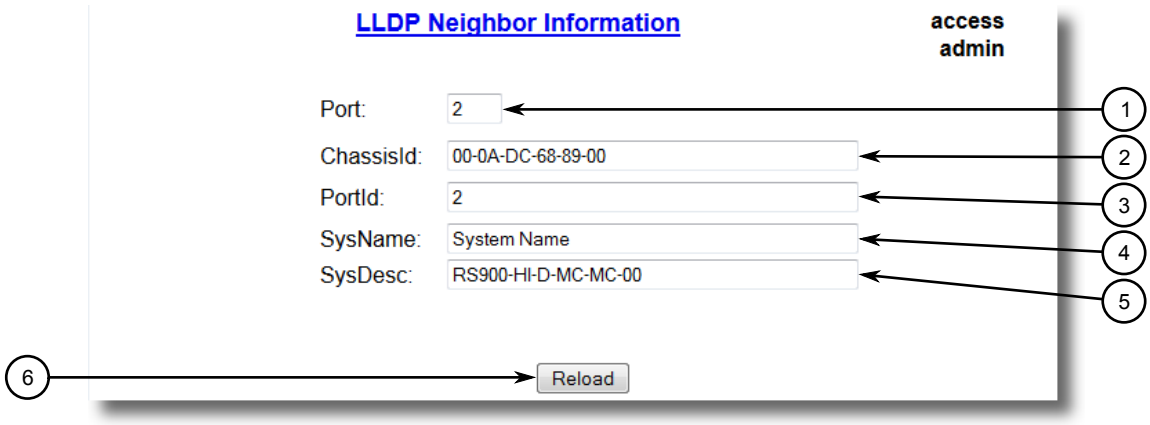


Figure 65: LLDP Neighbor Information Table

1. Port Box **2.** ChassisId Box **3.** PortId Box **4.** SysName Box **5.** SysDesc Box **6.** Reload Button

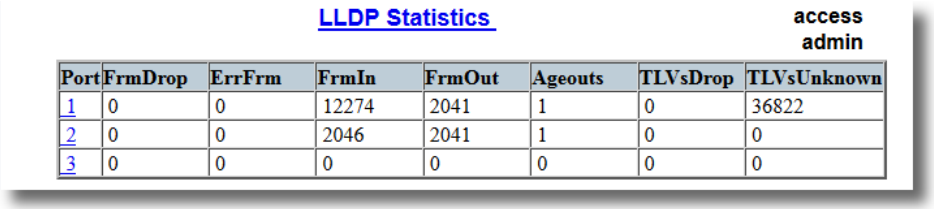
This form displays the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number The local port associated with this entry.
ChassisId	**Synopsis:** Any 45 characters Chassis Id information received from remote LLDP agent.
PortId	**Synopsis:** Any 45 characters Port Id information received from remote LLDP agent.
SysName	**Synopsis:** Any 45 characters System Name information received from remote LLDP agent.
SysDesc	**Synopsis:** Any 45 characters System Descriptor information received from remote LLDP agent.

Section 8.5

Viewing Statistics for LLDP Ports

To view statistics for LLDP ports, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Statistics***. The **LLDP Statistics** table appears.



LLDP Statistics

access
admin

Port	FrmDrop	ErrFrm	FrmIn	FrmOut	Ageouts	TLVsDrop	TLVsUnknown
1	0	0	12274	2041	1	0	36822
2	0	0	2046	2041	1	0	0
3	0	0	0	0	0	0	0

Figure 66: LLDP Statistics Table

This table displays the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
FrmDrop	**Synopsis:** 0 to 4294967295 A counter of all LLDP frames discarded.
ErrFrm	**Synopsis:** 0 to 4294967295 A counter of all LLDPDUs received with detectable errors.
FrmIn	**Synopsis:** 0 to 4294967295 A counter of all LLDPDUs received.
FrmOut	**Synopsis:** 0 to 4294967295 A counter of all LLDPDUs transmitted.
Ageouts	**Synopsis:** 0 to 4294967295 A counter of the times that a neighbor's information has been deleted from the LLDP remote system MIB because the txinfoTTL timer has expired.
TLVsDrop	**Synopsis:** 0 to 4294967295 A counter of all TLVs discarded.
TLVsUnknown	**Synopsis:** 0 to 4294967295 A counter of all TLVs received on the port that are not recognized by the LLDP local agent.

9 Diagnostics

RUGGEDCOM ROS provides the following diagnostics features:

- Alarm System to view and clear alarms
- Viewing and clearing the system log
- Viewing CPU diagnostics
- Viewing the product information
- Loading the factory default configuration
- Resetting the device
- Transferring Files

The Diagnostics menu is accessible from the main menu:

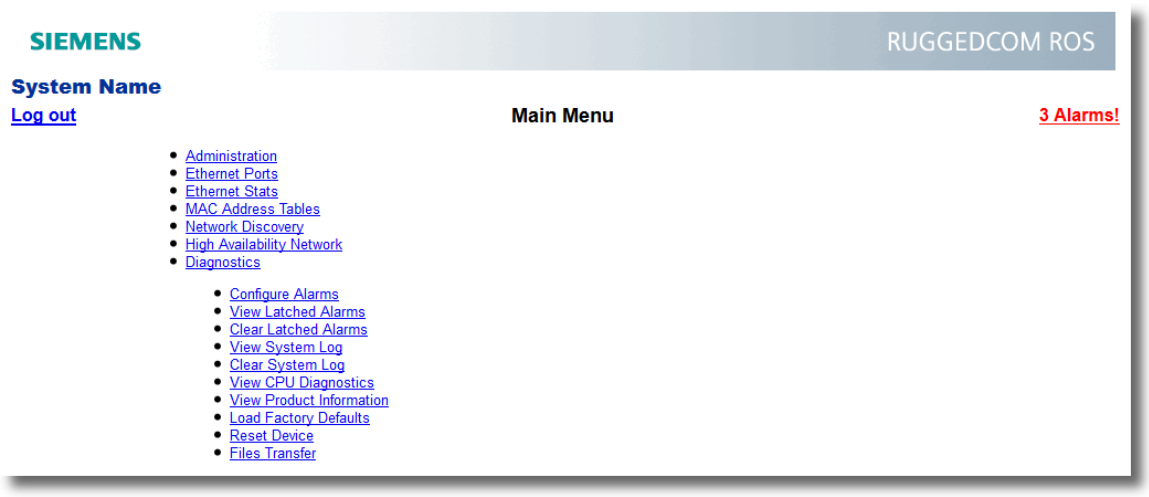


Figure 67: Diagnostics Menu

Section 9.1

Using the Alarm System

Alarms are the occurrence of events of interest that are logged by the device. If alarms have occurred, the device will indicate the number of alarms in the top right corner of all menu screens.

