

GE Vernova

GE Vernova Reason S20

Industrial Managed Ethernet Switches



Technical Manual

S20 Platform Hardware Version: C

S20 Platform Software Version: 07

Publication Reference: GE_Reason_S20_TM_EN_5.1_HWC



GE VERNOVA

TABLE OF CONTENTS

Chapter 1: Introduction	12
1.1 Foreword	12
1.2 Target Audience	12
1.3 Acronyms and Abbreviations	12
2 Product Scope	16
3 Functional Overview	16
4 Key Features	19
5 Compliance	20
5.1 Standard Compliance	20
5.2 Product Safety	21
6 Cyber Security Disclaimer	21
7 S20 Order Code	23
Chapter 2: Safety Information	25
1 Health and Safety	25
2 Symbols	25
3 Installation, Commissioning and Servicing	26
3.1 Lifting Hazards	26
3.2 Electrical Hazards	26
3.3 Fusing and Insulation Requirements	28
3.4 Equipment Connections	29
3.5 Pre-energization Checklist	30
3.6 Upgrading/Servicing	31
4 Decommissioning and Disposal	31
Chapter 3: Installation Guide	32
1 Mechanical Design	32
2 Unpacking	32
3 Rack Mounting	33
4 Power Connections	33
5 Ground Connection	35
6 Communications Ports	35
6.1 Electrical Ethernet Ports (RJ45)	35
6.2 SFP Pluggable Transceiver	35
7 Dry Contact Relay (Failsafe)	36
8 Energizing	37

9	Preventive Maintenance	37
9.1	Preventive Actions	37
Chapter 4: Interfaces & Operation		39
1	Communication Interfaces	39
1.1	Local Interface – USB	39
1.2	Remote Interface – Ethernet	40
2	Accessing Reason S20	41
2.1	Factory Default Parameters	41
2.2	First Access	42
2.3	Commands from CLI	44
3	Signalizing LEDs	45
4	Reboot Button	46
5	Factory Reset	46
Chapter 5: Functions & Configuration		47
1	Configuration overview	47
2	System Settings	48
2.1	System Information	48
2.2	IP (Internet Protocol)	48
2.3	NTP Synchronization	51
2.4	Time Configuration	54
2.5	Log	55
3	Ports Settings	56
4	Switch Security	59
4.1	User & Password	59
4.2	User Privilege Level	60
4.3	Authentication Methods	61
4.4	Telnet/SSH Protocols	63
4.5	HTTP/HTTPS Protocols	64
4.6	Access Management	66
5	Simple Network Management Protocol (SNMP)	67
5.1	SNMP Fundamentals	67
5.2	SNMP Configuration	69
6	Aggregation Settings	73
6.1	Static Aggregation Configuration	76
6.2	Link Aggregation Control Protocol (LACP) Settings	77
7	Loop Protection	78
7.1	Loop Fundamentals	78
7.2	Loop Protection	79

7.3	Loop Protection Configuration	80
8	Spanning Tree Protocol (STP)	81
8.1	Spanning Fundamentals	81
8.2	Bridge Settings	91
8.3	MSTI Mapping Configuration	93
8.4	MSTI Priorities Configuration	93
8.5	CIST Ports Configuration	94
8.6	MSTI Ports Configuration	97
9	IP Multicast (IPMC)	97
9.1	IPMC Profile	99
9.2	IGMP Snooping	101
9.3	MLD Snooping	106
10	MAC Table	107
10.1	MAC Table Fundamentals	107
10.2	MAC Table Configuration	110
11	Virtual LAN (VLAN)	111
11.1	Legacy LAN Technology	111
11.2	Virtual LAN Basics	113
11.3	LAN in Modern Power System Communication	115
11.4	IEEE 802.1Q Switch operation concepts	117
11.5	Reason S20 Operation	118
11.6	VLAN Configuration	120
12	Quality of Service (QoS)	124
12.1	QoS Basics	125
12.2	Port Classification	132
12.3	Port Policing	133
12.4	Queue Policing	134
12.5	Port Scheduler	134
12.6	Port Shaping	136
12.7	Port Tag Remarking	137
12.8	Port DSCP	138
12.9	DSCP-Based QoS	139
12.10	DSCP Translation	139
12.11	DSCP Classification	140
12.12	QoS Control List	140
12.13	Storm Policing	145
12.14	WRED	146
13	Mirroring	147
13.1	Mirroring Basics	147
13.2	Mirroring Configuration	149
14	Precision Time Protocol (PTP) - IEEE 1588v2	151

14.1	Precision Time Protocol (PTP) Functional	151
14.2	PTP in GE Reason S20	153
15	Routing Information Protocol (RIP)	155
15.1	RIP Basics	155
15.2	RIP Configuration	156
15.3	Command Line Interface (CLI)	157
16	Open Shortest Path First (OSPF)	159
16.1	OSPF Basics	159
16.2	OSPF Configuration	159
16.3	Command Line Interface (CLI)	161
17	Virtual Router Redundancy Protocol (VRRP)	162
17.1	VRRP Basics	162
17.2	VRRP Configuration	163
17.3	Command Line Interface (CLI)	163
18	Failsafe Alarm	164
19	DDM Interface (DDMI)	167
20	Application Examples	168
20.1	Configuring VLANs in a Digital Substation Network	168
20.2	RSTP Configuring in a Ring Network Topology	172
20.3	PTP Transparent Clock	173
Chapter 6: Web Interface Monitoring		177
1	System Management	177
2	Ports	179
3	Security	181
4	Link Aggregation Control Protocol (LACP)	183
5	Loop Protection	184
6	Spanning Tree	184
7	IPMC	186
8	MAC Table	188
9	VLAN	189
10	PTP	189
Chapter 7: Maintenance & Troubleshooting		191
1	Network Diagnostics	191
1.1	Ping	191
1.2	Ping6	192
1.3	VeriPHY	192
2	Maintenance	193

2.1	Restart Device	193
2.2	Factory Defaults	194
2.3	Software Upload	194
2.4	License	195
2.5	Configuration	195
3	Troubleshooting	197
4	Equipment Return	200
5	Instructions for Equipment Repair Service	200
Chapter 8: Technical Specifications		202
<hr/>		
1	General Switching Characteristics	202
2	Ethernet Communication	202
3	USB Communication	202
4	Time Synchronization	203
5	Networking Standards Supported	203
6	Networking RFC Standards	204
7	RJ45 Ethernet (10/100/1000 Mbps) Ports	205
8	Optical Transceivers (100/1000 Mbps)	206
9	Power Supply	206
10	Failsafe Relay	206
11	Operating/Storage Environment	207
12	Physical Characteristics	207
13	Safety Compliance	208
14	Environmental Tests	209
15	EMC Tests	211

LIST OF FIGURES

Figure 1: S20 mechanical design	32
Figure 2: Rack Mounting design	33
Figure 3: Power Supply connector	34
Figure 4: SFP transceiver	36
Figure 5: Failsafe form C dry-contact relay	36
Figure 6: B-type USB connector	40
Figure 7: Example of HTTP or HTTPS first screen	40
Figure 8: Web Interface Search bar, logout and info	41
Figure 9: Putty configuration for SSH access	43
Figure 10: Local HMI LEDs indicators	45
Figure 11: Reboot button	46
Figure 12: IP routing example	51
Figure 13: NTP Time Protocol mechanism	52
Figure 14: NTP Syslog Message Basics	55
Figure 15: Ports at a Transparent Bridge	57
Figure 16: List of group to be classified with privilege levels (default config)	61
Figure 17: Example of SNMP management architecture	68
Figure 18: Comparison between common and aggregated links speed	74
Figure 19: Link failure behaviour of an aggregated link	75
Figure 20: Load balancing in aggregated links	76
Figure 21: Bridge Loop	78
Figure 22: Usage situations for Loop Protection	79
Figure 23: BPDU Packet	82
Figure 24: Ring topology LAN and possible paths for data traffic from IED A to B	82
Figure 25: Example of a loop-topology showing bridge	83
Figure 26: Logical topology after the Spanning Tree protocol was executed	84
Figure 27: Port states in the Spanning Tree Protocol	84
Figure 28: STP protocol mechanism and maximum port changing time	85
Figure 29: Port states when STP protocol is used in a ring physical topology	86
Figure 30: Failure on the designated link of the Spanning tree	86
Figure 31: Reconfigured topology after a designated link failure	86
Figure 32: RSTP protocol mechanism	87
Figure 33: RSTP port status in a loop topology	88
Figure 34: RSTP edge and trunk ports	88
Figure 35: BPDU flag field at RSTP protocol	89

