Division / Business Unit: Enterprise Services
Function: Signalling
Document Type: Work Instruction

Recommended Settings for Ruggedcom RS400, RS900 and RS900G Series Switch

For use with Westrace MkII CBI, Microlok CBI, VHLC and EC5 CBI in a Fibre Ring Topology within ARTC Network

ESW-01-01

Applicability

ARTC Network Wide SMS

Publication Requirement

Internal / External

Primary Source

ESW-02-01

Document Status

Version #	Date Reviewed	Prepared by	Reviewed by	Endorsed	Approved
1.1	01 Jun 23	Senior Train Control Systems Engineer	Standards	Manager Signalling Standards	Head of Engineering Standards 14/06/2023

Amendment Record

Amendment Version #	Date Reviewed	Clause	Description of Amendment
1.0	08 Mar 23	Section 2, 4	Renumbered document from ESW-02-01, update to be align with ROS version 4.3.5
1.1	01 Jun 23	Section 2.5	Update VLAN configuration settings

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide a configuration base with settings on the Ruggedcom RS400, RS900 and RS900G Series Switch.

1.2 Scope

It is primarily directed for use with Microlok Interlockings, VHLC and EC5 Interlockings and Westrace MkII Interlocking using a fibre redundant ring system within ARTC network, but it is not necessarily limited to that use.

This document should be used in conjunction with a detailed Network design.

This document also describes other relevant information or limitations.

This document also includes information on utilisation for RS900, RS900G series switch within the same RS400 switch network.

1.3 Definitions

Preferred setting – **preferred** values to be set

Optional setting – **optional** values to be set dependent on a number of factors including network design

(Assigned as per Network Design – **critical information** relating to values to be set

(Comment on configuration setting) – General comments or information

2 CONFIGURATION SETTINGS

2.1 Administration

IP Interfaces (ipIfCfg)

Provide the ability to configure IP interfaces.
1 of 16 entries used.

Type
Synopsis: { VLAN }
Default: VLAN
Specifies the type of the interface for which this IP interface is created.

ID
Synopsis: 1 to 4094
Default: 1 (Default is native VLAN) (Assigned as per the network design)
Specifies the ID of the interface for which this IP interface is created. If interface type is VLAN, represents VLAN ID.

Mgmt
Synopsis: { No, Yes }
Default: No (This setting is required to be turned on for access to management via Ethernet)
Specifies whether the IP interface is the device management interface.

IP Address Type
Synopsis: { Static, Dynamic, DHCP, BOOTP }
Default: Static
Specifies whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server.
Must be static for non-management interfaces

IP Address
Synopsis: ###.###.###.### where ### ranges from 0 to 255
Default: 192.168.0.1 (Assigned as per the network design)
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 (Assigned as per the network design)
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.

IP Gateways (GatewayCfg)

Provide the ability to configure gateways.
1 of 10 entries used. Multiple Path can be set (Assigned as per the network design)

Destination
Synopsis: ###.###.###.### where ### ranges from 0 to 255
Default: (Assigned as per the network design)

Specifies the IP address of destination network or host. For default gateway, both the destination and subnet are 0.

Subnet
Synopsis: ###.###.###.### where ### ranges from 0 to 255
Default: (Assigned as per the network design)
Specifies the destination IP subnet mask. For default gateway, both the destination and subnet are 0.

Gateway
Synopsis: ###.###.###.### where ### ranges from 0 to 255
Default: (Assigned as per the network design)
Specifies the gateway to be used to reach the destination.

IP Services (ipServices)

Provide the ability to configure IP connection parameters such as address, network mask and gateway, and other IP services provided by the device.

Inactivity Timeout
Synopsis: 1 min to 60 min 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 maximum timeout value is limited to 30 minutes.

Telnet Sessions Allowed
Synopsis: 0 to 4 or { Disabled }
Default: Disabled
Limits the number of Telnet sessions. A value of zero prevents any Telnet access.

Web Server Users Allowed
Synopsis: 1 to 4 or { Disabled }
Default: 4
Limits the number of simultaneous web server users.

TFTP Server
Synopsis: { Disabled, Get Only, Enabled } (used by Maintenance Tools)
Default: Disabled
As TFTP is a very insecure protocol, this parameter allows user to limit or disable TFTP Server access.
DISABLED - disables read and write access to TFTP Server
GET ONLY - only allows to read files via TFTP Server
ENABLED - allows to read and write files via TFTP Server

ModBus Address
Synopsis: 1 to 255 or { Disabled }
Default: Disabled
Determines the Modbus address to be used for Management through Modbus.

SSH Sessions Allowed
Synopsis: 1 to 4
Default: 4
Limits the number of SSH sessions.

RSH Server
Synopsis: { Disabled, Enabled }
Default: Disabled (controlled version) or Enabled (non-controlled version)
Disables/enables Remote Shell access.

System Identification (systemId)

Provide the ability to configure system identification parameters for the switch which makes it easier to identify the switch.

System Name
Synopsis: Any 24 characters
Default: System Name (Assigned as per the network design)
The system name is displayed in all RuggedSwitch 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 (Assigned as per the network design)
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 (Assigned as per the network design)
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.

Passwords (passwordCfg)

Provides ability to configure usernames&passwords and authorization/authentication type. Passwords and usernames can be up to fifteen characters long and must not contain spaces. Three groups of passwords and names can be programmed, which correspond to three access levels.

Auth Type
Synopsis: { Local, RADIUS, TACACS+, RADIUSorLocal, TACACS+orLocal }
Default: Local (Assigned as per the network design)

Password can be authenticated using locally configured values, or remote RADIUS or TACACS+ server. Setting value to any of combinations that involve RADIUS or TACACS+ require Security Server Table to be configured.
Settings:
Local - authentication from local Password Table
RADIUS - authentication using RADIUS server
TACACS+ - authentication using TACACS+ server
RADIUSOrLocal - authentication using RADIUS.
If server cannot be reached, authenticate
from local Password Table
TACACS+OrLocal - authentication using TACACS+.
If server cannot be reached, authenticate
from local Password Table

Guest Username
Synopsis: Any 15 characters

Default: guest
Related password is in field Guest Password; view only, cannot change settings or run any commands.

Guest Password
Synopsis: Any 19 character ASCII string (Assigned as per the network design)
Related username is in field Guest Username; view only, cannot change settings or run any commands.

Confirm Guest Password
Synopsis: Any 19 character ASCII string (Assigned as per the network design)
Related username is in field Guest Username; view only, cannot change settings or run any commands.

Operator Username
Synopsis: Any 15 characters
Default: operator
Related password is in field Operator Password; cannot change settings; can reset alarms, statistics, logs, etc.

Operator Password
Synopsis: Any 19 character ASCII string
Related username is in field Operator Username; cannot change settings; can reset alarms, statistics, logs, etc.

Confirm Operator Password
Synopsis: Any 19 character ASCII string
Related username is in field Operator Username; cannot change settings; can reset alarms, statistics, logs, etc.

Admin Username
Synopsis: Any 15 characters
Default: admin
Related password is in field Admin Password; full read/write access to all settings and commands.