There are two broad types of alarms - active and passive alarms.

Section 9.1.1
Active Alarms

Active alarms are ongoing. They signify states of operation that are not in accordance with normal operation. Examples of active alarms include links that should be up but are not or error rates that are continuously exceeding a certain threshold.

Active alarms are removed (cleared) either by solving the original cause of the alarm or by explicitly clearing the alarm itself.

Section 9.1.2
Passive Alarms

Passive alarms are historic in nature. They signify events that represented abnormal conditions in the past, and do not affect the current operational status. Examples of passive alarms include authentication failures or error rates that temporarily exceeded a certain threshold.

Passive alarms are cleared through the Clear Alarms option under the diagnostics menu.

Section 9.1.3
Alarms and the Critical Failure Relay

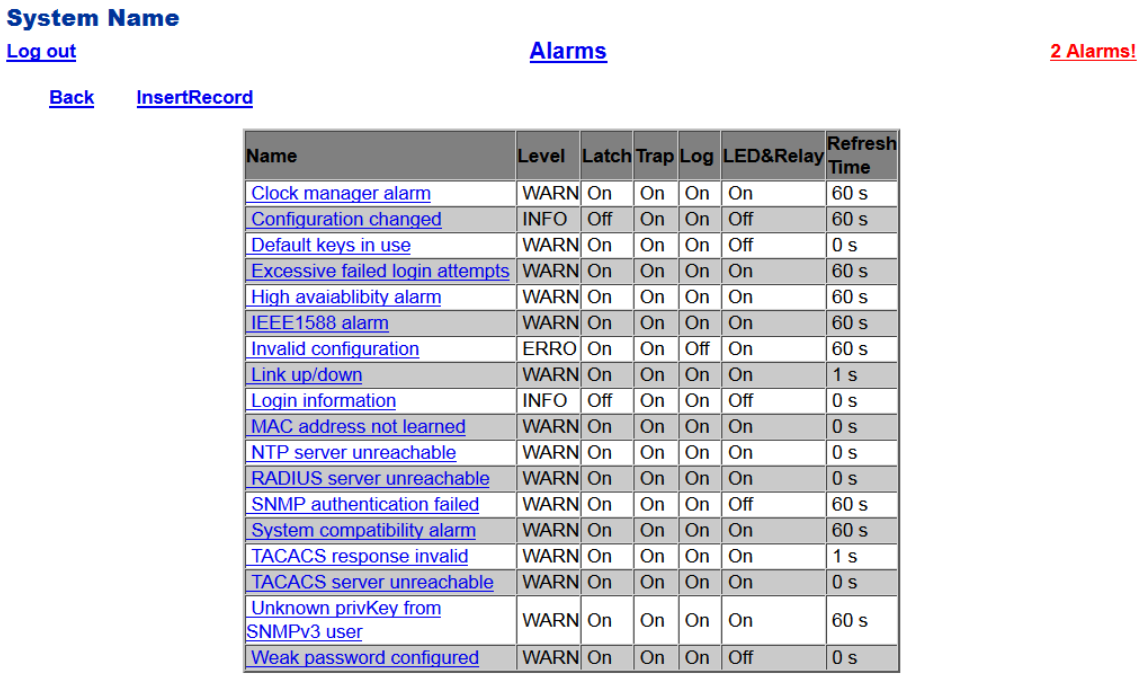
All active alarms will immediately de-energize the critical fail relay (thus signifying a problem). The relay will be re-energized when the last outstanding active alarm is cleared.

NOTE
Alarms are volatile in nature. All alarms (active and passive) are cleared at startup.

Section 9.1.4
Configuring Alarms

RUGGEDCOM ROS provides a means for selectively configuring alarms in fine-grained detail. Some notes on alarm configuration in RUGGEDCOM ROS:

- Alarms at levels CRITICAL or ALERT are not configurable nor can they be disabled.
- The "Level" field is read-only; the pre-configured alarm level is not a configurable option.
- Alarms cannot be added to or deleted from the system.
- Alarm configuration settings changed by a user will be saved in the configuration file.
- The "alarms" CLI command lists all alarms - configurable and non-configurable.



Name	Level	Latch	Trap	Log	LED&Relay	Refresh Time
Clock manager alarm	WARN	On	On	On	On	60 s
Configuration changed	INFO	Off	On	On	Off	60 s
Default keys in use	WARN	On	On	On	Off	0 s
Excessive failed login attempts	WARN	On	On	On	On	60 s
High avaiablibity alarm	WARN	On	On	On	On	60 s
IEEE1588 alarm	WARN	On	On	On	On	60 s
Invalid configuration	ERRO	On	On	Off	On	60 s
Link up/down	WARN	On	On	On	On	1 s
Login information	INFO	Off	On	On	Off	0 s
MAC address not learned	WARN	On	On	On	On	0 s
NTP server unreachable	WARN	On	On	On	On	0 s
RADIUS server unreachable	WARN	On	On	On	On	0 s
SNMP authentication failed	WARN	On	On	On	Off	60 s
System compatibility alarm	WARN	On	On	On	On	60 s
TACACS response invalid	WARN	On	On	On	On	1 s
TACACS server unreachable	WARN	On	On	On	On	0 s
Unknown privKey from SNMPv3 user	WARN	On	On	On	On	60 s
Weak password configured	WARN	On	On	On	Off	0 s

Figure 68: Alarm Configuration Table

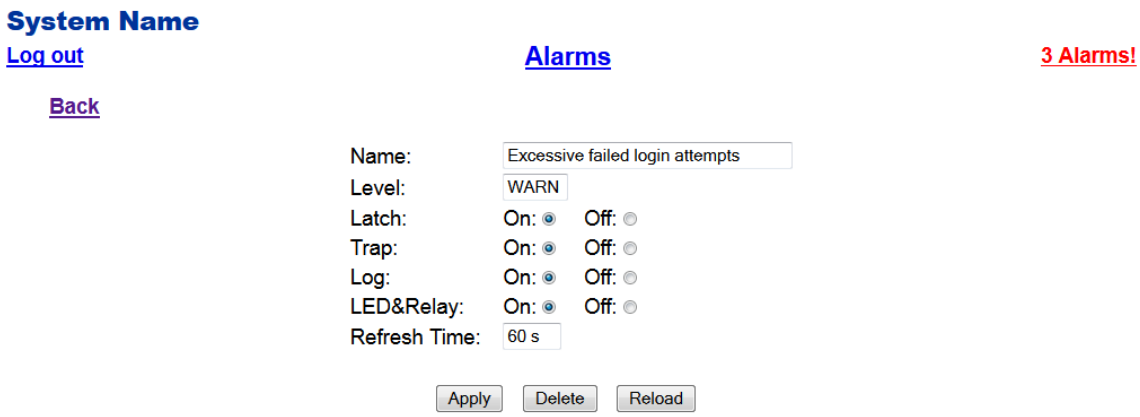


Figure 69: Alarm Configuration Form

Parameter	Description
Name	Synopsis: Any 34 characters Default: sys_alarm The alarm name (e.g. as obtained via CLI:"alarms")
Level	Synopsis: { EMRG, ALRT, CRIT, ERRO, WARN, NOTE, INFO, DEBG } Severity level of the alarm: • EMERG - The device has had a serious failure that caused a system reboot.