Figure 36: MSTP regions and legacy RSTP LAN connection	90
Figure 37: CIST roots an MSTP regions and legacy RSTP LAN	90
Figure 38: MSTP regions behaviour using RSTP protocol	90
Figure 39: Network fault recovery using GE Reason S20s	91
Figure 40: Unicast and Broadcast communication	98
Figure 41: Multicast communication	99
Figure 42: IGMP protocol mechanism	102
Figure 43: IGMP Snooping at a given LAN	103
Figure 44: Ethernet frame	108
Figure 45: Address a table at a given Switch	109
Figure 46: Forwarding traffic in an Ethernet switch	109
Figure 47: LAN access restriction with MAC address configuration	110
Figure 48: Different LAN from different departments	112
Figure 49: Addition of new hosts to the legacy VLAN-unaware equipment	112
Figure 50: Adding new VLAN-aware hosts	113
Figure 51: VLAN segregation in different departments	114
Figure 52: 802.1Q Ethernet frame	114
Figure 53: Typical topology in power system communication environment	116
Figure 54: Logical topology of typical power system communication environment	116
Figure 55: Traffic flow inside an 802.1Q switch	117
Figure 56: Traffic in an oversized	125
Figure 57: Network with prioritization of traffic	126
Figure 58: CoS bits inside and 802.1Q frame	126
Figure 59: IP Header frame and Differentiated Service Code Point explained	128
Figure 60: CoS queues and remarking functions	129
Figure 61: DSCP queues and translation functions	130
Figure 62: DPL level usage	147
Figure 63: Port Mirroring Being Executed by a Switch	147
Figure 64: Port Mirroring in One Switch	148
Figure 65: Port Mirroring in Many Switch	148
Figure 66: Data Monitor Flow Network	149
Figure 67: PTP protocol mechanism	152
Figure 68: Led/Alarm operation example 1	165
Figure 69: Led/Alarm operation example 2	165
Figure 70: Led/Alarm operation example 3	165
Figure 71: SFP DDM monitoring	168

Figure 72: Topology to be configured in a VLAN environment	168
Figure 73: Topology to be configured in a RSTP environment	172
Figure 74: Topology to be configured in a PTP environment	174
Figure 75: S20 dimensions	208

LIST OF TABLES

Table 1: Terminal description from Power Connection	34
Table 2: LEDs color description	45
Table 3: Spanning cost range recommendation	83
Table 4: Port State behavior using STP protocol	85
Table 5: Port State behavior using RSTP protocol	87
Table 6: CoS Traffic Priority	127
Table 7: CoS classification as recommended by IEC 61850-90-4	127
Table 8: General Switching Characteristics	202
Table 9: Ethernet Communication Characteristics	202
Table 10: USB Communication Characteristics	202
Table 11: Time Synchronization Characteristics	203
Table 12: Networking Standards supported	203
Table 13: Networking Request for Comments (RFC) Standards	204
Table 14: RJ45 Ethernet Ports specification	205
Table 15: Optical Transceivers specification	206
Table 16: Power Supply specification	206
Table 17: Failsafe Relay specification	206
Table 18: Operating/Storage Environment	207
Table 19: Physical Characteristics	207
Table 20: Safety Tests	208
Table 21: Climatic Tests	209
Table 22: Mechanic Tests	209
Table 23: EMC – Emission tests	211
Table 24: EMC – Immunity tests	211

GE Reason S20

Industrial Managed Ethernet Switch

Chapter 1: Introduction

This chapter provides some general information about the technical manual and an introduction to the device(s) described in this technical manual.

1.1 Foreword

This technical manual provides a functional and technical description of GE Reason S20, as well as a comprehensive set of instructions for using the device. The level at which this manual is written assumes that you are already familiar with protection engineering and have experience in this discipline. The description of principles and theory is limited to that which is necessary to understand the product.

We have attempted to make this manual as accurate, comprehensive and user-friendly as possible. However, we cannot guarantee that it is free from errors. Nor can we state that it cannot be improved. We would therefore be very pleased to hear from you if you discover any errors or have any suggestions for improvement. Our policy is to provide the information necessary to help you safely specify, engineer, install, commission, maintain, and eventually dispose of this product. We consider that this manual provides the necessary information, but if you consider that more details are needed, please contact us.

All feedback should be sent to our contact center via the following URL:

<https://www.gevernova.com/grid-solutions/contact>

1.2 Target Audience

This manual has been designed for all professionals charged with installing, commissioning, maintaining, troubleshooting, or operating any of the products within the specified product range. This includes installation and commissioning personnel who will be responsible for operating the product. The level at which this manual is written assumes that installation and commissioning personnel have knowledge of handling electronic equipment and a thorough knowledge of Ethernet switches and associated equipment.

1.3 Acronyms and Abbreviations

BC	Boundary Clock
BPDU	Bridge Protocol Data Unit

CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CIST	Common Internal Spanning Tree
CPU	Central Processing Unit
CoS	Class-of-Service
CLI	Command Line Interface
IEC TR 61850-90-4	Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines
UTC	Universal Time Coordinated
DDM	Digital Diagnostics Monitoring
DEI	Drop Eligible Indicator
DST	Daylight Saving Time
DSCP	Differentiated Services Code Point
DNS	Domain Name Server
DHCP	Dynamic Host Configuration Protocol
DPL	Drop Precedence Level
EMC	Electromagnetic compatibility
E2E	End-to-end
ECN	Explicit Congestion Notification
FCS	Frame Check Sequence
FDDI	Fixed Distributed Data Interface
FE	Fast Ethernet
Gbps	Gigabits per second
GE	General Electrics (if referring to Reason S20), or Gigabit Ethernet (if referring to RJ45 Ethernet port)
GPS	Global Positioning System
GMC	Grandmaster Clock
HRC	High Rupture Capacity
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
GOOSE	IEC 61850 - Generic Object Oriented Substation Event
SV	IEC 61850 - Sampled Values
IEC 61850-9-2LE	Implementation guideline for Digital Interface to Instrument Transformers using IEC 61850-9-2
IEEE	Institute of Electrical and Electronics Engineers

IED	Intelligent Electronic Device
IEC	International Electrotechnical Commission
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPMC	IP Multicast
LACP	Link Aggregation Control Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
LAN	Local Area Network
LVD	Low Voltage Directive
MIB	Management Information Base, used by SNMP protocol
MMS	Manufacturing Message Specification
MAC	Media Access Control
Mbps	megabits per second
MCB	Miniature Circuit Breaker
MLD	Multicast Listener Discovery
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol (IEEE 802.1Q)
NTP	Network Time Protocol
NC	Normally Close
NO	Normally Open
OSI	Open Systems Interconnection model
OSPF	Open Shortest Path First
P2P	Peer-to-peer
PPE	Personal Protective Equipment
PDC	Phasor Data Concentrator
PDU	Protocol Data Units
PMU	Phasor Measurement Unit
PVID	Port VLAN Identifier
PTP	Precision Time Protocol (IEEE 1588)
PCP	Priority Code Point
PCT	Protective Conductor Terminal
PPS	Pulse per second

QCE	QoS Control Entry
QCL	QoS Control List
QoS	Quality-of-Service
R&TTE	Radio and Telecommunications Terminal Equipment
RSTP	Rapid Spanning Tree Protocol (IEEE 802.1D)
RADIUS	Remote Authentication Dial In User Service
RMON	Remote Network Monitoring
RIP	Routing Information Protocol
RFC	Request for Comments
SFP	Small-form Pluggable
SSH	Secure Shell
SSL	Secure Sockets Layer
VLAN ID	See VID
VRRP	Virtual Routing Redundancy Protocol
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol (IEEE 802.1D)
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TC	Transparent Clock
ToS	Type-of-Service
USB	Universal Serial Bus
UTP	Unshielded twisted pair
UDP	User Datagram Protocol
VLAN	Virtual LAN (IEEE 802.1Q)
VID	VLAN Identifier
WRED	Weighted Random Early Detection
WAMS	Wide Area Monitoring System

2 Product Scope

The GE Reason S20 managed Ethernet switch range is designed for harsh environments, such as power systems and industry applications, providing all elements needed in a IEC 61850 digital substation network, including mandatory IEEE 1588v2 (PTP). Using Reason S20, packet switching between IEDs is flexible, reliable and robust, even in situations where routing is necessary.

Reason S20 can perform traffic isolation of Sampled Values (IEC 61850-9-2LE), GOOSE messages, PTP synchronizing protocol and other messages using virtual LANs (VLANs). Switch traffic and ports monitoring is performed using the SNMP protocol, and loop-based topologies, such as ring topology, can be monitored and reconfigured using the RSTP (IEEE 802.1D) protocol.

Packet switched transmission in the switches is totally done by hardware, which ensures agility and maximum reliability even when interconnecting IEDs to distinct interfaces and speeds.

The switches configuration may be done through interactive mode of text commands (SSH and Telnet) or in a friendly graphic environment (HTTP or HTTPS) with native or remote authentication (RADIUS and TACACS+).

Statistical data collection can be obtained using SNMP v2/v3 protocol, with possibility of PulseNet integration as a Network Management Software (NMS). Communication interfaces are the Ethernet port or a dedicated USB-2.0 port.