Admin Password
Synopsis: Any 19 character ASCII string
Related username is in field Admin Username; full read/write access to all settings and commands.

Confirm Admin Password
Synopsis: Any 19 character ASCII string
Related username is in field Admin Username; full read/write access to all settings and commands.

Password Minimum Length
Synopsis: 1 to 17
Default: 1
Configure the password string minimum length. The new password shorter than the minimum length will be rejected.

Time and Date (timeDateCfg)

Allows the time and date to be viewed and set.

Time

Synopsis: HH:MM:SS
This parameter allows for both the viewing and setting of the local time.

Date

Synopsis: MMM DD, YYYY
This parameter allows for 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), ... }
Default: UTC+10:00 (Melbourne, Sydney)
This setting allows for the conversion of UTC (Universal Coordinated Time) to local time.
Time Zone setting refers to geographical location including use of Daylight Savings Time variable as required

DST Offset

Synopsis: HH:MM:SS
Default: 00:00:00 01:00:00
This parameter specifies the amount of time to be shifted forward/backward when DST begins and ends. For example for most part of 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
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 – nth d-day in month (1 – 1st d-day, 5 – 5th/last d-day)
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 part of USA and Canada:
03.2.0/02:00:00 11.1.0/02:00:00
DST begins on March's 2nd Sunday at 2:00am.
DST ends on November 1st Sunday at 2:00am.

NTP Service (ntpLocalServerCfg)

To enable or disable NTP Service.

SNTP

Synopsis: { Enabled, Disabled }
Enable or Disable NTP service

NTP Servers (ntpCfg)

To configure either the primary or backup NTP server

Server
Synopsis: Any 8 characters
Default: Primary
This field tells whether this configuration is for Primary or a Backup Server.

IP Address
Synopsis: ###.###.###.### where ### ranges from 0 to 255
The Server IP Address.

Reachable
Synopsis: { No, Yes }
Shows the status of the server.

Update Period
Synopsis: 1 to 1440 min
Default: 60 min
Determines how frequently the (S)NTP server is polled for a time update. If the server cannot be reached in three attempts that are made at one minute intervals an alarm is generated.

SNMP

SNMP Users (snmpV3UsersCfg)
Configure users for the local SNMPv3 engine.
1 of 32 entries used.

Name
Synopsis: Any 32 characters (ARTC)
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
(10.15.1.7) (Allow access from the 4site server)
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 addressed. 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.

v1/v2c Community
Synopsis: Any 32 characters (ARTC)
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, HMACSHA }
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
The secret authentication key (password) that must be shared with SNMP client. If the key is not an empty string, it must be at least 6 characters long

Confirm Auth Key
Synopsis: 31 character ascii string
The secret authentication key (password) that must be shared with SNMP client. If the key is not an empty string, it must be at least 6 characters long

Priv Key
Synopsis: 31 character ascii string
The secret encryption key (password) that must be shared with SNMP client. If the key is not an empty string, it must be at least 6 characters long

Confirm Priv Key
Synopsis: 31 character ascii string
The secret encryption key (password) that must be shared with SNMP client. If the key is not an empty string, it must be at least 6 characters long

SNMP Security to Group Maps (vacmSecurityToGroupCfg)
Provides ability to map configuration of security model and security name into a group name, which is used to define an access control policy.
1 of 32 entries used.

Security Model
Synopsis: { snmpV1, snmpV2c, snmpV3 } (4site uses v2)
Default: snmpV3
The Security Model that provides 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 index to SNMPv3 VACM Access Table.

SNMP Access (snmpV3AccessCfg)
Provides 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
1 of 32 entries used.

Group
Synopsis: Any 32 characters (read)
The group name to which the security model and name belong. This name is used as index to SNMPv3 VACM Access Table.

SecurityModel
Synopsis: { snmpV1, snmpV2c, snmpV3 }
Default: snmpV3
In order to gain the access rights allowed by this entry, 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 no read access is granted.

WriteViewName
Synopsis: { noView, V1Mib, allOfMib }
Default: noView
This parameter identifies the MIB tree(s) to which this entry authorizes write access. If the value is noView, then no write access is 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 no access for notifications is granted.

Configure Security Server

RADIUS Server (radiusCfg) **(NOT USED)**
These parameters provide the ability to configure RADIUS server for management and 802.1x authentication.

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 Server IP Address.

Auth UDP Port
Synopsis: 1 to 65535
Default: 1812
The authentication Port on server.

Max Retry
Synopsis: 1 to 10

Default: 2
The maximum number of times the Authenticator will attempt to contract the authentication server to authenticate the user in case of any failure.

Timeout
Synopsis: 1000 to 120000
Default: 10000
The amount of time in milliseconds the Authenticator will wait for a response from the authentication server.

Auth Key
Synopsis: 31 character ascii string
Default:
The authentication key to be shared with server. Only available on Controlled versions.

Confirm Auth Key
Synopsis: 31 character ascii string
The authentication key to be shared with server. Only available on Controlled versions.

TACACS Plus Server (tacPlusCfg) (NOT USED)
These parameters provide the ability to configure TACACS+ server for device access control.

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 Server IP Address.

Auth TCP Port
Synopsis: 1 to 65535
Default: 49
The authentication Port on server.

Max Retry
Synopsis: 1 to 10
Default: 3
The maximum number of times the Authenticator will attempt to contract the authentication server to authenticate the user in case of any failure.

Timeout
Synopsis: 1000 to 120000
Default: 10000
The amount of time in milliseconds the Authenticator will wait for a response from the authentication server.

Auth Key
Synopsis: 31 character ascii string
Default: mySecret
The authentication key to be shared with server.

Confirm Auth Key
Synopsis: 31 character ascii string
The authentication key to be shared with server.

DHCP Parameters (dhcpParamsCfh) (NOT USED)

Provides the ability to configure the switch to act as DCHP Relay Agent (using DHCP Option 82).

DHCP Server Address
Synopsis: ###.###.###.### where ### ranges from 0 to 255
Default:
IP address of the DHCP server to which DHCP queries will be forwarded. DHCP server IP must be configured for Relay Agent to work.

DHCP Port Parameters (dhcpPortParamsCfg) (NOT USED)

To enable DHCP Relay Agent (Option 82) for any Ethernet port connected to DHCP client.

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

Option-82
Synopsis: { Disabled, Enabled }
Default: Disabled
Insert DHCP Option 82.

Syslog

Local Syslog (LocalSyslogLevelCfg)
This parameter provide the ability to configure local syslog level.

Local Syslog Level
Synopsis: { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL , DEBUGGING }
Default: INFORMATIONAL
Syslog severity level - {EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING}.

Remote Syslog Client (RemSyslogClntCfg)
This parameter provide the ability to configure syslog client port number.

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

Remote Syslog Server (RemoteSyslogConfig) (NOT USED)
Provides the ability to configure syslog server IP address, port number, facility name and severity level.
0 of 5 entries used.

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 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 }.

Severity
Synopsis: { EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING }
Default: DEBUGGING
Syslog severity level - {EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUGGING}.

2.2 Serial Protocols

The Ruggedcom serial ports will be configured generally for three purposes for Microlok.
1. Microlok Vital Data
2. Microlok Non-Vital
3. Microlok Maintenance Port.