Parameter	Description
	• ALERT - The device has had a serious failure that did not cause a system reboot. • CRITICAL - The device has a serious unrecoverable problem. • ERROR - The device has a recoverable problem that does not seriously affect operation. • WARNING - Possibly serious problem affecting overall system operation. • NOTIFY - Condition detected that is not expected or not allowed. • INFO - Event which is a part of normal operation, e.g. cold start, user login etc. • DEBUG - Intended for factory troubleshooting only.
Latch	Synopsis: { On, Off } Default: Off Enables latching occurrence of this alarm in the Alarms Table.
Trap	Synopsis: { On, Off } Default: Off Enables sending an SNMP trap for this alarm.
Log	Synopsis: { On, Off } Default: Off Enables logging the occurrence of this alarm in syslog.txt.
LED & Relay	Synopsis: { On, Off } Default: Off Enables LED and fail-safe relay control for this alarm. If latching is not enabled, this field will remain disabled.
Refresh Time	Synopsis: 0 s to 60 s Default: 60 s Refreshing time for this alarm.

Section 9.1.5

Viewing and Clearing Latched Alarms

The alarm table provides a summary of all alarms that have recently occurred. Alarms are 'latched' until explicitly cleared by the user so that transient problems can be easily identified and corrective action taken. It is intended to be a simple tool to aid in system troubleshooting.

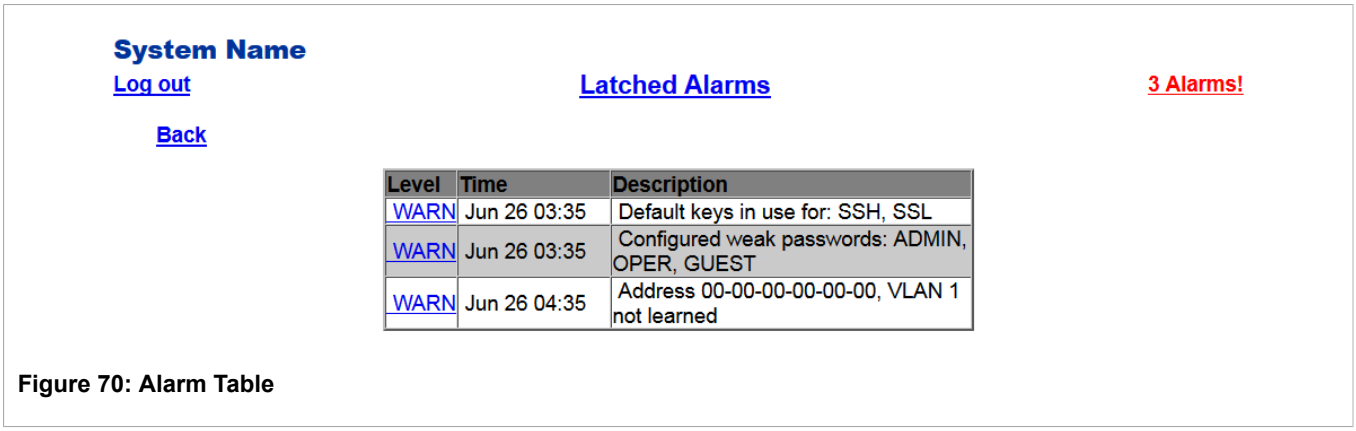


Figure 70: Alarm Table

Parameter	Description
Level	Synopsis: { EMRG, ALRT, CRIT, ERRO, WARN, NOTE, INFO, DEBG } Severity level of alarm. • EMERG - The device has had a serious failure that caused a system reboot. • ALERT - The device has had a serious failure that did not cause a system reboot. • CRITICAL - The device has a serious unrecoverable problem. • ERROR - The device has a recoverable problem that does not seriously affect operation. • WARNING - Possibly serious problem affecting overall system operation. • NOTIFY - Condition detected that is not expected or not allowed. • INFO - Event which is a part of normal operation, e.g. cold start, user login etc. • DEBUG - Intended for factory troubleshooting only.
Time	Synopsis: MMM DD HH:MM Time of first occurrence of the alarm.
Description	Synopsis: Any 127 characters Description of the alarm; gives details about the frequency of the alarm if it has occurred again since the last clear.

Alarms can be cleared from the Clear Alarms option.

Section 9.1.6

Security Messages for Authentication

RUGGEDCOM ROS provides various logging options related to login authentication. A user can log into a RUGGEDCOM ROS device in three different ways: Console, SSH or Telnet. RUGGEDCOM ROS can log messages in the syslog, send a trap to notify an SNMP manager, and/or raise an alarm when a successful and unsuccessful login event occurs. In addition, when a weak password is configured on a unit or when the primary authentication server for TACACS+ or RADIUS is not reachable, RUGGEDCOM ROS will raise alarms, send SNMP traps and log messages in the syslog.

The following is a list of log and alarm messages related to user authentication:

- Weak Password Configured
- Default Keys In Use
- Login and Logout Information
- Excessive Failed Login Attempts
- RADIUS Server Unreachable
- TACACS Server Unreachable
- TACACS Response Invalid
- SNMP Authentication Failure
- Unknown privKey from SNMPv3 User

NOTE
All alarms and log messages related to login authentication are configurable. See Section 9.1.4, "Configuring Alarms" for more information.

Section 9.1.6.1
Weak Password Configured

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when a weak password is configured in the Passwords table.

Table: Configurable Options

Message Name	Alarm	SNMP Trap	Syslog
Weak Password Configured	Yes	Yes	Yes

Section 9.1.6.2
Default Keys In Use

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when default keys are in use. For more information about default keys, refer to Section 1.4, "Certificate and Key Requirements".

NOTE
For Non-Controlled (NC) versions of RUGGEDCOM ROS, this alarm is only generated when default SSL keys are in use.