Critical applications can benefit from the optional redundant power supply for even greater uptime and reliability. A dry-contact relay is available in Reason S20 to indicate a failsafe alarm to the supervisory system when an interface communication becomes unavailable or the equipment is missing of its power supplies.

3 Functional Overview

S2020 model

S2020 is the most cost-effective choice, offering a high density of Ethernet ports in a 1U form factor for easy rack mounting. This model supports up to 5 modules with 4 ports each and allows configurations with up to 20 fast Ethernet ports (100 Mbps), or up to 4 gigabit ports plus 16 fast Ethernet ports.

- Up to 5 modules of 4 Ethernet ports each;
- 1 module may either Gigabit or Fast Ethernet speed, the remaining 4 must be Fast Ethernet.
- Gigabit/Fast Ethernet modules are available in RJ45 copper or SFP ports;
- Copper interface modules consist of RJ45 (Cat5e) connectors for 10/100BASE-TX or 10/100/1000BASE-TX with auto-negotiation and automatic treatment of polarity inversion (HP Auto-MDIX);

- SFP Optic interfaces with LC connectors, been multimode for short distances and single mode for distances up to 120 km;
- SFP RJ45 10/100BASE-TX/1000BASE-T interfaces;
- Layer 3 functions and IEEE 1588v2 PTP may be upgraded via a licensing file.

S2024 model

S2024 is the premium model, offering full gigabit Ethernet switch functionality. This model supports up to 24 ports, provided by 6 interface modules with 4 ports each. The 1U mechanical design is identical to the S2020 model.

- Up to 6 Gigabit modules of 4 Ethernet ports each;
- Gigabit/Fast Ethernet modules are available in RJ45 copper or SFP ports;
- Copper interface modules consist of RJ45 (Cat5e) connectors for 10/100BASE-TX or 10/100/1000BASE-TX with auto-negotiation and automatic treatment of polarity inversion (HP Auto-MDIX);
- SFP Optic interfaces with LC connectors, been multimode for short distances and single mode for distances up to 120 km;
- SFP RJ45 10/100BASE-TX/1000BASE-T interfaces;
- Layer 3 functions and IEEE 1588v2 PTP may be upgraded via a licensing file.

Time Synchronization

- S20 switches are adequate to IEEE 1588 v2 standard, by licensing, in all ports;
- Operates as IEEE 1588v2 transparent (TC) or boundary (BC) clock;
- Operation as NTP client.
- Operation as NTP server using source of time based on IEEE 1588v2 PTP, NTP or internal clock.

High immunity to external interferences (EMI)

- Adequate to IEC 61000-4 standard;
- Adequate to IEC 60255-5 standard;
- Adequate to IEC 60068-2 standard.

Packet switched transmission

- Packet switched transmission done totally by hardware;
- Automatic learning with auto-negotiation and detection/treatment of polarity inversion in copper ports;
- Formation and automatic loop-based topologies control with STP protocols (IEEE 802.1D): STP, RSTP and MSTP;
- Transfers only reliable packets (store-and-forward operation);
- Provides support to the VLAN (IEEE 802.1Q) with independent (IVL) or shared (SVL) learning by hardware of up to 4,095 VLANs and 32,000 MAC addresses;
- Quality of service (QoS) ranking with 512 inputs and 8 priority lines per port, with strict or weighted priority operation;
- Operation as routing, either static or dynamically using RIP v1/2 or OSPF;
- Supports IPv4 and IPv6 in broadcast, multicast and unicast;
- Supports IGMP v2/v3 and MLD v1/v2;
- Detection and avalanche control in broadcast, multicast and unicast.

Management

- Network Management Integration (NMS) integration with PulseNet software;
- Configuration in text mode on a safe connection (SSH);
- Configuration in graphic mode on a safe connection (HTTPS);
- Authentication and native or remote authorization (RADIUS and TACACS+);
- Remote monitoring via RMON;
- DDM (Digital Diagnostic Monitoring) support for optical SFPs
- Dedicated configuration settings port is an USB 2.0;
- Statistical data collection of use via internal agent.

SNMP v3

- Traffic mirroring for monitoring.

Failsafe alarm relay

- Dry contact NO and NC;
- Several configurable alarms

Mounting options

- Removable fixation flap for a standard 19" rack and 1U tall;
- Interface connectors on the rear of the chassis;

Power Supplies

- 110-240 V_{AC} / 125-250 V_{DC} and 48 V_{DC} power supplies options
- Redundant power supply available

4 Key Features

- Switching capacity of 68 Gbps;
- Automatic learning, auto-negotiation and automatic detection/treatment of polarity at the copper ports (RJ45 connectors);
- Store-and-forward packet switching;
- IP Routing functionalities: Static, RIP and OSPF;
- VRRP to eliminate a single point of failure in static routed environments;
- Support to IPv4 and IPv6 protocols (Multicast, Unicast and Broadcast);
- Storm detection and control (Multicast, Unicast and Broadcast storm types);
- Cyber Security features, been ready for NERC CIP v5 requirements;
- SSH text mode configuration on a safe connection;
- HTTPS graphic mode configuration on a safe connection;

- Native and remote authentication and authorization through RADIUS and TACACS+;
- Remote monitoring through RMON;
- DDM (Digital Diagnostic Monitoring) support for optical SFPs, with alarms through SNMP and failsafe relay.
- SNMP v1/v2c/v3
- IP multicast management through IGMP v2/v3 (for IPv4 applications) and MLD v1/v2 (for IPv6 applications);
- VLAN traffic segregation (IEEE 802.1Q), and up to 4095 VLANs allowed;
- MAC Table with up to 8192 entries (dynamic and static);
- Traffic prioritization (up to 8 Class of Service levels) using QoS (IEEE 802.1Q);
- Loop detection and protection through Spanning-tree protocols: STP, RSTP (IEEE 802.1D) and MSTP (IEEE 802.1Q);
- Bridge Protocol Data Unit (BPDU) guard and filtering to prevent external interference in Spanning Tree networks;
- UltraRSTP performs fault recovery time around 5 ms per hop;
- Loop detection and protection function without Spanning-tree protocols;
- Internal clock synchronization using either a 1588v2 grandmaster clock or up to 5 NTP time servers;
- Hardware-based IEEE 1588v2 compliant (Precision Time Protocol – PTP) at all ports;
- Operation as NTP server using IEEE 1588v2 as source of time
- USB 2.0 communication port for local configuration;
- Dry-contact relay for external signalization failsafe alarm.

5 Compliance

The device has undergone a range of extensive testing and certification processes to ensure and prove compatibility with all target markets. A detailed description of these criteria can be found in the Technical Specifications chapter.

5.1 Standard Compliance

Compliance with the European Commission Directive and UK Conformity Assessed on EMC and LVD is demonstrated by self-certification against international standards.



When available, recognition by UL 60950-1 is demonstrated by a UL certificate and the label.



Further than that, S20 complies with:

- IEC 60255-27: 2013 for safety requirements, demonstrated by laboratory type testing;
- IEC 60255-26:2013 for EMC requirements, demonstrated by laboratory type testing
- IEC 61850-3 ed.2: 2013 for EMC, environment and safety requirements demonstrated by laboratory type testing;
- IEEE 1613 and IEEE 1613.1 for EMC requirements demonstrated by laboratory type testing;
- RoHS directive 2011/65/EU with amendment Directive (EU) 2015/863 ;
- R&TTE - Radio and Telecommunications Terminal Equipment directive 99/5/EC. Conformity is demonstrated by compliance with both the EMC directive and the Low Voltage directive, to zero volts.

5.2 Product Safety

Compliance with IEC 60255-27:2013 was used to establish conformity.

Protective Class

IEC 60255-27:2013 Protective Class I

Installation category

IEC 60255-27:2013 Overvoltage Category III (110-240 V_{AC} / 125-250 V_{DC} power supply) and Overvoltage Category II (48 V_{DC} power supply)

6 Cyber Security Disclaimer

S20 is a digital device designed to be installed and operated in industrial and power sub-station environments and connected to secure private networks. S20 should not be connected to the public internet.

GE strongly recommend users to protect their digital devices using a defense-in-depth strategy to protect their products, their network, its systems and interfaces against cyber security threats. This includes, but is not limited to, placing digital devices inside the control system network security perimeter, deploy and maintain access controls, monitoring of Intrusion Detection, security awareness training, security policies, network segmentation and firewalls, strong and active password management, data encryption, antivirus and other mitigating applicable technologies. GE Grid Solution may also provide additional instructions and recommendations to users from time to time relating to S20 and cyber security threats or vulnerabilities.

It is the users' sole responsibility to make sure that S20 is installed and operated considering its cyber security capabilities, security context, and

the instructions and recommendations provided to the user relating to S20. Users assume all risks and liability associated with damages or losses incurred in connection with any and all cyber security incidences.