The Ruggedcom serial ports will be configured for RawSocket for VHLC and EC5

Serial Ports (serPortCfg)

These parameters provide the ability to configure a protocol to be supported on the serial port and serial port settings.

Port
Synopsis: 1 to 4
Default: 1 (Assigned as per the network design)
The port number as seen on the front plate silkscreen of the switch.

Name
Synopsis: Any 15 characters
Default: Port 1 (Assigned as per the network design)
A descriptive name that may be used to identify the device connected on that port.

Protocol
Synopsis: { None, RawSocket, ModbusServer, ModbusClient, DNP, WIN, TIN, Microlok, Mirrored Bits, PreemptRawSocket }
Default: None
The serial protocol supported on this serial port.

(Assigned as per the network design)
Dependant on intended use of port
Microlok = Vital Microlok
RawSocket = Non-Vital Microlok, Microlok Maintenance, VHLC or EC5

Type
Synopsis: { RS232, RS485, RS422 }
Default: RS232
A serial port interface type.

(Assigned as per the network design)
Dependant on connected Microlok, VHLC or EC5 port.

ForceHD
Synopsis: { On, Off }
Default: Off
Enables forcing half duplex mode of operation. While sending data out of the serial port all received data are ignored. This mode of operation is available only on ports that operate in full duplex mode.

Baud
Synopsis: 100 to 230400
Default: 9600
The baud rate at which to operate the port.

(Assigned as per the network design)
Dependant on Microlok, VHLC or EC5 port configuration Baud rate

Data Bits
Synopsis: { 7, 8 }
Default: 8
The number of data bits to operate the port with.

Stop
Synopsis: { 1, 1.5, 2 }
Default: 1
The number of stop bits to operate the port with.

Parity
Synopsis: { None, Even, Odd }
Default: None
The parity to operate the port with.

Even only used for LCP with VHLC / EC5. None for all others.

Turnaround
Synopsis: 0 ms to 1000 ms
Default: 0 ms
The amount of delay (if any) to insert between the transmissions of individual messages out the serial port.

DSCP
Synopsis: 0 to 63
Default: 0
DSCP - to set the DS byte in the IP header. DS byte setting is supported in the egress direction only.

Configure Protocols

Protocol (rawsockPortCfg)
These parameters provide the ability to configure RawSocket settings for ports. If no ports appear, then a RawSocket protocol must first be assigned to the port in the Configure Serial Protocol menu

This sets the raw socket protocol settings.
Use for Microlock Non Vital (Genisys), Microlock Maintenance,
VHLC/EC5 Vital (RP2000), VHLC/EC5 Non Vital (Genisys or LCP), VHLC/EC5 Maintenance.

Port
Synopsis: 1 to 4

Default: 1 (Assigned as per the network design)
The port number as seen on the front plate silkscreen of the switch.

Pack Char
Synopsis: 0 to 255 or { Off } 246
Default: 2
The character that can be used to force forwarding of accumulated data to the network. If a packetization character is not configured, accumulated data will be forwarded based upon the packetization timeout parameter.

246 for Genisys (All) and RP2000 (VHLC / EC5) Maintenance (Microlok)
10 for Maintenance (VHLC / EC5)
Off for LCP (VHLC / EC5)

Pack Timer
Synopsis: 3 ms to 1000 ms
Default: 10 ms
The delay from the last received character until when data is forwarded.

50ms for RP2000 (VHLC / EC5)
10ms for all others

Pack Size
Synopsis: 64 to 1400 or { Maximum }
Default: Maximum
Maximum number of bytes received from serial port to be packed in one IP packet.

Flow Control
Synopsis: { None, XON/XOFF }
Default: None
Whether to use XON-XOFF flowcontrol on the port.

Transport
Synopsis: { TCP, UDP }
Default: TCP
The network transport used to transport protocol data over IP network.

UDP for RP2000 (VHLC / EC5) and Genisys (EC5)
TCP for all Microlok and Maintenance / LCP (VHLC/EC5)

Call Dir
Synopsis: { In, Out, Both }
Default: In
Whether to accept an incoming connection, to place an outgoing connection, or to place outgoing connection and wait for incoming (both directions). This parameter is applicable only for TCP transport.

Max Conns
Synopsis: 1 to 64
Default: 1 As per requirements
The maximum number of allowed incoming TCP connections.

Loc Port
Synopsis: 1 to 65535 5000x where x=port number
Default: 50001
The local IP port to use when listening for an incoming connection or UDP data.

Rem Port
Synopsis: 1 to 65535 (Assigned as per the network design)
Default: 50000
The remote TCP port to use when placing an outgoing connection.

IP Address (Assigned as per the network design)
Synopsis: ###.###.###.### where ### ranges from 0 to 255 or { <empty string> }
Default:
For outgoing TCP connection (client) this is the remote IP address to communicate with.
For incoming TCP connection (server), this is the local interface IP address to listen to the local port for connection request. If empty string is configured, IP address of management interface is used.
For both, outgoing and incoming connections enabled (client or server), this is remote IP address where to place an outgoing TCP connection request or from which to accept calls.
</empty string>

Link Stats
Synopsis: { Disabled, Enabled }
Default: Enabled
Enables links statistics collection for protocol.

Remote Hosts (rawSocketHostsCfg)

(As per Network Design when UDP Transport used)
Provides the ability to configure RawSocket using UDP transport for communication with multiple remote hosts.
0 of 64 entries used.

IP Address
Synopsis: ###.###.###.### where ### ranges from 0 to 255
Default:
The IP address of the remote host.

IP Port
Synopsis: 1 to 65535 or { Unknown }
Default: 50000
IP port that remote host listens to.
If this number is 0 (Unknown), the unit only receives from the remote host but not transmit to it.

Port(s)
Synopsis: Any combination of numbers valid for this parameter
Default: All
Local serial ports the remote host is allowed to communicate with.
Examples:
All - all of the serial ports
1 - serial port 1
2,4-6,8 - serial ports 2,4,5,6 and 8

Microlok (microlokCfg)

These parameters provide the ability to configure specific settings for Microlok protocol.

Transport
Synopsis: { TCP, UDP }
Default: UDP
The network transport used to transport protocol data over IP network.

IP Port
Synopsis: 1024 to 65535
Default: 60000
A local port number on which protocol listens to UDP datagrams or TCP connections.

Link Stats
Synopsis: { Disabled, Enabled }
Default: Enabled
Enables links statistics collection for protocol.

DSCP
Synopsis: 0 to 63
Default: 0
DSCP - to set the DS byte in the IP header. DS byte setting is supported in the egress direction only.

Device Address Table (sdaConfigTable)

(Assigned as per the network design)
Settings for the Microlok peer to peer address locations and ports to be used

These parameters provide ability to configure device addresses and local or remote locations.
2 of 1024 entries used.

Protocol
Synopsis: { ModbusServer, ModbusClient, DNP, WIN, TIN, Microlok }
Default: ModbusServer
The serial protocol for which this address is created.