Table: Configurable Options

Message Name	Alarm	SNMP Trap	Syslog
Default Keys In Use	Yes	Yes	Yes

Section 9.1.6.3
Login and Logout Information

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when a successful and unsuccessful login attempt occurs. A message is also logged in the syslog when a user with a certain privilege level is logged out from the device.

Login attempts are logged regardless of how the user accesses the device (i.e. SSH, Web, Console, Telnet or RSH). However, when a user logs out, a message is only logged when the user is accessing the device through SSH, Telnet or Console.

Table: Configurable Options

Message Name	Alarm	SNMP Trap	Syslog
Successful Login	Yes	Yes	Yes
Failed Login	Yes	Yes	Yes
User Logout	No	No	Yes

Section 9.1.6.4
Excessive Failed Login Attempts

RUGGEDCOM ROS generates this alarm and logs a message in the syslog after 10 failed login attempts by a user.

Table: Configurable Options

Message Name	Alarm	SNMP Trap	Syslog
Excessive Failed Login Attempts	Yes	Yes	Yes

Section 9.1.6.5
RADIUS Server Unreachable

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when the primary RADIUS server is unreachable.

Table: Configurable Options

Message Name	Alarm	SNMP Trap	Syslog
Primary RADIUS Server Unreachable	Yes	Yes	Yes

Section 9.1.6.6
TACACS Server Unreachable

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when the primary TACACS server is unreachable.

Table: Configurable Options

Message Name	Alarm	SNMP Trap	Syslog
Primary TACACS Server Unreachable	Yes	Yes	Yes

Section 9.1.6.7
TACACS Response Invalid

RUGGEDCOM ROS generate this alarm and logs a message in the syslog when the response from the TACACS server is received with an invalid CRC.

Table: Configurable Options

Message Name	Alarm	SNMP Trap	Syslog
TACACS Response Invalid	Yes	Yes	Yes

Section 9.1.6.8
SNMP Authentication Failure

RUGGEDCOM ROS generates this alarm, sends an authentication failure trap, and logs a message in the syslog when an SNMP manager with incorrect credentials communicates with the SNMP agent in RUGGEDCOM ROS.

Table: Configurable Options

Message Name	Alarm	SNMP Trap	Syslog
SNMP Authentication Failure	Yes	Yes	Yes

Section 9.2
Viewing CPU Diagnostics

The diagnostics table provides CPU information useful for troubleshooting hardware and software operation and performance.

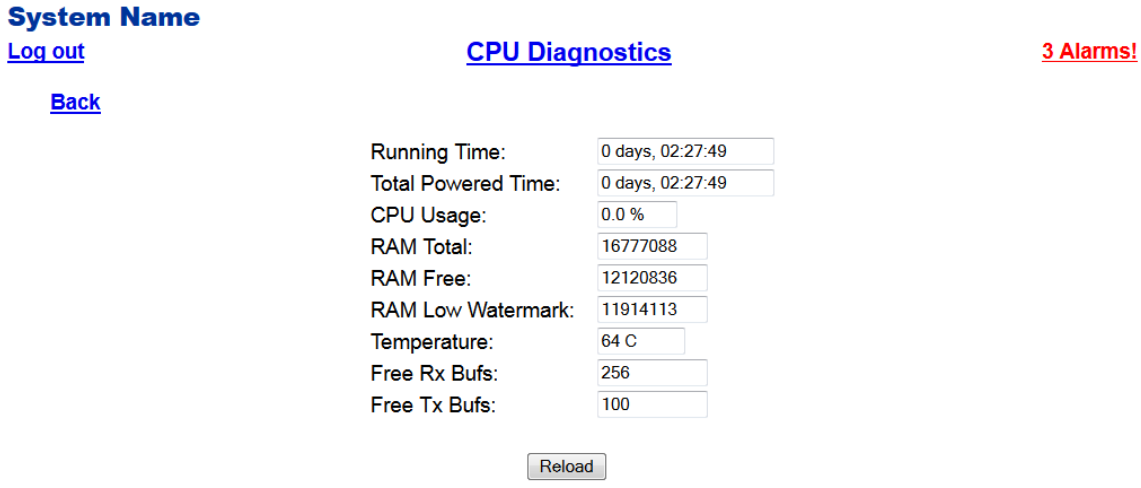


Figure 71: CPU Diagnostics Form

Parameter	Description
Running Time	Synopsis: DDDD days, HH:MM:SS The length of time since the device was last powered on.
Total Powered Time	Synopsis: DDDD days, HH:MM:SS The cumulative powered up time of the device.
CPU Usage	Synopsis: 0% to 100% The percentage of available CPU cycles used for device operation as measured over the last second.
RAM Total	Synopsis: 0 to 4294967295 The total number of bytes of RAM in the system.
RAM Free	Synopsis: 0 to 429496729

Parameter	Description
	The total number of bytes of RAM still available.
RAM Low Watermark	Synopsis: 0 to 4294967295 The total number of bytes of RAM that have not been used during the system runtime.
Temperature	Synopsis: -32768 to 32767 C The temperature of the CPU board.
Free Rx Bufs	Synopsis: 0 to 4294967295 Free Rx Buffers.
Free Tx Bufs	Synopsis: 0 to 4294967295 Free Tx Buffers.

Section 9.3

Viewing and Clearing the System Log

The system log records various events including reboots, user sign-ins, alarms and configuration saves.