7 S20 Order Code

Order Number	1-3	4-5	6	7	8	9	10	11	12	13	14	15	16	17-18	19	20		
Model Type S20 Industrial Managed Ethernet Switch	S20																	
Number of ports Up to 20 ports (4x Gigabit) Up to 24 Gigabit ports	20 24																	
Power Supply 1 48 Vdc** 125-250 Vdc / 110-240 Vac	1 3																	
Power Supply 2 48 Vdc** 125-250 Vdc / 110-240 Vac Not installed	1 3 X																	
Mounting Options 19" Rack Mount / Rear Mount	P																	
Software Functionality (Licensing) Standard Layer 2 packet switching (MAC Based) Advanced Layer 2 and Layer 3 packet switching (MAC Based and IP Based)	2 3																	
PTP Support (Licensing) With PTP (IEEE 1588v2) support Without PTP (IEEE 1588v2) support	P X																	
Interface Module 1 Four 1 Gbps RJ45 copper 10/100BASE-TX/1000BASE-T Ethernet ports Four slots for SFP transceivers (up to 1 Gbps) Four 1 Gbps LC-type SFP transceivers multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-LX Ethernet for up to 20 km Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 40 km Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 80 km Four 100 Mbps LC-type SFP transceivers multi mode fiber 100BASE-FX Ethernet for up to 2 km Four RJ45 copper 10/100BASE-TX Four 1 Gbps RJ45 SFP transceivers Ethernet 10/100BASE-TX/1000BASE-T Two 1 Gbps RJ45 SFP transceivers 10/100BASE-TX/1000BASE-T Ethernet ports + Two 1 Gbps LC-type SFP transceivers multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km Two 1 Gbps RJ45 SFP transceivers 10/100BASE-TX/1000BASE-T Ethernet ports + Two 100 Mbps LC-type SFP transceivers multi mode fiber 100BASE-FX Ethernet for up to 2 km Two 1 Gbps LC-type SFP transceivers multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km + Two 100 Mbps LC-type SFP transceivers multi mode fiber 100BASE-FX Ethernet for up to 2 km	A B C D E F H I J K L M																	
Interface Module 2 Four 1 Gbps RJ45 copper 10/100BASE-TX/1000BASE-T Ethernet ports* Four slots for SFP transceivers (Up to 1 Gbps in the 24 ports model / Up to 100 Mbps in the 20 ports model) Four 1 Gbps LC-type SFP transceivers multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-LX Ethernet for up to 20 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 40 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 80 km* Four 100 Mbps LC-type SFP transceivers multi mode fiber 100BASE-FX Ethernet for up to 2 km Four RJ45 copper 10/100BASE-TX Four 1 Gbps RJ45 SFP transceivers Ethernet 10/100BASE-TX/1000BASE-T* Not installed	A B C D E F H I J X																	
Interface Module 3 Four 1 Gbps RJ45 copper 10/100BASE-TX/1000BASE-T Ethernet ports* Four slots for SFP transceivers (Up to 1 Gbps in the 24 ports model / Up to 100 Mbps in the 20 ports model) Four 1 Gbps LC-type SFP transceivers multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-LX Ethernet for up to 20 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 40 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 80 km* Four 100 Mbps LC-type SFP transceivers multi mode fiber 100BASE-FX Ethernet for up to 2 km Four RJ45 copper 10/100BASE-TX Four 1 Gbps RJ45 SFP transceivers Ethernet 10/100BASE-TX/1000BASE-T* Not installed	A B C D E F H I J X																	
Interface Module 4 Four 1 Gbps RJ45 copper 10/100BASE-TX/1000BASE-T Ethernet ports* Four slots for SFP transceivers (Up to 1 Gbps in the 24 ports model / Up to 100 Mbps in the 20 ports model) Four 1 Gbps LC-type SFP transceivers multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-LX Ethernet for up to 20 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 40 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 80 km* Four 100 Mbps LC-type SFP transceivers multi mode fiber 100BASE-FX Ethernet for up to 2 km Four RJ45 copper 10/100BASE-TX Four 1 Gbps RJ45 SFP transceivers Ethernet 10/100BASE-TX/1000BASE-T* Not installed	A B C D E F H I J X																	
Interface Module 5 Four 1 Gbps RJ45 copper 10/100BASE-TX/1000BASE-T Ethernet ports* Four slots for SFP transceivers (Up to 1 Gbps in the 24 ports model / Up to 100 Mbps in the 20 ports model) Four 1 Gbps LC-type SFP transceivers multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-LX Ethernet for up to 20 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 40 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 80 km* Four 100 Mbps LC-type SFP transceivers multi mode fiber 100BASE-FX Ethernet for up to 2 km Four RJ45 copper 10/100BASE-TX Four 1 Gbps RJ45 SFP transceivers Ethernet 10/100BASE-TX/1000BASE-T* Not installed	A B C D E F H I J X																	
Interface Module 6 (Only available in the 24 ports model) Four 1 Gbps RJ45 copper 10/100BASE-TX/1000BASE-T Ethernet ports* Four slots for SFP transceivers (up to 1 Gbps) Four 1 Gbps LC-type SFP transceivers multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-LX Ethernet for up to 20 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 40 km* Four 1 Gbps LC-type SFP transceivers single mode fiber 1000BASE-ZX Ethernet for up to 80 km* Four 100 Mbps LC-type SFP transceivers multi mode fiber 100BASE-FX Ethernet for up to 2 km* Four RJ45 copper 10/100BASE-TX 10/100BASE-TX/1000BASE-T* Four 1 Gbps RJ45 SFP transceivers Ethernet 10/100BASE-TX/1000BASE-T* Not installed	A B C D E F H I J X																	
Firmware Version Firmware release number 07	07																	
Hardware Design Suffix Hardware C version Hardware B version	C B																	
UL/CSA Recognized Yes*** No	1 0																	

* Only available in the 24 ports model

** Power supply rating varies depending on hardware version, please refer to manual

*** UL/CSA recognition available in hardware C only

Issue M

Chapter 2: Safety Information

This chapter provides information about the safe handling of the equipment. The equipment must be properly installed and handled in order to maintain it in a safe condition and to keep personnel safe at all times. You must be familiar with information contained in this chapter before unpacking, installing, commissioning, or servicing the equipment.

1 Health and Safety

Personnel associated with the equipment must be familiar with the contents of this Safety Information.

When electrical equipment is in operation, dangerous voltages are present in certain parts of the equipment. Improper use of the equipment and failure to observe warning notices will endanger personnel.

Only qualified personnel may work on or operate the equipment. Qualified personnel are individuals who are:

- familiar with the installation, commissioning, and operation of the equipment and the system to which it is being connected.
- familiar with accepted safety engineering practices and are authorized to energized and de-energized equipment in the correct manner.
- trained in the care and use of safety apparatus in accordance with safety engineering practices
- trained in emergency procedures (first aid).

The documentation provides instructions for installing, commissioning and operating the equipment. It cannot, however cover all conceivable circumstances. In the event of questions or problems, do not take any action without proper authorization. Please contact your local sales office and request the necessary information.

The user is responsible to ensure the equipment is installed, operated and used for its intended function in the manner specified by the manufacturer. Please refer to the next sections carefully to ensure safety instructions are being followed.

2 Symbols

Throughout this manual you will come across the following symbols. You will also see these symbols on parts of the equipment.



Caution: Refer to equipment documentation. Failure to do so could result in damage to the equipment



Risk of electric shock



Protective bonding (ground) terminal



Alternating current



Continuous current



Instructions on disposal requirements

3 Installation, Commissioning and Servicing

3.1 Lifting Hazards

Many injuries are caused by:

- Lifting heavy objects
- Lifting things incorrectly
- Pushing or pulling heavy objects
- Using the same muscles repetitively

Plan carefully, identify any possible hazards and determine how best to move the product. Look at other ways of moving the load to avoid manual handling. Use the correct lifting techniques and Personal Protective Equipment (PPE) to reduce the risk of injury.

3.2 Electrical Hazards



All personnel involved in installing, commissioning, or servicing this equipment must be familiar with the correct working procedures.



Consult the equipment documentation before installing, commissioning, or servicing the equipment.



Always use the equipment as specified. Failure to do so will jeopardize the protection provided by the equipment.



Removal of equipment panels or covers may expose hazardous live parts. Do not touch until the electrical power is removed. Take care when there is unlocked access to the rear of the equipment.



Isolate the equipment before working on the terminal strips.



Use a suitable protective barrier for areas with restricted space, where there is a risk of electric shock due to exposed terminals.



Disconnect power before disassembling. Disassembly of the equipment may expose sensitive electronic circuitry. Take suitable precautions against electrostatic voltage discharge (ESD) to avoid damage to the equipment.



NEVER look into optical fibers or optical output connections. Always use optical power meters to determine operation or signal level.



Testing may leave capacitors charged to dangerous voltage levels. Discharge capacitors by reducing test voltages to zero before disconnecting test leads.



If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.



Operate the equipment within the specified electrical and environmental limits.