Address
Synopsis: Any 31 characters
Default:
The destination (source) device address. Could be local or remote. Local address is the address of the device connected to the serial port on this device, and then serial port must be configured. Remote address is the address of the device connected to the remote host's serial port. In that case Remote IP Address must be configured.
NOTE: The range and format of the address is defined by a protocol. For example:
Modbus: 1 to 254
Microlok: 1 to 65535, or 8 to 15 hexadecimal digits '1' to 'a'
DNP 3.0: 1 to 65520
WIN: 6 bit address (0 to 63)
TIN: String 'wdr' for wayside data radio (TIN mode 2), or 32 bit address (8 hexadecimal digits '0' to 'f'). All zeros are not allowed.

Remote IP Addr
Synopsis: ###.###.###.### where ### ranges from 0 to 255
Default:
The IP address of remote host where device with configured remote address is connected.

Port
Synopsis: 1 to 16 or { Unknown }
Default: Unknown
For ModbusClient:
The serial port to which master that is polling device with this address is attached.
For all other protocols:

The serial port to which device is attached. If the device with this address is attached to the serial port of remote host, the value of this parameter is 'Unknown'.

Name
Synopsis: Any 16 characters
Default:
The addressed device name.

2.3 Ethernet Ports

Port Parameters (ethPortCfg)

Provides the ability to configure Ethernet ports.

Port
Synopsis: 1 to 4
Default: 0 (Assigned as per the network design)
The port number as seen on the front plate silkscreen of the switch.

Name
Synopsis: Any 15 characters
Default: Port x (Assigned as per the network design)
A descriptive name that may be used to identify the device connected on that port.

Media Dependant on Port
Synopsis: { 100TX, 10FL, 100FX, 1000X, 1000T, 802.11g, EoVDSL, 100TX }
The type of the port media.

RS400
Ports 1 and 2 (Fibre) = 100FX
Ports 3 and 4 (Copper) = 100TX

RS900
Ports 7 and 8 (Fibre) = 100FX
Ports 1 to 6 (Copper) = 100TX

RS900G
Ports 9 and 10 (Fibre) = 1000X
Ports 1 and 8 (Copper) = 100TX

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 signal is not sent so that the link/activity LED will never be lit. You may want to disable a port for troubleshooting or to secure it from unauthorized connections.

(Assigned as per the network design)
Any port that is not in use can be disabled if unauthorised use is desired.

AutoN
Synopsis: { On, Off }
Default: On
Enable or disable IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results. 10Mbps and 100Mbps fibre optic media do not support auto-negotiation so these media must be explicitly configured to either half or full duplex. Full duplex

operation requires that both ends are configured as such or else severe frame loss will occur during heavy network traffic

Speed
Synopsis: { Auto, 10M, 100M, 1000M}
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 explicitly forced to this speed mode.
AUTO means advertise all supported speed modes.

All connected device ports are recommended to be set to 100M speed except for :-
RS900G Gigabit Fibre Port = 1000M
Westrace MK1 Ethernet Port = 10M.

Dupx
Synopsis: { Auto, Half, Full }
Default: Auto
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 explicitly forced to this duplex mode.
AUTO means advertise all supported duplex modes.

All connected device ports are recommended to be set to Full Dulplex except for :-
Westrace MK1 Ethernet Port = Half

FlowCtrl
Synopsis: { On, Off }
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 half-duplex it is accomplished using 'backpressure' where the switch simulates collisions causing the sending device to retry transmissions according to the Ethernet backoff algorithm. When the port is full-duplex it is accomplished using PAUSE frames which causes the sending device to stop transmitting for a certain period of time.

LFI
Synopsis: { Off }
Default: Off
Enabling Link-Fault-Indication (LFI) inhibits transmitting link integrity signal when the receive link has failed. This allows the device at 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.

Act on LinkDown
Synopsis: { Do nothing, Admin Disable }
Default: Do nothing
The action to be taken upon a port LinkDown event. Options include:
Do nothing – No action is taken
Admin Disable – The port state is disabled

Port Rate Limiting (ethPortRateLimitCfg)

Provides the ability to limit the rates of Broadcast, Multicast and Unicast traffic on each port.

Port
Synopsis: 1 to maximum port number
Default: 1
The port number as seen on the front plate silkscreen of the switch.

Ingress Limit
Synopsis: 62 to 256000 Kbps or { Disabled }
Default: 1000 Kbps
The rate at which received frames (of the type described by the ingress frames parameter) will start to be discarded by the switch.

Ingress Frames
Synopsis: { Broadcast, Bcast&Mcast, Bcast&Mcast&FloodUcast, Bcast&FloodUcast, FloodUcast, All }
Default: Broadcast
This parameter specifies the types of frames to rate-limit on this port. It applies only to received frames:
Broadcast - only broadcast frames
Bcast&Mcast – broadcast and multicast frames
Bcast&FloodUcast – broadcast and flooded unicast frames
Bcast&Mcast&FloodUcast – broadcast, multicast and flooded unicast frame
FloodUcast – only flooded unicast frames
ALL - all (multicast, broadcast and unicast) frames

Egress Limit
Synopsis: { Broadcast, Multicast, Mcast&FloodUcast, All }”>62 to 256000 Kbps or { Disabled }
Default: Disabled
The maximum rate at which the switch will transmit (multicast, broadcast and unicast) frames on this port. The switch will discard frames in order to meet this rate if required.

Port Mirroring (portMirrorCfg)

Configure port mirroring.

Generally not used. Only used for network diagnostics captures

Port Mirroring
Synopsis: { Disabled, Enabled }
Default: Disabled
Enabling port mirroring causes all frames received and/or transmitted by the source port to be transmitted out of the target port.

Source Port
Synopsis: 1 to 4
Default: 1
The port(s) being monitored.

Source Direction
Synopsis: { Egress and Ingress, Egress Only }
Default: Egress and Ingress
Specifies monitoring whether both egress and ingress traffics or only egress traffic of the source port.

Target Port
Synopsis: 1 to maximum port number
Default: 1
The port where a monitoring device should be connected.

Link Detection (ethLinkDetect)

Configure different options related to Ethernet link detection process.

Fast Link Detection
Synopsis: { Off, On, On_withPortGuard }
Default: On_withPortGuard
This parameter provides protection against faulty end devices generating an improper link integrity signal. When a faulty end device or a mis-matching fibre port is connected to the unit, a large number of continuous link state changes could be reported in a short period of time. These large number of bogus link state changes could render the system unresponsive as most, if not all, of the system resources are used to process the link state changes. This could in turn cause a serious network problem as the unit's RSTP process may not be able to run, thus allowing network loop to form.

Three different settings are available for this parameter:

ON_withPortGuard - This is the recommended setting. With this setting, an extended period (~2 minutes) of excessive link state changes reported by a port will prompt Port Guard feature to disable FAST LINK DETECTION on that port and raise an alarm. By disabling FAST LINK DETECTION on the problematic port, excessive link state changes can no longer consume substantial amount of system resources. However if FAST LINK DETECTION is disabled, the port will need a longer time to detect a link failure. This may result in a longer network recovery time of up to 2s. Once Port Guard disables FAST LINK DETECTION of a particular port, user can re-enable FAST LINK DETECTION on the port by clearing the alarm.