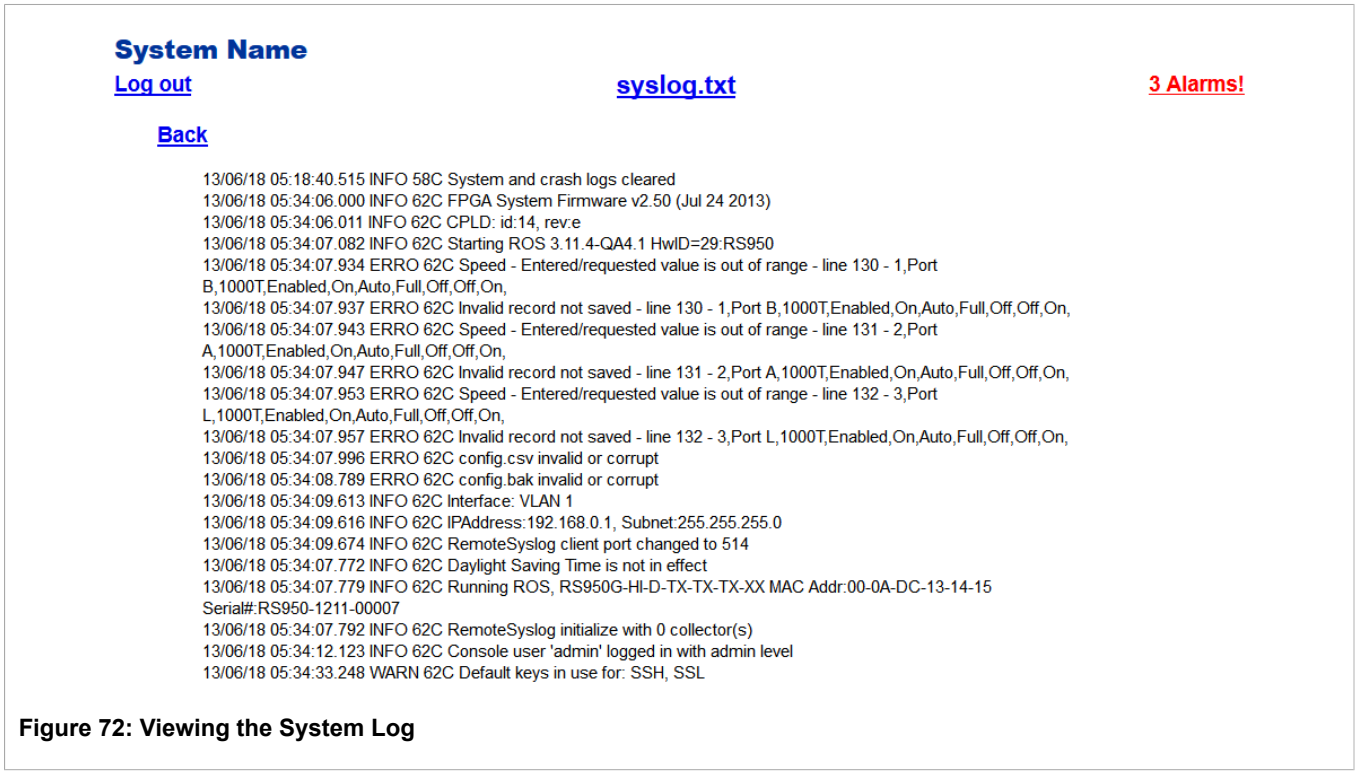


Figure 72: Viewing the System Log

The system log will continue to accumulate information until it becomes full. There is enough room in the file to accumulate logs for months or years under normal operation.

The Clear System Log option will clear the system log. Clearing the log is recommended after a firmware upgrade.

Section 9.4
Viewing Product Information

Figure 73: Product Information Form

Parameter	Description
MAC Address	Synopsis: ##-##-##-##-##-## where ## ranges 0 to FF Shows the unique MAC address of the device.
Order Code	Synopsis: Any 57 characters Shows the order code of the device.
Classification	Synopsis: Any 15 characters Provides system classification. The value 'Controlled' indicates the main firmware is a Controlled release. The value 'Non-Controlled' indicates the main firmware is a Non-Controlled release. The 'Controlled' main firmware can run on Controlled units, but it cannot run on Non-Controlled units. The 'Non-Controlled' main firmware can run on both Controlled and Non-Controlled units.
Serial Number	Synopsis: Any 31 characters Shows the serial number of the device.
Main Version	Synopsis: Any 47 characters Shows the version and build date of the main operating system software.
Hardware ID	Synopsis: { RS950G } Shows the type, part number, and revision level of the hardware.

Section 9.5
Loading Factory Default Configuration

The Load Factory Defaults menu is used to reset the unit's configuration to its factory default. Optionally, it is possible to exclude parameters that affect basic connectivity from the reset in order to be able to remain in

communication with the device. Specifically, configuration items in the following categories are *not* affected by a selective configuration reset:

- IP Interfaces
- IP Gateways
- RuggedCom Discovery Protocol™ (RCDP)
- Time Zone
- DST Offset
- DST Rule

The menu presents a choice of whether to reset all or only the selected set of configuration parameters to their factory default values:

Figure 74: Load Factory Defaults Dialog

Parameter	Description
Defaults Choice	Synopsis: { None, Selected, All } Setting some records such as the IP Interfaces management interface, default gateway settings, to the default value would cause the switch to be inaccessible with management applications. This parameter allows the user to choose to load defaults to selected tables (i.e. excluding those listed above), which would preserve configuration of the tables that are critical for basic communication and switch management applications, or to force All tables to default settings.

NOTE
It is possible to explicitly reset configuration items in the exceptional categories listed above to their default values by using the "sql" command. Refer to Section 2.6.1, "Available CLI Commands".

Section 9.6

Resetting the Device

This operation will warm-start the device after the user has confirmed the reset operation from the Reset Device option.

Figure 75: Reset Device Dialog

Section 9.7

Transferring Files

The Files Transfer form is used to transfer files between the device and a PC. To transfer files using this form, either a TFTP server must be installed and running on the PC, or a TELNET connection must be established with the device so that XMODEM can be used to transfer files.

If a TFTP server is installed and running on the PC, press **GET** to transfer from the PC to the device, or **PUT** to transfer from the device to the PC.

Available files include:

- main.bin (application software)
- config.csv (configuration file)
- syslog.txt (system log file)

NOTE
If the transfer is not completed within 1 minute, an error will be reported.

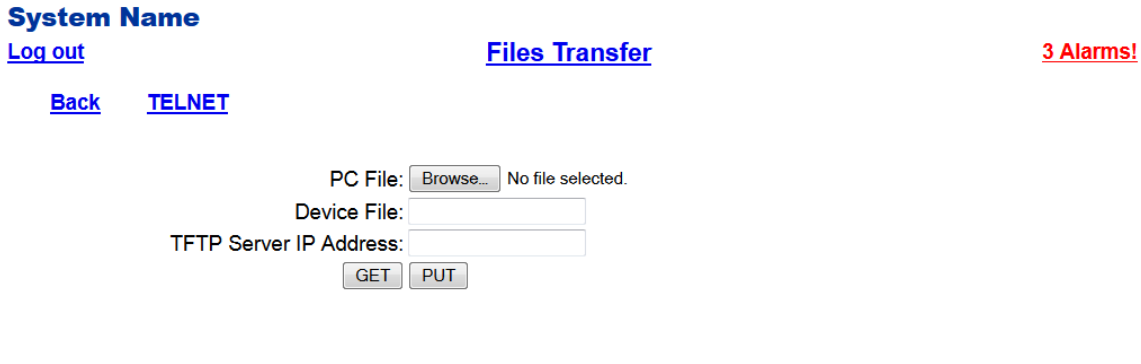


Figure 76: Files Transfer Form

Parameter	Description
PC File	The path and name of the file on your local PC. Use the Browse button to locate the file.
Device File	The name of the file on the device.