Before cleaning the equipment, ensure that no connections are energized. Use a lint free cloth dampened with clean water.



Integration of the equipment into systems shall not interfere with its normal functioning.



The functioning of the device has been certified under the circumstances described by the standards mentioned in the following subsection: Insulation, EMI and Environmental Tests. Usage of the equipment in different conditions from the specified in this manual might affect negatively its normal integrity.



The equipment shall have all their rear connectors and SFPs attached even if they are not being used, in order to keep their levels of ingress protection as high as possible



Never manipulate liquid containers near the equipment even when it is powered off.



Avoid modification to the wiring of panel when the system is running.

3.3 Fusing and Insulation Requirements



A high rupture capacity (HRC) fuse type with a maximum current rating of 10 Amps and a minimum dc rating of 250 V dc may be used for the auxiliary supply (for example Red Spot type NIT or TIA). Alternatively, a miniature circuit breaker (MCB) of type C, 10A rating, compliant with IEC 60947-1 and IEC 60947-3 may be used.



Reason devices contain an internal fuse for the power supply which is only accessed by opening the product. This does not remove the requirement for external fusing or use of an MCB as previously mentioned. The ratings of the internal fuses are:

3.15 Amp, type T, 250V rating



Models with a low DC power source must be supplied with a DC supply source to the equipment that is derived from a secondary circuit which is isolated from the AC/DC Mains by Double or Reinforced Insulation (e.g.: UL Certified ITE power supply which provides Double or Reinforced Insulation).

3.4 Equipment Connections



Terminals exposed during installation, commissioning and maintenance may present a hazardous voltage unless the equipment is electrically isolated.



Tighten M3 clamping screws of heavy duty terminal block connectors to a nominal torque of 1.0 Nm. Tighten captive screws of header-type (Euro) terminal blocks to 0.5 Nm minimum and 0.6 Nm maximum.



Always use insulated crimp terminations for voltage connections..



Always use the correct crimp terminal and tool according to the wire size.



In order to maintain the equipment's requirements for protection against electric shock, other devices connected to Reason S20 shall have protective class equal or superior to Class II.



Watchdog (self-monitoring) contacts are provided to indicate the health of the device on some products. We strongly recommend that you hard wire these contacts into the substation's automation system, for alarm purposes.



Ground the equipment with the supplied PCT (Protective Conductor Terminal).



Do not remove the PCT.



The PCT is sometimes used to terminate cable screens. Always check the PCT's integrity after adding or removing such ground connections.



The user is responsible for ensuring the integrity of any protective conductor connections before carrying out any other actions.



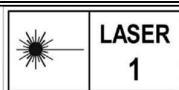
The PCT connection must have low-inductance and be as short as possible.



All connections to the equipment must have a defined potential. Connections that are pre-wired, but not used, should be earthed, or connected to a common grouped potential.



Pay extra attention to diagrams before wiring the equipment. Always be sure that the connections are correct before energizing the circuits.



This product is fitted with Class I lasers.

3.5 Pre-energization Checklist



Check voltage rating/polarity (rating label/equipment documentation).



Check protective fuse or miniature circuit breaker (MCB) rating.



Check integrity of the PCT connection.



Check voltage rating of external wiring, ensuring it is appropriate for the device.

3.6 Upgrading/Serviceing



Do not insert or withdraw modules, PCBs or expansion boards from the equipment while energized, as this may result in damage to the equipment. Hazardous live voltages would also be exposed, endangering personnel.



Internal modules and assemblies can be heavy and may have sharp edges. Take care when inserting or removing modules into or out of the IED.

4 Decommissioning and Disposal



Before decommissioning, completely isolate the equipment power supplies (both poles of any dc supply). The auxiliary supply input may have capacitors in parallel, which may still be charged. To avoid electric shock, discharge the capacitors using the external terminals before decommissioning.



Avoid incineration or disposal to water courses. Dispose of the equipment in a safe, responsible and environmentally friendly manner, and if applicable, in accordance with country-specific regulations.

GE Reason S20

Industrial Managed Ethernet Switches

Chapter 3: Installation Guide

1 Mechanical Design

S20 is 19" rack mounting with 1U high (44.45 mm) and a depth of 310 mm. With a fanless design, the case is made from pre-finished steel and painted with epoxy paint.



Figure 1: S20 mechanical design

2 Unpacking

Unpack the equipment carefully and make sure that all accessories and cables are put away so they will not be lost.

Check the contents against the packing list. If any of the contents listed is missing, please contact GE immediately (see contact information at the beginning of this manual).

Examine the equipment for any shipping damage. If the unit is damaged or fails to operate, notify the shipping company immediately. Only the consignee (the person or company receiving the unit) can file a claim against the carrier for occasional shipping damages.

We recommend that the user retain the original packing materials for use in case of need to transport or ship the equipment at some future time.

3 Rack Mounting

To maintain the equipment integrity, levels of protection and assure user safety, Reason S20 shall be installed in an enclosed panel with recommended ingress protection rating of IP42 or above. During the normal use of the device only its frontal panel shall be accessible.

The enclosing panel shall ensure that the equipment rear connections and sides are unexposed and protected against impact and water, meanwhile maintaining adequate temperature and humidity condition for the devices. Reason S20 is designed for standard 19" rack mounting and since it is fanless, the heat is channeled to the case. Thus, it is recommended to keep 1U rack unit (1.75") unpopulated above each S20 for convectional airflow. Although not necessary, the conventional airflow will improve long-term reliability.



Figure 2: Rack Mounting design

4 Power Connections

Multiple power supplies options are available, which can be selected as main and/or redundant power supply. Mixed power supplies in the same equipment is allowed, so look carefully to the power labels to identify the nominal power range of each one.

All power connections should use insulated flameproof flexible cable (BWF type) with a 1.5 mm² cross section, 70 °C (158 °F) thermal class, and 750 V insulation voltages.

Models with a low DC power source must be supplied with a DC supply source to the equipment that is derived from a secondary circuit which is isolated from the AC/DC Mains by Double or Reinforced Insulation (e.g.: UL Certified ITE power supply which provides Double or Reinforced Insulation).

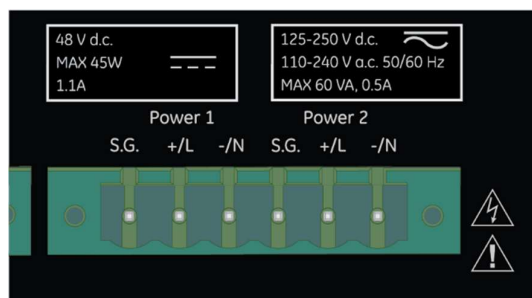


Figure 3: Power Supply connector



Ensure the power supply connection aligns precisely with the terminal description in Table 1, with particular attention to the surge ground terminal when using 48Vdc power supply.

Table 1: Terminal description from Power Connection

Terminal Number	Description	Use
1	Surge Ground (S.G.)	When using 48Vdc power supply only, S.G (terminal 1) must be connected to -/N (terminal 3) to meet surge withstand
2	+/L	+/L is connected to the positive cable (+) if the power source is DC, or to the phase cable if the power source is AC.
3	-/N	-/N is connected to the negative cable (-) if the Power source is DC, or to the neutral cable if the power source is DC.
4	Surge Ground (S.G.)	When using 48Vdc power supply only, S.G (terminal 4) must be connected to -/N (terminal 6) to meet surge withstand
5	+/L	+/L is connected to the positive cable (+) if the power source is DC, or to the phase cable if the power source is AC. (Available only for equipment that provide a redundant source)
6	-/N	-/N is connected to the negative cable (-) if the power source is DC, or to the neutral cable if the power source is DC. (Available only for equipment that provide redundant source)

Note the surge ground terminals must be disconnected in case of conducting an insulation test in the circuit that includes the product's power connections.

For safety purposes, install a suitable external switch or circuit breaker for each S20 power supply, in accordance with its nominal voltage, which may interrupt both the positive (+/L) and neutral (-/N) power leads.

As recommendation, considers an external 10 A, category C, bipolar circuit-breaker. The circuit breaker should have an interruption capacity of at least 25 kA and comply with IEC 60947-2. The switch or circuit-breaker must be suitably located and easily reachable, also it shall not interrupt the protective earth conductor.

5 Ground Connection

The protective grounding connector located in the rear of the equipment shall be connected to the metallic mass of the rack cabinet in which the switch shall be installed. Keep the grounding connection permanently connected during normal use, before the equipment is powered on and after the equipment is powered off.

The protective grounding conductor must use a UL-listed ring terminal lug suitable for number 10-to-12 AWG wire and at least a 4 mm² conductor to connect to the external protective grounding screw.

6 Communications Ports

6.1 Electrical Ethernet Ports (RJ45)

Reason S20 is equipped with 10/100BASE-TX and 10/100/1000BASE-TX ports that feature auto-negotiation, auto-polarity, and auto-crossover functions.