ON - In certain special cases where a prolonged excessive link state changes constitute a legitimate link operation, using this setting can prevent Port Guard from disabling FAST LINK DETECTION on the port in question. If excessive link state changes persist for more than 2 minutes, an alarm will be generated to warn user about the observed bouncing link. If the excessive link state changes condition is resolved later on, the alarm will be cleared automatically. Since this option does not disable FAST LINK DETECTION, a persistent bouncing link could continue affect the system in terms of response time. This setting should be used with caution.

OFF - Turning this parameter OFF will disable FAST LINK DETECTION completely. The switch will need a longer time to detect a link failure. This will result in a longer network recovery time of up to 2s.

Link Detection Time
Synopsis: 100 ms to 1000 ms
Default: 100 ms
The time that the link has to continuously stay up before the “link up” decision is made by the device.
(The device performs de-bouncing of Ethernet link detection to avoid multiple responses to an occasional link bouncing event, e.g. when a cable is shaking while being plugged-in or unplugged).

2.4 Spanning Tree

Bridge RSTP Parameters (rstpCfg)

Configure RSTP bridge level parameters.

State
Synopsis: { Disabled, Enabled }
Default: Enabled
Enable STP/RSTP/MSTP for the bridge globally. Note that STP/RSTP/MSTP is enabled on a port when it is enabled globally and along with enabling per port setting.

(Assigned as per the network design)
Ports not contained in ring should be disabled

Version Support
Synopsis: { STP, RSTP, MSTP }
Default: RSTP
Selects the version of Spanning Tree Protocol to support, either only STP or Rapid STP or Multiple STP.

Bridge Priority (Assigned as per the network design)
Synopsis: { 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49 152, 53248, 57344, 61440 }
Default: 32768
Bridge Priority provides a way to control the topology of the STP connected network. The desired Root and Designated bridges can be configured for a particular topology. The bridge with the lowest priority will become root. In the event of a failure of the root bridge, the bridge with the next lowest priority will then become root. Designated bridges that (for redundancy purposes) service a common LAN also use priority to determine which bridge is active. In this way careful selection of Bridge Priorities can establish the path of traffic flows in normal and abnormal conditions.

Hello Time
Synopsis: 1 s to 10 s
Default: 2 s
Time between configuration messages issued by the root bridge. Shorter hello times result in faster detection of topology changes at the expense of moderate increases in STP traffic.

Default used under general conditions but may be changed under design requirements

Max Age Time
Synopsis: 6 s to 40 s 28s
Default: 20 s
The time for which a configuration message remains valid after being issued by the root bridge. Configure this parameter with care when many tiers of bridges exist, or slow speed links (such as those used in WANs) are part of the network

Default used under general conditions but may be changed under design requirements

Transmit Count
Synopsis: 3 to 100
Default: 32
Maximum number of configuration messages on each port that may be sent in a special event (such as recovering from a failure or bringing up a new link). After the maximum number of messages is reached, RSTP will be limited to 1 message per second. Larger values allow the network to recover from failed links more quickly. If RSTP is being used in a ring architecture the transmit count should be larger than the number of switches in the ring.

Default used under general conditions but may be changed under design requirements

Forward Delay
Synopsis: 4 s to 30 s
Default: 15 s
The amount of time a bridge spends learning MAC addresses on a rising port before beginning to forward traffic. Lower values allow the port to reach the forwarding state more quickly, but at the expense of flooding unlearned addresses to all ports.

Max Hops
Synopsis: 6 to 40
Default: 20
This parameter is only relevant for MSTP - ignore it otherwise.
This parameter specifies the maximum possible bridge diameter inside an MST region. MSTP BPDUs propagating inside an MST region carry a time-to-live parameter decremented by every switch that propagates the BPDU. If the maximum number of hops inside the region exceeds the configured maximum, BPDUs may be discarded due to their time-to-live information.

Default used under general conditions but may be changed under design requirements

eRSTP Parameters (rstpEnhCfg)

To configure eRSTP

Max Network Diameter
Synopsis: { MaxAgeTime, 4*MaxAgeTime }
Default: 4*MaxAgeTime
The RSTP standard puts a limit on the maximum network size that can be controlled by the RSTP protocol. The network size is described by the term ‘maximum network diameter’, which is the number of switches that comprise the longest path that RSTP BPDUs have to traverse. The standard supported maximum network diameter is equal to the value of the ‘MaxAgeTime’ RSTP configuration parameter.
eRSTP offers an enhancement to RSTP which allows it to cover networks larger than ones defined by the standard.
This configuration parameter selects the maximum supported network size.

BPDU Guard Timeout
Synopsis: 1 to 86400 s or { Until reset, Don’t shutdown }
Default: Don't shutdown
The RSTP standard does not address network security. RSTP must process every received BPDU and take an appropriate action. This opens a way for an attacker to influence RSTP topology by injecting RSTP BPDUs into the network.
BPDU Guard is a feature that protects the network form BPDUs received by a port where RSTP capable devices are not expected to be attached. If a BPDU is received by a poer for which ‘Edge’ parameter is set to ‘TRUE’ or RSTP is disabled, the port will be shutdown for the time period specified by this parameter.
DON’T SHUTDOWN – BPDE Guard is disabled
UNTIL RESET – port will remain shutdown until the port reset command is issued by the user

Fast Root Failover
Synopsis: { On, On with standard root, Off }
Default: On
In mesh network topologies, the standard RSTP algorithm does not guarantee deterministic network recovery time in the case of a root switch failure. Such a recovery time is hard to

calculate and it can be different (and may be relatively long) for any given mesh topology.
This configuration parameter enables Siemens's enhancement to RSTP which detects a failure of the root switch and performs some extra RSTP processing steps, significantly reducing the netwok recovery time and making it deterministic.
The Fast Root Failover algorithm must be supported by all switches in the network, including the root, to guarantee optimal performance. However, it is not uncommon to assign the root role to a switches in the network. In other words, it is possible that the root might not support the Fast Root Failover algorithm. In such a scenario, a "relaxed" algorithm should be used, which tolerates the lack of support in the root switch.
These are supported configuration options:
Off – Fast Root Failover algorithm is disabled and hence a root switch failure may result in excessive connectivity recovery time.
On – Fast Root Failover is enabled and the most robust algorithm is used, which requires the appropriate support in the root switch.
On with standard root – Fast Root Failover is enabled but a "relaxed" algorithm is used, allowing the use of a standard switch in the root role.

IEEE802.1w Interoperability
Synopsis: { On, Off }
Default: On
The original RSTP protocol defined in the IEEE802.1w standard has minor differences from more recent, enhanced, standard(s). Those differences cause interoperability issues which, although they do not completely break RSTP operation, can lead to a longer recovery time from failures in the network.
eRSTP offers some enhancements to the protocol which make the switch fully interoperable with other vendors' switches, which may be running IEEE 802.1w RSTP. The enhancements do not affect interoperability with more recent RSTP editions.
This configuration parameter enables the aforementioned interoperability mode.