Parameter	Description
TFTP Server IP Address	The IP address of a TFTP server. A TFTP server application must be installed on your local PC.

10 Firmware Upgrade and Configuration Management

RUGGEDCOM ROS provides flexible, powerful mechanisms for the bulk update and backup of system firmware and of the configuration database. The RUGGEDCOM ROS firmware and configuration database are represented as files in the internal file system, and bulk update and backup consist of simply transferring files to and from the RUGGEDCOM ROS device, by one of the several means provided.

Section 10.1
Files Of Interest

The files in RUGGEDCOM ROS that may be updated and backed up are described below:

- *main.bin*: the main RUGGEDCOM ROS application firmware image – upgrades to RUGGEDCOM ROS Main Firmware are made via updates to this file.
- *config.csv*: the complete configuration database, in the form of a comma-delimited ASCII text file.
- *banner.txt*: contains text that appears on the login screen.
- *system.bin*: encapsulates FPGA firmware and first stage bootloader – upgrades to FPGA Firmware are made via updates to this file.

Section 10.2
File Transfer Mechanisms

Several mechanisms are available to transfer these files to and from a RUGGEDCOM ROS-based device:

- *Xmodem* using the RUGGEDCOM ROS CLI over a (telnet or RS232) console session.
- *TFTP client* (using the RUGGEDCOM ROS CLI in a console session and a remote TFTP server).
- *TFTP server* (from a remote TFTP client).
- *SFTP* (secure FTP over SSH, from a remote SFTP client).

Section 10.3
Console Sessions

Console sessions may be established (depending on the settings in the IP Services menu) by the following means:

- *RS232* direct RS232 serial connection to the RUGGEDCOM ROS device.
- *telnet* remote terminal protocol via TCP/IP (unencrypted).
- *RSH* Remote SHell, the remote login shell protocol via TCP/IP (unencrypted).

- *SSH* Secure SHell, the standard remote login shell protocol via TCP/IP – Both authentication and session are encrypted.

Section 10.4
Upgrading Firmware

Upgrading RUGGEDCOM ROS firmware may sometimes be necessary in order to take advantage of new features or bug fixes. In normal circumstances, only the main RUGGEDCOM ROS application firmware is updated; the boot loader and FPGA firmware remain invariant. The main RUGGEDCOM ROS application firmware image is a binary file available from Siemens. Please check the Siemens web site, http://support.automation.siemens.com, for the availability of updates to RUGGEDCOM ROS firmware or contact Siemens support.

Main firmware upgrades are paired with system firmware versions. The table below lists the current minimum requirements:

ROS Version	System Version	Main Firmware Version
3.11.2	1.40	3.11.2
3.11.3	2.21	3.11.3
3.11.4	2.57	3.11.4
3.11.5	4.44	3.11.5
3.11.6	4.44	3.11.6
3.11.7	4.44	3.11.7

Firmware upgrades may be performed using any of the transfer methods and protocols listed in Section 10.2, “File Transfer Mechanisms”.

IMPORTANT!
Refer to the firmware release notes before installing any upgrade. They may contain additional information not found in the User Guide.

IMPORTANT!
Non-Controlled (NC) versions of RUGGEDCOM ROS can not be upgraded to Controlled firmware versions. However, Controlled firmware versions can be upgraded to an NC firmware version.

Section 10.4.1
Applying the Upgrade

Binary firmware images transferred to the RUGGEDCOM ROS-based device are stored in non-volatile memory and require a device reset in order to take effect. The “version” RUGGEDCOM ROS shell command will display any firmware updates that are pending. Currently running firmware is labeled “Current”; pending upgrades are labeled “Next”:

```
>version
Current FPGA System Firmware v3.86 (Nov 11 2013)
Next    FPGA System Firmware v4.44 (Feb 26 2014 10:51)
Current ROS-Microblaze Main Software v3.11.5.QA2_18 (Mar 11 2014 12:40)
```

```
Next    ROS-Microblaze Main Software v3.11.5 (Mar 20 2014 13:43)
```

NOTE
Make sure to transfer both the main.bin and the system.bin files to the device before rebooting the device. Verify that the newest versions are labelled "Next".

To reset the device from the command line, type

```
reset
```

and press Enter.

Section 10.4.2
Security Considerations

File transfers using methods that require RUGGEDCOM ROS login authentication, namely Xmodem, SFTP, and the RUGGEDCOM ROS TFTP client, are subject to the following conditions:

- transfers *from* the RUGGEDCOM ROS-based device may be performed by any user with login privileges.
- transfers *to* the RUGGEDCOM ROS-based device may only be performed by those with administrator privileges.

The exception is that the SFTP server does not support transmission of the firmware or configuration file using anything less than administrator privileges.

File transfers (in both directions) that make use of the RUGGEDCOM ROS TFTP server do not require authentication, since TFTP does not define an authentication scheme. Instead, the TFTP server must be enabled from the IP Services Configuration Menu when it is needed.

NOTE
It is recommended to use the RUGGEDCOM ROS TFTP server (or any TFTP server) only on a secure network, owing to TFTP's lack of an authentication scheme. Even so, and especially in a production environment, it is also recommended to leave the TFTP server enabled for only as long as it is needed.

The following sections describe briefly how to upgrade the main application firmware using each of the mechanisms provided by RUGGEDCOM ROS.

Section 10.4.3
Upgrading Firmware Using XModem

This method requires that the binary image file of the main RUGGEDCOM ROS application firmware, along with serial terminal or telnet software and the ability to do Xmodem transfers, be available on a computer with an RS232 or network connection, respectively, to the RUGGEDCOM ROS device to be upgraded.

Establish a console connection with administrative privileges, either via the RS232 port or via telnet. Enter the RUGGEDCOM ROS command, "xmodem receive main.bin<CR>". When RUGGEDCOM ROS responds with "Press Ctrl-X to cancel", begin your Xmodem transmission, using the means provided by your terminal software. After the file transfer has been completed, the device will provide an indication that the file has been transferred successfully. Repeat the previous steps for the system.bin file. The transcript of a sample exchange, looking at the RUGGEDCOM ROS CLI, follows:

```
>xmodem receive main.bin
Press Ctrl-X to cancel
Receiving data now ...C
```

```
Received 4905579 bytes. Closing file main.bin ...
main.bin transferred successfully
>xmodem receive system.bin
Press Ctrl-X to cancel
Receiving data now ...C
Received 4227098 bytes. Closing file main.bin ...
system.bin transferred successfully
```

If possible, select the “XModem 1K” protocol for transmission; otherwise, select “XModem”. The device must be reset in order for the new software to take effect. If you want to reset the device immediately, enter “reset<CR>”. The device will reboot within a few seconds.