In high electrical noise environments, follow these:

- Data cable lengths should be as short as possible – ideally limited to 3 m (10') in length. Copper data cables should not be used for inter-building communication, since they might be operating in a different current power and may suffer from EMC generated by high-voltage equipment;
- Power and data cables should not be run in parallel for long distances, and should be installed in separate conduits. Power and data cables should intersect at 90° angles when necessary to reduce inductive coupling.

Shielded/screened cabling can optionally be used. The cable shield should be grounded at one single point to avoid the generation of ground loops.

6.2 SFP Pluggable Transceiver

Reason S20 can operate with a SFP transceiver (Small Form-factor Pluggable) which can be inserted and removed safely while the switch is powered and operating. However, when inserting or removing the SFP transceiver, there are precautions that should be taken:

- Be sure that the protection covers are always mounted on the SFP transceiver, unless a user is on the process of inserting or removing of the SFP module;
- Be sure that the user has taken all possible precautions in relation to the electrostatic charge accumulation (ESD);

- Disconnect all cables from the SFP module before inserting or removing the module;
- Use only transceivers certified by GE Reason.

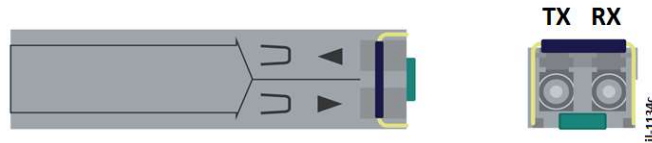


Figure 4: SFP transceiver

Before removing the SFP transceiver, take the wires off and insert the protective cover against dust. The SFP transceivers should be removed pulling the safety catch located on the top of the transceiver. Grasp the metal bail latch and gently pull outwards to unlock and remove the module.



NEVER look into the optical fibers or optical output connections. Always use optical power meters to determine operation or signal level.

7 Dry Contact Relay (Failsafe)

Reason S20 is equipped with a failsafe dry contact relay (form C) for signaling an event as previously configured. By default, the Failsafe relay is disabled meaning it will not switch its state.

The failsafe works in a combination of three pins, been available one Normally Closed (NC) and one Normally Opened (NO) contact, in which the pin 2 is the common one:

- When there are no events to alarm in a normal condition or when the failsafe is disabled, contact 2-3 is normally closed and contact 2-1 is normally open;
- To signalize a condition of any configured event, contact 2-3 switch to opened and contact 2-1 switch to closed.

The dry contact connections are illustrated below and insulated flexible wires of 1.5 mm² cross section shall be used.

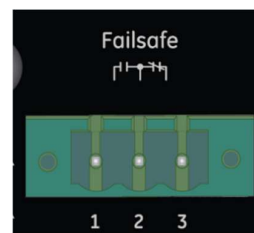


Figure 5: Failsafe form C dry-contact relay

8 Energizing

Reason S20 does not have a power on or power off button. After plug-in the power supply, the switch will power up. After powered up, the LEDs will perform a pattern that indicates S20 is being initialized. A Power LED for each power supply is available indicating when it is energized.

9 Preventive Maintenance

In view of the critical nature of application, GE products should be checked at regular intervals to confirm they are operating correctly. GE products are designed for a life more than 20 years. The devices are self-supervising and so require less maintenance than earlier designs of protection devices. Most problems will result in an alarm, indicating that remedial action should be taken. However, some periodic tests should be carried out to ensure they are functioning correctly and that the external wirings are intact. It is the responsibility of the customer to define the interval between maintenance periods. If your organization has a Preventive Maintenance Policy, the recommended product checks should be included in the regular program. Maintenance periods depend on many factors, such as:

- The operating environment
- The Accessibility of the site
- The amount of available manpower
- The importance of the installation in the power system
- The consequences of failure

9.1 Preventive Actions

Switches do not fail very often. However, there is a need for preventive maintenance of switches. Periodically switches should be checked for smooth and correct operation, and physical damage. Any problems found should be corrected immediately.

For optimum performance, make sure to follow the preventive maintenance procedures and actions:

- Keep temperature and humidity at adequate levels inside the panel. The American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE) recommends operating network equipment within the following ranges of temperature and relative humidity (see the ASHRAE TC 9.9 “2011 Thermal Guidelines for Data Processing Environments – Expanded Data Center Classes and Usage Guidance”):
 - Temperature within 18° C to 27° C (64° F to 80.6° F)
 - Relative humidity less than 60%
 - Dew point within the range of 5.5° C to 15° C (41.9° F to 59.0° F)

- Operating within the range supports the highest degree of equipment reliability, even though the equipment data sheets may state wider ranges of minimum and maximum temperature and humidity (for example, -40° C to 55°C and 5% to 95% RH). Continuous equipment operation at the minimum and maximum limits is not recommended.
- Keep panel sealed to avoid dust and/or animals and insects.
- Inspect the installation site for moisture, loose wires or cables, and excessive dust. Make sure that airflow is unobstructed around the switch and into the air intake vents.
- Check the device status reporting on syslog server. The log function is a file that records information of a running operating system or software at a device. Many applications use this for analysis purposes, as it keeps stored running routines or physical connections information, such as active Ethernet ports.
- Reason S20 has the capability to send log messages to dedicate log servers. The syslog level is divided in 4 categories: error (severity 3), warning (severity 4), notice (severity 5) and informational (severity 6). When choosing higher severity level, the equipment will send all messages from lower levels plus the severity level selected. Thus, choosing informational severity level allows the user to receive all log messages that the equipment can send. Choosing error severity level the user will receive just error messages.
- SNMP can be configured to monitor the S20's temperature;
- The recommended preventive actions described above will help to keep the unit running smoothly and will also avoid any inconvenience.

GE Reason S20

Industrial Managed Ethernet Switch

Chapter 4: Interfaces & Operation

1 Communication Interfaces

Reason S20 has local and remote communication interfaces:

- Local interface:
 - USB 2.0 communication port for local configuration (console interface).
- Remote interfaces:
 - Ethernet interface communication (Electrical or Optical) for remote or local monitoring and configuration. Available protocols for this interface are HTTP, HTTPS, SSH and Telnet.

For security reasons, only SSH and HTTPS are available by default.

1.1 Local Interface – USB

Reason S20 has a USB (Universal Serial Bus) interface to configure the equipment and monitor running settings using command line interface (CLI). If used, this interface would require a computer with a USB communication port, a serial communication software and to install a driver which is available for download in the

<https://www.gevernova.com/grid-solutions/> website.

When accessing the Reason S20 using the USB local interface, it is necessary to configure the USB port serial communication parameters at the computer to meet the USB port specifications. Serial parameter must be as follow:

- Speed: 115200 bits per second;
- Data bits: 8;
- Stop bits: 1;
- Parity: None;
- Flow control: None.

The USB connector is a female B-type, as illustrated by figure below.



Figure 6: B-type USB connector

1.2 Remote Interface – Ethernet

Reason S20 may be configured, monitored, do firmware update and maintenance actions using an Ethernet connection, either accessing the Web Interface through HTTP/HTTPS protocols or using the SSH/Telnet via CLI. This interface requires a computer with network port and a browser installed. Both Ethernet electrical or optical interfaces may be used for remote interface.

HTTP and HTTPS are the most friendly-to-use interfaces available, as it runs in a Web browser interface. The figure below illustrates an example of the first screen interface when accessed.