Cost Style
Synopsis: { STP (16 bit), RSTP (32 bit) }
Default: STP (16 bit)
This parameter selects the style of link costs to employ. STP uses 16-bit path costs based upon 1x10E9/link speed (4 for 1Gbps, 19 for 100 Mbps and 100 for 10 Mbps) whereas RSTP uses 32-bit costs based upon 2x10E13/link speed (20,000 for 1Gbps, 200,000 for 100 Mbps and 2,000,000 for 10 Mbps).Note that RSTP link costs are used only when the bridge version support is set to allow RSTP and the port does not migrate to STP.

Port RSTP Parameters (rstpPortCfg)

Configure RSTP port level parameters.

Port(s)
Synopsis: Any combination of numbers valid for this parameter
The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).

Enabled
Synopsis: { Disabled, Enabled }
Default: Enabled
Enabling STP activates the STP or RSTP protocol for this port as per the configuration in the STP Configuration menu. STP may be disabled for the port ONLY if the port does not attach to an STP

enabled bridge in any way. Failure to meet this requirement WILL result in an undetectable traffic loop in the network. A more desirable alternative rather than disabling the port is to leave STP enabled but to configure the port as an edge port. A good candidate for disabling STP would be a port that services a single host computer.

Priority
Synopsis: { 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 }
Default: 128
Selects the STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.

STP Cost
Synopsis: Auto to 65535 or { Auto }
Default: Auto
Selects the cost to use in cost calculations, when the Cost Style parameter is set to STP in the Bridge RSTP Parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to "auto" to use the standard STP port costs as negotiated (4 for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links).
For MSTP, this parameter applies to both external and internal path cost.

RSTP Cost (Assigned as per the network design)
Synopsis: Auto to 2147483647 or { Auto }
Default: Auto
Selects the cost to use in cost calculations, when the Cost Style parameter is set to RSTP in the Bridge RSTP Parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to "auto" to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links).
For MSTP, this parameter applies to both external and internal path cost.

Edge Port
Synopsis: { False, True, Auto }
Default: Auto
Edge ports are ports that do not participate in the Spanning Tree, but still send configuration messages. Edge ports transition directly to frame forwarding without any listening and learning delays. The MAC tables of Edge ports do not need to be flushed when topology changes occur in the STP network. Unlike an STP disabled port, accidentally connecting an edge port to another port in the spanning tree will result in a detectable loop. The "Edgeness" of the port will be switched off and the standard RSTP rules will apply (until the next link outage).

(Assigned as per the network design) AUTO NOT TO BE USED

PORTS NOT CONTAINED IN RING SHOULD BE SET TO TRUE

Point to Point
Synopsis: { False, True, Auto }
Default: Auto
RSTP uses a peer to peer protocol that provides for rapid transitioning on point-to-point links. This protocol is automatically turned off in situations where multiple STP bridges communicate over a shared (non point-to-point) LAN. The bridge will automatically take point-to-point to be true when the link is found to be operating full duplex. The point-to-point parameter allows this behaviour or overrides it, forcing point-to-point to be true or false. Force the parameter true when the port operates a point-to-point link but cannot run the link full duplex. Force the parameter false

when the port operates the link full duplex, but is still not point to point (e.g. a full duplex link to an unmanaged bridge that concentrates two other STP bridges).

(Assigned as per the network design) AUTO NOT TO BE USED

PORTS CONTAINED IN RING SHOULD BE SET TO TRUE

Restricted Role
Synopsis: True or False
Default: False
A Boolean value set by management. If TRUE causes the Port not to be selected as Root Port for the CIST or any MSTI, even it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter should be FALSE by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

Restricted TCN
Synopsis: True or False
Default: False
A Boolean value set by management. If TRUE causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter should be FALSE by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or MAC_Operational for the attached LANs transitions frequently.

2.5 VLAN’s

Global VLAN Parameters (vlanCfg)

Switch global VLAN configuration parameters.

VLAN-aware
Synopsis: { No, Yes }
Default: Yes
Set either VLAN-aware or VLAN-unaware mode of operation.

Ingress Filtering
Synopsis: { Disabled, Enabled }
Default: Enabled
Enables or disables VLAN ingress filtering on all ports When enabled, any tagged packet arriving at a port, which is not a member of a VLAN with which that packet is associated, is dropped. When disabled, packets are not dropped.

QinQ
Synopsis: { 0x8100, 0x88A8 }
Default: 0x8100
Selects an Ethertype to be used as the Tag Protocol Identifier (TPID) on VLAN QinQ ports when QinQ is enabled. Frames that ingress a VLAN QinQ port will be identified as outer VLAN tagged if the first Ethertype matches this value; an outer VLAN tag with the TPID field assigned to this value will be inserted to frames that egress a VLAN QinQ port.

Static VLANs (vlanStaticCfg)

Provides the ability to explicitly create and configure VLANs.
0 of 15 entries used.

As a minimum VLAN 3 shall be configured as in the following table.

VID	Name
3	Non-vital / Mgmt
21	Vital Axle Counters
22	Axle Counters Diag
31	Vital Interlocking

Additional VLANS May be assigned with appropriate network design

VID
Synopsis: 1 to 4094
Default: 1
The VLAN Identifier is used to identify the VLAN in tagged Ethernet frames according to IEEE 802.1Q.

May be assigned other than “1” with appropriate network design

VLAN Name
Synopsis: Any 19 characters
Default:
Provides a description of the VLAN purpose (for example, Engineering VLAN).

May be assigned with appropriate network design

Forbidden Ports
Synopsis: Any combination of numbers valid for this parameter
Default: None
Ports that are disallowed to be members of the VLAN.
Examples:
None – all ports of the switch are allowed to be members of the VLAN
2,4-6,8 – all ports except ports 2,4,5,6 and 8 are allowed to be members of the VLAN

IGMP
Synopsis: { On, Off }
Default: Off
Enable or disable IGMP Snooping on the VLAN.

MSTI
Synopsis: 0 to 16
Default: 0
This parameter is only valid for Multiple Spanning Tree Protocol (MSTP) and has no effect, if MSTP is not used.
The parameter specifies Multiple Spanning Tree Instance (MSTI) the VLAN should be mapped to.

Port VLAN Parameters (vlanPortCfg)

VLAN configuration parameters for a specific port.

Port(s)
Synopsis: Any combination of numbers valid for this parameter
The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).

May be assigned with appropriate network design

Type
Synopsis: { Edge, Trunk, PVLANEdge, QinQ }
Default: Edge
This parameter specifies how the port determines its membership in VLANs. There are few types of ports:
EDGE - the port is only a member of one VLAN (its native VLAN specified by the 'PVID' parameter).
PVLANEdge - the port does not forward traffic to other PVLANedge ports within the same VLAN.
TRUNK - the port is automatically a member of all configured VLANs. Frames transmitted out of the port on all VLANs except the port's native VLAN will be always tagged. It can also be configured to use GVRP for automatic VLAN configuration.
QinQ - Ports are NOT to be configured as Qin - the port is a trunk port using double-VLAN tagging, or nested VLANs. An extra VLAN tag is always added to all frames egressing this port, VID in the added extra tag is the PVID of the frame's ingress port. VLAN tag is always stripped from frames ingressing this port.