Section 10.4.4

Upgrading Firmware Using the RUGGEDCOM ROS TFTP Server

This method requires that the binary image file of the main RUGGEDCOM ROS application firmware, along with TFTP client software, be available on a computer with a network connection to the RUGGEDCOM ROS device to be upgraded.

NOTE

*The **TFTP Server** parameter in **IP Services Configuration** controls how a TFTP client can access the device’s built-in TFTP server. A setting of “Disabled” prevents all access, “Get Only” allows retrieval of files only, and “Enabled” allows both storing and retrieval of files. Ensure that this parameter is set appropriately for the type of access you wish to perform.*

Enable TFTP transfers to the RUGGEDCOM ROS device, as noted above. Begin a TFTP transfer in binary mode to the device, specifying a destination filename of “main.bin”. A TFTP client utility will provide an indication that the file was transferred properly, but it is recommended to also query the device directly in order to verify successful transfer. Establish a console session to the RUGGEDCOM ROS device (using RS232, telnet, or SSH) and enter the “version” command, as described in Section 10.4.1, “Applying the Upgrade”, above. If the transfer was successful, the version of the firmware file that was transferred will appear as the “Next” firmware version, i.e. that will appear after the next reset. Repeat the previous steps for the system.bin file.

The transcript of a sample TFTP transfer, looking at a DOS/Windows CLI, follows:

```
C:\>tftp -i 192.168.0.1 PUT C:\files\ROS-MBlaze_Main_v3-11-5.bin main.bin
Transfer successful: 4905579 bytes in 28 second(s), 175199 bytes/s

C:\>tftp -i 192.168.0.1 PUT C:\files\FPGA_System_v4_44.bin system.bin
Transfer successful: 4227098 bytes in 27 second(s), 156559 bytes/s
```

Section 10.4.5

Upgrading Firmware Using the RUGGEDCOM ROS TFTP Client

This method requires that the binary image file of the main RUGGEDCOM ROS application firmware, along with a correctly configured TFTP server, be available on a computer with a network connection to the RUGGEDCOM ROS device to be upgraded.

Identify the IP address of the host providing the TFTP server capability. Ensure that the firmware revision to be downloaded (e.g. RUGGEDCOM ROS-MBlaze_Main_v3.11.2.bin) is present there. Establish a console

connection with administrative privileges to the RUGGEDCOM ROS device to be upgraded (i.e. via RS232, telnet, or SSH). Enter the CLI shell and run the TFTP client command to receive the firmware image, for example:

```
tftp <TFTP server> get <remote filename> main.bin
```

where:

- *TFTP server* is the IP address of the TFTP server
- *remote filename* is the name of the binary image file of the main RUGGEDCOM ROS application firmware residing in the TFTP server outgoing directory

Verify, as above, the successful transfer via the RUGGEDCOM ROS CLI “version” command. Repeat the previous steps for the system.bin file. A sample transcript from the RUGGEDCOM ROS CLI:

```
>tftp 192.168.0.254 get ROS-MBlaze_Main_v3.11.5.bin main.bin
TFTP CMD: main.bin transfer ok. Please wait, closing file ...
TFTP CMD: main.bin loading succesful.
>tftp 192.168.0.254 get FPGA_System_v4_44.bin system.bin
TFTP CMD: system.bin transfer ok. Please wait, closing file ...
TFTP CMD: system.bin loading succesful.
```

Section 10.4.6

Upgrading Firmware Using SFTP

This method requires that the binary image file of the main RUGGEDCOM ROS application firmware, along with SFTP client software, be available on a computer with a network connection to the RUGGEDCOM ROS device to be upgraded. SFTP is the Secure File Transfer Protocol (also known as the SSH File Transfer Protocol), a file transfer mechanism that uses SSH to encrypt every aspect of file transfer between a networked client and server.

Establish an SFTP connection with administrative privileges to the RUGGEDCOM ROS device to be upgraded. Begin a transfer to the device, specifying a destination filename of “main.bin”. An SFTP client utility will provide an indication that the file was transferred properly, but, again, it is recommended to also query the device directly in order to verify successful transfer via the RUGGEDCOM ROS CLI command. Repeat the previous steps for the system.bin file. A sample SFTP session to upgrade the RUGGEDCOM ROS main firmware image from a Linux workstation follows:

```
user@host$ sftp admin@ros_ip
Connecting to ros_ip...
admin@ros_ip's password:
sftp> put ROS-MBlaze_Main_v3-11-5.bin main.bin
Uploading ROS-MBlaze_Main_v3-11-5.bin to /main.bin
ROS-MBlaze_Main_v3-11-5.bin 100% 2139KB 48.6KB/s 00:44
sftp> put FPGA_System_v4_44.bin system.bin
Uploading FPGA_System_v4_44.bin to /system.bin
FPGA_System_v4_44.bin 100% 2139KB 48.6KB/s 00:44
```

Section 10.5

ROS Recovery

If for any reason, the `main.bin` file becomes corrupted, the device will be unresponsive. In this case, you will need to send the file again to complete the upgrade. To finish the upgrade correctly and return the device to normal functioning, complete the following procedure. In the example provided, a Tera Term terminal is being used to perform an upgrade of the `main.bin` file using a TFTP client, and the upgrade has just failed.

1. The device is unresponsive. In the terminal window, the following message appears:

```
Rugged Bootloader v1.0.QA1
- Press <CTRL><C> to enter boot shell
- RAM Test .................[Passed]
- Verifying main.bin...100%
Press any key and transfer main.bin
```

The prompt, *Press any key and transfer main.bin*, indicates that `main.bin` has been corrupted.

Press any key on the keyboard.