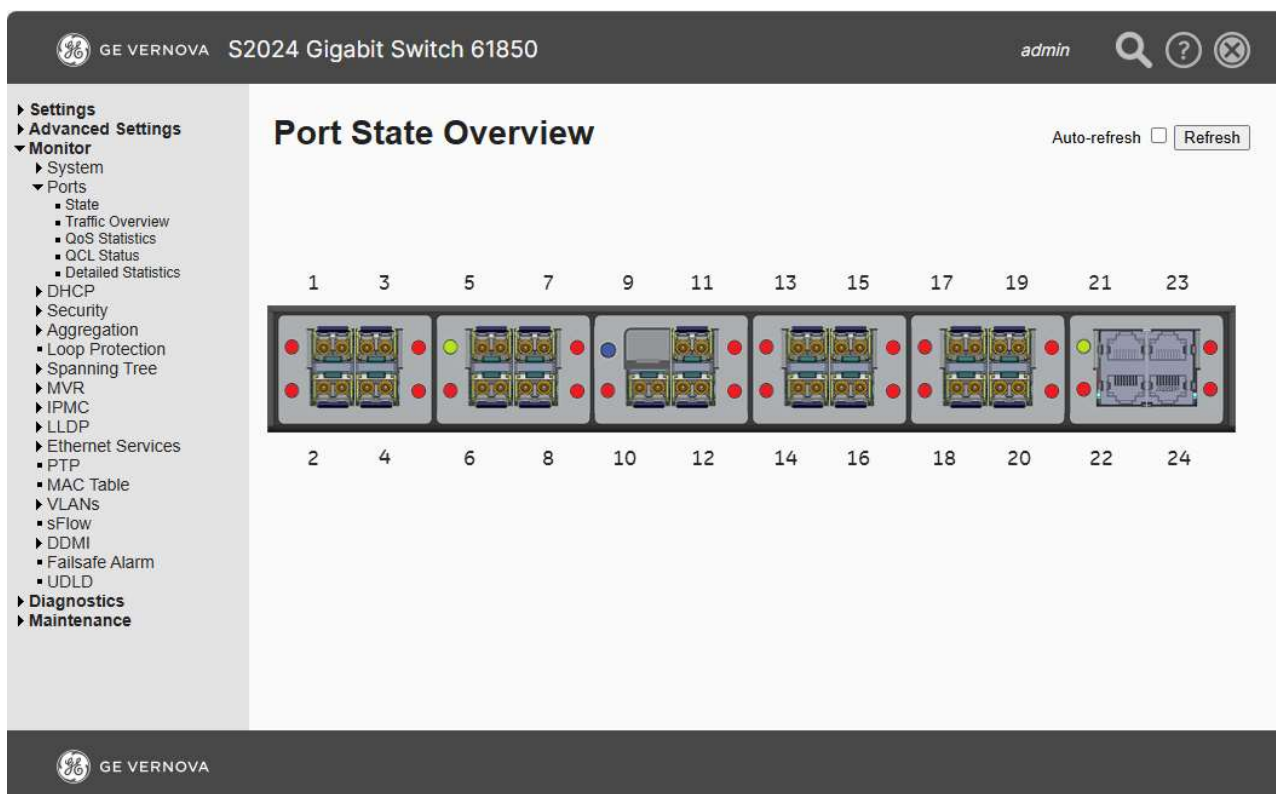


Figure 7: Example of HTTP or HTTPS first screen

To use HTTPS protocol, make sure to type **https://** before the IP address in the web browser. A message of a non-secure connection may appear, as the browser cannot find a valid certification for the web site. It does not

affect equipment functions and configuration, the user can continue the connection to normally access the equipment Web Interface.

There are three buttons on the top right corner of Web Interface, which has the following purposes:

- **Search Bar:** the user may search for any type of settings, monitoring, diagnostics or maintenance information. For instance, to search for IEEE 1588 PTP, the user may either type “PTP” or “IEEE 1588”.
- **Logout button:** click to finish the current user session;
- **Info:** click on this button to find out more about the current web page been displayed. This is an online guidance for interfacing when using HTTP or HTTPS.



Figure 8: Web Interface Search bar, logout and info

2 Accessing Reason S20

As previously mentioned, it is possible to access the Reason S20 by:

- Web Interface through HTTP/HTTPS protocols using Ethernet interface, or;
- CLI, either through SSH/Telnet Ethernet or USB console interface.

A disclaimer message may be configured to popup when accessing the S20 either by Web Interface or CLI, if required. By default, the disclaimer message is empty and does not appear.

To access the Reason S20 for the first time, please find below the factory default parameters.

2.1 Factory Default Parameters

IP Address (from all ports) and Netmask

IP Address: 192.168.4.88
Netmask : 255.255.255.0

Login and Password

Login: admin
Password: {serial number from Reason S20}

The serial number may be found in a label attached to the equipment case.

2.2 First Access

Configuring the Terminal

To access the software configuration via Ethernet communication for the first time, configure the terminal for any address between 192.168.4.1 and 192.168.4.254 (except 192.168.4.88, which is the factory IP). Mask is 255.255.255.0 for local connection.

At Windows OS, follow the steps to change the terminal IP address:

- Enter at Control Panel;
- Choose the network connections option;
- At the Local Connection Status, choose the Properties option;
- At the Local Area Connection Properties, choose IP version 4 protocol;
- After selecting IPv4, choose Properties;
- At the General Tab, choose the Use the Following IP address option and then type:
 - IP address: any value from 192.168.4.1 to 192.168.4.254, except Reason S20 default IP address 192.168.4.88;
 - Subnet Mask: 255.255.255.0;
 - Default gateway: leave it empty.
- At the General Tab, the Obtain DNS server address automatically can be selected.

Web Interface

Once the terminal is configured, open a web browser and:

- Type the address: <https://192.168.4.88> and press enter;
- If a warning message appears, click to continue the access;
- Enter the default login and password;

Command Line Interface (CLI)

- To access Reason S20 via Command Line Interface (CLI), use a Telnet/SSH configuration tool like PuTTY and select the connection type. In the example below, the device is being connected via SSH using the IP address 192.168.4.88.

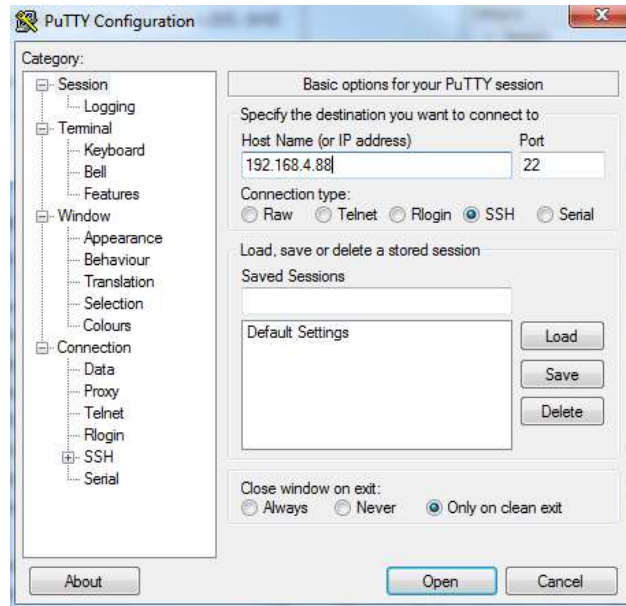


Figure 9: Putty configuration for SSH access

- As you click OPEN, a window will open and require the default login/password.

Changing the Default Password

By following such steps, you should have accessed the web interface by now.

When accessing for the first time, the default password must be changed. The new password must have at least 8 characters including lower/uppercase alphabetic, numeric and special non-alphabetic (e.g. #, \$, @, &). Note the password expiration is enabled by default, and if chosen to keep it (as recommended) the new password will be considered saved on January 1st, 1970 as the internal time was not configured yet.

Make sure to save the new password on the startup configuration, otherwise the password will be back the serial number once the equipment is restarted and the user must pass through the same process once again. To save the new password in the startup configuration using the Web Interface:

- Go to Maintenance > Configuration > Save startup-config
- Click on "Save Configuration"

To save the new password in the startup configuration using CLI, enter the following command line: ***copy running-config startup-config***

Password Expiration and Internal Time Configuration

From now on, the user shall use the new password created and continue the remaining configuration desired. If password expiration is enabled and the internal clock is refreshed to current data and time (by NTP or PTP), the user password will expire and will have to be changed once again in the next section.

2.3 Commands from CLI

The commands presented here may be used for Telnet, SSH or USB local communication.

Each command has a menu inside with its own subcommands, and it can be seeing by typing the “?” character. The most common commands from main menu are:

- *clear* reset functions;
- *configure terminal* enter configuration mode;
- *copy* copy from source to destination;
- *delete* delete one file in flash: file system;
- *dir* directory of all files in flash: file system;
- *disable* turn off privileged commands;
- *do* to run exec commands in configuration mode;
- *dot1x* IEEE standard for port-based access control;
- *enable* turn on privileged commands;
- *erps* Ethernet Ring Protection switching;
- *exit* exit from EXEC mode;
- *failsafe* configure failsafe relay;
- *firmware* firmware upgrade or swap;
- *help* description of the interactive help system;
- *ipv4* IPv4 commands;
- *ipv6* Ipv6 commands;
- *link-oam* link OAM configuration;
- *logout* exit from EXEC mode;
- *more* display file;
- *no* negate a command or set its defaults;
- *ping* send ICMP echo messages;
- *platform* platform configuration;
- *ptp* misc non persistent 1588 settings;
- *reload* reload system;
- *send* send a message to other tty lines;
- *show* show running system information;
- *terminal* set terminal line parameters;
- *veriphy* veriphy keyword.

How to enable/disable SSH or Telnet

First it is necessary to enter in the configuration terminal of S20. To do so, enter the following command:

configure terminal

And then type the following command to enable SSH:

ip ssh

To disable SSH once again, enter the opposite command:

no ip ssh

To enable/disable the Telnet protocol, simply use the same commands but replacing ***ssh*** by ***telnet***.

How to enable/disable HTTP or HTTPS

As usual, it is necessary to enter in the configuration terminal of S20. To do so, enter the following command:

configure terminal

And then type the following command to enable HTTPS:

ip http secure-server

To disable SSH once again, enter the opposite command:

no ip http secure-server

To enable/disable the HTTP protocol, simply use the same commands but replacing **secure-server** by **server**.

3 Signalizing LEDs

The signalization LEDs are placed in the front of the equipment, indicating the status of the ports. The number in the left of each LED means port number associated to it.