May be assigned with appropriate network design

PVID
Synopsis: 1 to 4094

Default: 1
The Port VLAN Identifier specifies 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.
Modify this parameter with care! By default, the switch is programmed to use VLAN 1 for management and every port on the switch is programmed to use VLAN 1. If you modify a switch port to use a VLAN other than the management VLAN, devices on that port will not be able to manage the switch.

May be assigned with appropriate network design

PVID Format
Synopsis: { Untagged, Tagged }
Default: Untagged ALL edge ports shall be configured as Untagged
Specifies whether frames transmitted out of the port on its native VLAN (specified by the 'PVID' parameter) will be tagged or untagged.

May be assigned with appropriate network design

GVRP
Synopsis: { Disabled, Adv Only, Adv&Learn }
Default: Disabled
Configures GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes:

DISABLED - the port is not capable of any GVRP processing.

ADVERTISE ONLY - the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs.

ADVERTISE & LEARN - the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.

Only Trunk ports are GVRP capable.

2.6 CoS NOT USED

Global CoS Parameters (cosCfg)

Switch global Classes of Service configuration parameters.

CoS Weighting
Synopsis: { 8:4:2:1, Strict }
Default: 8:4:2:1
During traffic bursts, frames queued in the switch pending transmission on a port may have different CoS priorities.
This parameter specifies weighting algorithm for transmitting different priority CoS frames.
Examples:
8:4:2:1 - 8 Critical, 4 High, 2 Medium and 1 Normal priority CoS frame
Strict - lower priority CoS frames will be only transmitted after all higher priority CoS frames have been transmitted.

Port CoS Parameters (cosPortCfg)

Classes of Service configuration parameters for specific port.

Port(s)
Synopsis: Any combination of numbers valid for this parameter
The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).

Default CoS
Synopsis: { Normal, Medium, High, Crit }
Default: Normal
This parameter allows to prioritize frames received on this port that are not prioritized based on the frames contents (e.g. priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).

Inspect TOS
Synopsis: { No, Yes }
Default: No
This parameters enables or disables parsing of the Type-Of-Service (TOS) field in the IP header of the received frames to determine what Class of Service they should be assigned. When TOS parsing is enabled the switch will use the Differentiated Services bits in the TOS field.

Priority to CoS Mapping (cosPriCfg)

Map each IEEE 802.1p priority value to the switch Class of Service.

Priority
Synopsis: 0 to 7
Default: 0
Value of the IEEE 802.1p priority.

CoS
Synopsis: { Normal, Medium, High, Crit }
Default: Normal
CoS assigned to received tagged frames with the specified IEEE 802.1p priority value.

DSCP to CoS Mapping (cosDscpCfg)

Map each Differentiated Services Code Point (DSCP) in the Type-Of-Service (TOS) field in the headers of the received IP packets to the switch Class of Service.

DSCP
Synopsis: 0 to 63
Default: 0
Differentiated Services Code Point (DSCP) - a value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header.

CoS
Synopsis: { Normal, Medium, High, Crit }
Default: Normal
Class of Service assigned to received frames with the specified DSCP.

2.7 Multicast Filtering

IGMP Parameters (mcastIgmpCfg)

Provides the ability to configure IGMP Snooping parameters.

Mode
Synopsis: { Passive, Active }
Default: Passive
Specifies IGMP mode:

PASSIVE - the switch passively snoops IGMP traffic and never sends IGMP queries

ACTIVE - the switch generates IGMP queries, if no queries from a better candidate for being the querier are detected for a while.

IGMP Version
Synopsis: { v2, v3 }
Default: v2
Specifies the configured IGMP version on the switch. Options include:

v2 – Sets the IGMP version to version 2. When selected for a snooping switch, all IGMP reports and queries greater than v2 are forwarded, but not added to the IGMP Multicast Forwarding table.

v3 – Sets the IGMP version to version 3. General queries are generated in IGMPv3 format, all versions of IGMP messages are processed by the switch, and traffic is pruned based on multicast group address only.

Query Interval
Synopsis: 10 s to 3600 s
Default: 60 s
The time interval between IGMP queries generated by the switch.
NOTE: This parameter also affects the Group Membership Interval (i.e. the group subscriber aging time), therefore, it takes effect even in PASSIVE mode.

Router Ports
Synopsis: Any combination of numbers valid for this parameter

Default: None
This parameter specifies ports that connect to multicast routers. If you do not configure known router ports, the switch may be able to detect them, however it is advisable to pre-configure them.

Router Forwarding
Synopsis: { On, Off }
Default: On
This parameter specifies whether multicast streams will always be forwarded to multicast routers.

RSTP Flooding
Synopsis: { On, Off }
Default: Off
This parameter specifies whether multicast streams will be flooded out of all RSTP non-edge ports upon topology change detection. Such flooding is desirable, if guaranteed multicast stream delivery after topology change is most important.

Port GMRP Parameters (gmrpPortCfg)

GMRP configuration parameters for a specific port.

Port(s)
Synopsis: Any combination of numbers valid for this parameter
The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).

GMRP
Synopsis: { Disabled, Adv Only, Adv&Learn }
Default: Disabled
Configures GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes:

DISABLED - the port is not capable of any GMRP processing.

ADVERTISE ONLY - the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses.

ADVERTISE & LEARN - the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.

Static Multicast Groups (mcastStaticGroups)

Configure multicast groups with statically assigned ports.
0 of 256 entries used.

MAC Address
Synopsis: ##-##-##-##-##-## where ## ranges 0 to FF
Default: 00-00-00-00-00-00
Multicast group MAC address.

ENTRIES for all Firmware versions from 3-7-x onwards (See Section 5 Firmware)

01-00-0C-00-00-00

01-00-0C-CC-CC-CC

AB-00-00-02-00-00

VID
Synopsis: 1 to 4094

Default: 1
VLAN Identifier of the VLAN upon which the multicast group operates.

CoS
Synopsis: { Normal, Medium, High, Crit }
Default: Normal
Specifies what Class Of Service is assigned to the multicast group frames

Ports
Synopsis: Any combination of numbers valid for this parameter
Default: None
Ports to which the multicast group traffic is forwarded.

2.8 MAC Address

MAC Address Learning Options (macAddrCfg)

Configure MAC address forwarding database options such as the MAC address aging time.

Aging Time
Synopsis: 15 s to 800 s
Default: 300 s
This parameter configures the time a learned MAC address is held before being aged out.

Age Upon Link Loss
Synopsis: { No, Yes }
Default: Yes
When link failure (and potentially a topology change) occurs the switch may have some MAC addresses previously learned on the failed port. As long as those addresses are not aged-out the switch will still be forwarding traffic to that port, thus preventing that traffic from reaching its destination via the new network topology. This parameter allows to age-out all MAC addresses learned on a failed port immediately upon link failure detection.

Static MAC Address Table (macAddrStaticCfg) NOT USED

Configure static and prioritized unicast MAC addresses.
0 of 64 entries used.

MAC Address
Synopsis: ##-##-##-##-##-## where ## ranges 0 to FF
Default: 00-00-00-00-00-00
MAC address that is to be statically configured.

VID
Synopsis: 1 to 4094
Default: 1
VLAN Identifier of the VLAN upon which the MAC address operates.