The following message appears:

```
Receiving data now...
```

2. On the toolbar, click *File*, and then point to *Transfer*. Point to *XMODEM*, and then click *Send*.

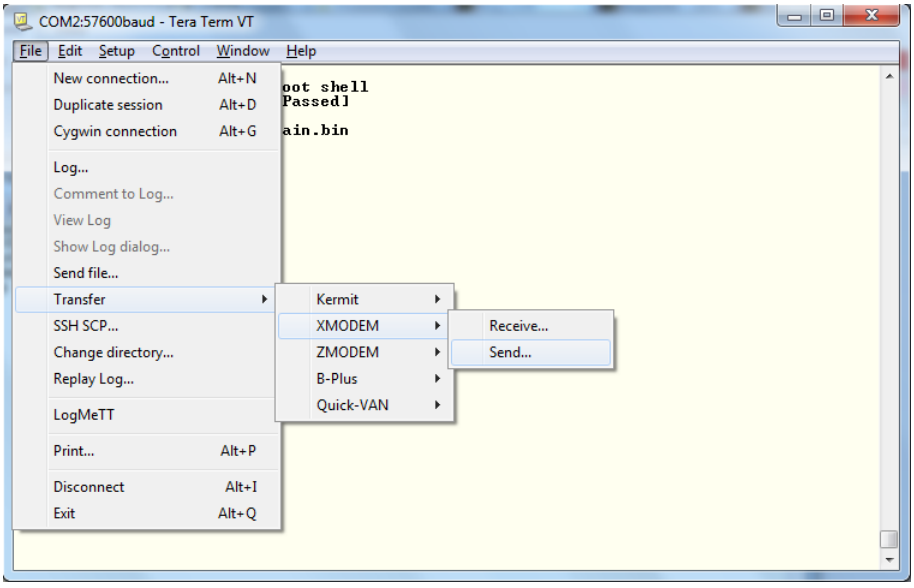


Figure 77: Clicking Send to Send the Data

A dialog box appears.

3. Select the file to be upgraded.

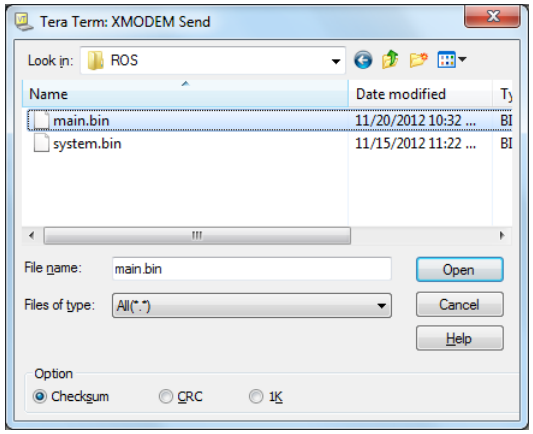


Figure 78: Selecting the File for the Upgrade

4. Click *Open*. The upgrade processes again and the device resets automatically. The device is now responsive.
5. Perform a firmware upgrade. For more information, see Section 10.4, “Upgrading Firmware”.

Section 10.6

Updating Configuration

By default, RUGGEDCOM ROS maintains its complete configuration in an ASCII text file, in CSV (Comma-Separated Value) format. The file can also be encrypted and assigned a passphrase key for protection. All configuration changes, whether they are performed using the web interface, console interface, CLI or SQL, are stored in this one file. The file, named *config.csv*, may be read from and written to the RUGGEDCOM ROS device in all the same ways that firmware image files can, as described in the preceding sections. The configuration file may be copied from the unit and used as a backup, to be restored at a later date. Configuration files from different units may be compared using standard text processing tools.

For more information about encrypting the configuration file, refer to Section 3.4, “Data Storage”.

NOTE

Data encryption is not available in NC versions of RUGGEDCOM ROS.

When switching between Controlled and Non-Controlled (NC) versions of RUGGEDCOM ROS, make sure data encryption is disabled. Otherwise, the NC version of RUGGEDCOM ROS will ignore the encrypted configuration file and load the factory defaults.

The transfer mechanisms supported for the update of *config.csv* are the same as for RUGGEDCOM ROS firmware image files:

- *Xmodem* using the RUGGEDCOM ROS CLI over a console session.
- *TFTP client* (using the RUGGEDCOM ROS CLI in a console session and a remote TFTP server).
- *TFTP server* (from a remote TFTP client).
- *SFTP* (secure FTP over SSH, from a remote SFTP client).

Please refer to the preceding section, Section 10.4, “Upgrading Firmware”, for examples of the use of each of these mechanisms for transferring a file to a RUGGEDCOM ROS device.

Once a configuration file has been successfully transferred, it is automatically applied.

Configuration File Format

The format of the configuration file makes it simple to apply a wide variety of tools to the task of maintaining RUGGEDCOM ROS configuration. Among the applications that may be used to manipulate RUGGEDCOM ROS configuration files are:

- Any text editing program capable of reading and writing ASCII files.
- Difference/patching tools (e.g. the UN*X “diff” and “patch” command line utilities).
- Source Code Control systems (e.g. CVS, SVN).

CAUTION!
Do not edit an encrypted configuration file. Any line that has been modified manually will be ignored.

RUGGEDCOM ROS also has the ability to accept partial configuration updates. It is possible to, for example, update only the parameters for a single Ethernet port. Transferring a file containing only the following lines to a RUGGEDCOM ROS device will result in an update of the parameters for Ethernet port 1 without changing any other parameters of the device’s configuration:

```
# Port Parameters
ethPortCfg
Port,Name,Media,State,AutoN,Speed,Dupx,FlowCtrl,LFI,Alarm,
1,Port 1,100TX,Enabled,On,Auto,Auto,Off,Off,On,
```

Security Considerations

The same limitations apply to writing *config.csv* to the RUGGEDCOM ROS device that apply to firmware images. Refer to Section 10.4, “Upgrading Firmware” for details on the permissions necessary to write the RUGGEDCOM ROS configuration file.

Section 10.7

Backing Up RUGGEDCOM ROS System Files

All of the same file transfer mechanisms discussed in the preceding sections may also be used to transfer files *from* a RUGGEDCOM ROS device, as well as to update firmware or configuration files. It might be desirable, in addition to creating an archive of the device’s firmware files, to back up the configuration database, *config.csv*, or system log file, *syslog.txt*, on a regular basis. Type “dir” at the RUGGEDCOM ROS CLI for a listing and description of files on the RUGGEDCOM ROS device.

An example of backing up a file using SFTP follows. For descriptions on the use of the other file transfer mechanisms, please refer to the examples in Section 10.4, “Upgrading Firmware”. Note that only the direction of file transfer changes.

Section 10.7.1

Backing Up Files Using SFTP

This method requires that SFTP client software be available on a computer with a network connection to the RUGGEDCOM ROS device that one wishes to back up. Establish an SFTP connection with administrative privileges to the RUGGEDCOM ROS device. Begin transferring the desired file from the device. An example of using an SFTP session to create a local backup of the RUGGEDCOM ROS main firmware image to a Linux workstation follows:

```
user31host$ sftp admin31ros_ip
Connecting to ros_ip...
admin31ros_ip's password:
sftp> get main.bin
Downloading /main.bin
main.bin                                      100% 2139KB  48.7KB/s   00:44
sftp>
```

All files in RUGGEDCOM ROS may be backed up using an SFTP session with administrative privileges.