Port
Synopsis: 1 to 4
Default: 1
Enter the port number upon which the device with this address is located.

CoS
Synopsis: { Normal, Medium, High, Crit }
Default: Normal
Set this parameter to prioritize the traffic for specified address.

2.9 Network Discovery

Global LLDP Parameters (lldpGlobalCfg)

Configure Global LLDP Parameters

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 s 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 s 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 s 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)

Port LLDP Parameters (lldpPortCfg)

Configure Port LLDP Parameters

Port
Synopsis: 1 to 4
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.

Notifications
Synopsis: { Disabled, Enabled }
Default: Disabled

Disabling notifications will prevent sending notifications and generating alarms for particular port from the LLDP agent.

RCDP Parameters (rcdpCfg)

Provide the ability to configure settings for Ruggedcom Discovery Protocol(RCDP).

RCDP Discovery
Synopsis: { Disabled, Enabled, Get Only }
Default: Enabled
Disabled – Disables read and write access
Get Only – Enables only read access
Enabled – Enables read and write access

3 Alarms and Alarm Settings

Alarms (alarmsCfg)

Provide the ability to configure per alarm settings.
21 of 512 entries used.

Name
Synopsis: Any 34 characters
Default: sys_alarm
The name of this alarm.

Level
Synopsis: { EMRG, ALRT, CRIT, ERRO, WARN, NOTE, INFO, DEBG }
Severity level of alarm:
EMERG - Device has had a serious failure that caused a system reboot
ALERT - Device has had a serious failure that however didn't cause a system reboot
CRITICAL - Device has a serious unrecoverable problem
ERROR - 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 Alarms Table.

Dependent on Setting in Section 4 ALARM SETTINGS

Trap
Synopsis: { On, Off }
Default: Off
Enables sending SNMP trap for this alarm.

Log
Synopsis: { On, Off }
Default: Off
Enables logging occurrence of this alarm in syslog.txt.

Dependent on Setting in Section 4 ALARM SETTINGS

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 as well.

Dependent on Setting in Section 4 ALARM SETTINGS

Refresh Time
Synopsis: 0 s to 60 s
Default: 60 s
Refreshing time for this alarm.

3.1 Types of Alarms:

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.

This could mask an ongoing problem!

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. RMON generated alarms are passive.

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.

These alarms will be indicated through the Train Control System. Therefore careful consideration needs to be made in which alarms are enabled so that superfluous alarms are not displayed.

Note

Alarms are volatile in nature. All alarms (active and passive) are cleared at start up.

3.2 Recommended Configuration

The recommended Alarm configuration is based on suitability of alarms for the maintainer and operator. There are two forms of Ruggedcom alarms are conveyed. These are through Relay and SNMP. Relay is generally conveyed to the Train Control System. SNMP can be conveyed to other alarm management systems. Relay method should convey most critical alarms which would impact on the system. All other alarms should be logged and conveyed through other methods.

Alarms (alarmsCfg)

Name - **The name of this alarm.**

Latch - Enables latching occurrence of this alarm in Alarms Table.
All OFF except “LINK UP / DOWN”

Trap - Enables sending SNMP trap for this alarm.
All OFF – This is not used.

Log - Enables logging occurrence of this alarm in syslog.txt.
All ON – Log all values in syslog for diagnosis.

LED&Relay - Enables LED and fail safe relay control for this alarm.
If latching is not enabled, this field will remain disabled as well.
All OFF except “LINK UP / DOWN”

Refresh Time - Refreshing time for this alarm.
All 60 s

Recommended Settings Table for Alarms

Name	Latch	Trap	Log	LED&Relay	Refresh Time
BPDU Guard activated	OFF	OFF	ON	OFF	60 s
Can't create more mcast IP groups	OFF	OFF	ON	OFF	60 s
Clock manager alarm	OFF	OFF	ON	OFF	60 s
Configuration changed	OFF	OFF	ON	OFF	60 s
Excessive failed login attempts	OFF	OFF	ON	OFF	60 s
GMRP cannot learn more addresses	OFF	OFF	ON	OFF	60 s
GVRP cannot learn more VLANs	OFF	OFF	ON	OFF	60 s
Invalid configuration	OFF	OFF	ON	OFF	60 s
Link up/down	ON	OFF	ON	ON	60 s
Login information	OFF	OFF	ON	OFF	60 s
MAC address not learned	OFF	OFF	ON	OFF	60 s
Mcast CPU filtering table full	OFF	OFF	ON	OFF	60 s
New STP root	OFF	OFF	ON	OFF	60 s
NTP server unreachable	OFF	OFF	ON	OFF	60 s
Received looped back BPDU	OFF	OFF	ON	OFF	60 s
Serial comm blocked, TCP flwctrld	OFF	OFF	ON	OFF	60 s
SNMP authentication failed	OFF	OFF	ON	OFF	60 s
STP events	OFF	OFF	ON	OFF	60 s
STP topology change	OFF	OFF	ON	OFF	60 s
TACACS response invalid	OFF	OFF	ON	OFF	60 s
Unknown route for serial protocol	OFF	OFF	ON	OFF	60 s

4 Firmware

Firmware Versions MUST be ROS v4.3.5 Revision

Firmware Versions from ROS v3.7.x onwards must have Static Multicast Groups (Section 3.7) configured as below

MAC Address

Synopsis: ##-##-##-##-##-## where ## ranges 0 to FF

01-00-0C-00-00-00

01-00-0C-CC-CC-CC

AB-00-00-02-00-00

VID

VLAN Identifier of the VLAN upon which the multicast group operates.

As per Section 3.5 (VLANs)

CoS

Specifies what Class Of Service is assigned to the multicast group frames

Normal

Ports

Ports to which the multicast group traffic is forwarded.

None

5 Bootware

Bootware Versions shall be compatible with the firmware version.

6 Addition Requirements and Limitation

[1]. Ruggedcom RS400, RS900 and RS900G Series switches shall operate from same Rugged Operating System (ROS).

[2]. The inclusion of RS400, RS900 and RS900G Series switch within the network shall be used in conjunction with a detailed Network design.

[3]. The inclusion of RS400, RS900 and RS900G Series switch within the network is primarily directed for use with Westrace MkII interlocking, Microlok Interlockings, VHLC and EC5 Interlockings using a fibre redundant ring system within ARTC but it is not necessarily limited to that use.

[4]. The utilisation of RS900 and RS900G series switch within a network containing RS400 components would be acceptable where it would be more efficient and cost effective to install the RS900 and RS900G series switch.

[5]. The RS400, RS900 and RS900G Series switches shall use the approved Firmware version, detailed in Section 0 Firmware.

[6]. The RS400, RS900 and RS900G Series switches shall use the Compatible Bootware version, detailed in Section 5 Bootware.

[7]. Configurations settings contained within this document shall be used in configuration of RS400, RS900 and RS900G series switch. In case of discrepancy contact ARTC standards standards@artc.com.au

[8]. Inclusion of 5db or 10db attenuators may be considered with short distances, less than 100 metres over fibre ports between two RuggedCom units. This is to minimise damage and to ensure reliability of RuggedCom units.