- LINK LED: Indicates port status. LED off means port down. LED on means connection with equipment;
 - Green color means Gigabit port speed;
 - Orange color means 100 Mbps port speed.
- Power 1 LED: Indicates that power-supply number 1 is energized;
- Power 2 LED: Indicates that power-supply number 2 is energized;
- Sync LED: Indicates that internal PTP clock is synchronized (when Adjust System Time from PTP is enabled or in Boundary PTP mode);
- Failsafe LED: Indicates that failsafe relay state changed, that is, normally open contact closed and normally closed contact opened.

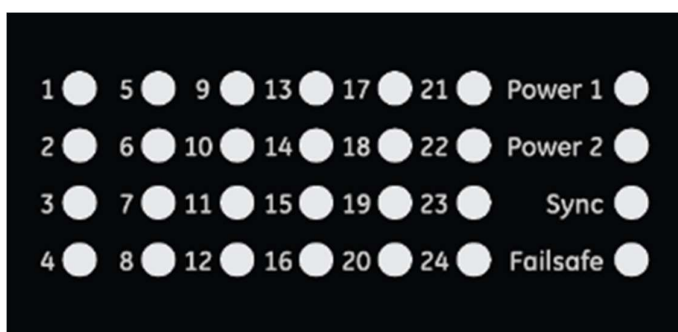


Figure 10: Local HMI LEDs indicators

Table 2: LEDs color description

LED	Color	Description
Link	Off	No connection
	Orange	10/100 Mbps connection
	Green	1000 Mbps connection
Sync	Off	Internal PTP clock unsynchronized
	Green	Internal PTP clock synchronized
Power (1 and 2)	Off	Power Supply off
	Green	Power Supply operating

LED	Color	Description
Failsafe	Off	Failsafe relay non-operating
	Green	Failsafe relay operation

4 Reboot Button

S20 has a reboot button that allows the user to perform a manual reboot without necessity of being connected through a configuration interface, or disconnection and reconnecting the power supply. When pressed, the system will reboot and the Reason S20 will be operating normally after initialization.

If configuration at a given switch is not saved at the start-up configuration, the reboot will discard this configuration (the running configuration). After reboot, the start-up configuration will be operating.



Figure 11: Reboot button

5 Factory Reset

To restore the factory default settings on Reason S20, the user has two options: the first is to login in the equipment and perform a factory reset through a web interface (Maintenance > Factory Defaults) or using CLI. The second option is performed by hardware, as the following procedure.

If the switch is powered on:

1. Connect ports 1 and 2 creating a loop at the switch;
2. Reboot the device with the port 1 and 2 connected to each other. The reboot can be done in the web interface or using the reboot button;
3. Wait around 60 seconds and check if the settings returned to defaults values;
4. Disconnect the loop from ports one 1 and 2.

If the Switch is powered off:

1. Connect ports 1 and 2 creating a loop at the switch;
2. Turn the unit on;
3. Wait around 60 seconds and check if the setting returned to defaults values;
4. Disconnect the loop from ports one 1 and 2.

GE Reason S20

Industrial Managed Ethernet Switch

Chapter 5: Functions & Configuration

Different topologies, IEDs connections and synchronization protocols may be done with Reason S20, and understanding the basic of an application is a good strategy to define the network design.

For power system applications, a set of functions are implemented when using the IEC 61850-90-4 Technical Support as a guide for design and configuration of IEC 61850 networks. Furthermore, Reason S20 counts with a set of cybersecurity features designed to meet NERC CIP v5 requirements.

This chapter describes an overview of common functions and protocols, as well as providing information of how configuring the equipment.

After changing any configuration, the user may save or discard them by clicking in:

- Save: save configuration at the Running Config;
- Reset: undo changes made locally at the Running Config.

1 Configuration overview

Reason S20 runs internally three configuration files, which can be freely selected by user.

Running Config

This file represents the actual configuration of the switch. When the save button is pressed at any settings menu, changes made at the configuration will be saved at this file. If the switch is restarted, this configuration is discarded and the switch will load, after the reboot, the Startup Config file.

Start-up Config

This file represents the configuration that the switch will run after it is powered up or restarted. If a change in the Running Config was performed and it is requested to maintain the Running Config at the Startup Config, the user must save it in Save Running Configuration to startup-config option, in the Maintenance menu.

Default Config

This file represents factory default configuration of the switch. If necessary, it can be loaded by software to replace actual running configuration or the start-up configuration file.

2 System Settings

2.1 System Information

In System Information menu, the user can configure intuitive and friendly-to-use identifications from the personnel name responsible for the switch, the switch (or system) name, where the equipment is located and a disclaimer message to popup when accessing the device. The system information is useful when using management protocols, such as SNMP or LLDP, as it will send the switch name in its messages in order to make network management and diagnosis much easier.

System Information Configuration menu is located at Settings > System > Information.

System Contact

In the Contact information field should be named the personnel responsible for this switch. Allowed string length is up to 255 and allowed characters are the ASCII characters from 32 to 126 (basically letters, numbers and other characters, such as “-” or “_”).

System Name

Administratively name for switch. This field is, by convention, the fully qualified domain name (FQDN). The first character must be an alpha character, and space character is not allowed. Allowed string length is up to 255, and allowed characters are strings drawn from the alphabet (letters), numbers and minus (“-”) signal.

System Location

Identification of where this switch is installed. Allowed string length is up to 255 and allowed characters are the ASCII characters from 32 to 126 (basically letters, numbers and other characters, such as “-” or “_”).

Disclaimer

Disclaimer message to be shown when S20 is accessed through Web Interface or CLI. Maximum length is up to 255 characters as per ASCII (basically letters, numbers and other characters, such as “-” or “_”). To configure the disclaimer through CLI, use the following command “*banner [login] <text>*”.

2.2 IP (Internet Protocol)

On this section is defined the main characteristics of IP (internet protocol) services from S20 on Ethernet networks. IP configuration DNS Servers, IP interfaces from VLANs (which can be correlated to interface ports) and Static IP routings.

IP menu is located at Settings > System > IP.

DNS Server

If required to use domain names instead of direct IP address to access interfaces, it is possible to define DNS Servers and DNS Proxy for address resolution. DNS servers can also be used for management access.

When using more than one DNS Server, the preference of the server used will be given by the Index number of the DNS Server. A smaller Index number means higher priority. If a higher priority server does not respond after 5 attempts, next index server will be requested. By default, no DNS servers are configured.

- From any DHCPv4 interfaces: the first server offered in a DHCPv4 interface will be used;
- No DNS server: no servers to name resolution are used;
- Configured IPv4: the server must be explicitly configured with a valid IPv4 address. The format of the IP address is dotted decimal notation;
- From this DHCPv4 interface: the server used will be the server configured at a given DHCPv4 interface. The field must be configured with the VLAN ID number of the DHCPv4 interface desired. Allowed VLAN ID values are from 1 to 4,095
- Configured IPv6: the server must be explicitly configured with a valid IPv6 address. The format of the IP address is hexadecimal with a colon (":") separating each field.
- From this DHCPv6 interface: the server used will be the server configured at a given DHCPv6 interface. The field must be configured with the VLAN ID (1 – 4,095) number of the DHCPv6 interface desired;
- From any DHCPv6 interfaces: the first server offered in a DHCPv6 interface will be used.
- DNS Proxy: This function is only allowed in IPv4 networks. When enabled, DNS requests are redirected to configured DNS servers, and the reply will be made to a DNS resolver to the client devices in the network.

IP Interfaces

This section is used to define the IP address from each VLAN. By default, all ports are configured on VLAN 1, sharing the same default IP address. However, it is possible to create a VLAN for each interface, for instance, and configure different IP address for each of them.

The IP address per VLAN can be static, or dynamically received by a DHCP server configuration. IPv4 and IPv6 addresses are allowed.

- VLAN: define the VLAN ID of the interface;
- DHCPv4 Enable: enable DHCPv4 IP address configuration. If enabled, switches will operate as DHCPv4 clients and its IP and netmask addresses will be defined by the DHCPv4 server available at the VLAN of this interface;
- DHCPv4 fallback: define the number of seconds to try to obtain an IP address from the DHCPv4 server at the VLAN of this interface. If no addresses are received, IP address used will be the IP configured at the IPv4 Address field. Value "0" disables this field, and allowed values are from 0 to 4,294,967,295 seconds;
- DHCPv4 Current Lease: For interfaces with DHCPv4 enabled, this field display the IP address obtained by the DHCPv4 server at the VLAN of this interface;

- IPv4 Address: define the static IP address to be used at this interface. Values must be inserted in dotted decimal notation. When DHCPv4 is enabled, this address will be used if the DHCPv4 server does not respond to the requests of the switch;
- IPv4 Mask Length: define the number of bits to be used as mask to the IP address, from the most significant bit to the lowest significant bit. Available values are from 0 to 30;
- DHCPv6 Enable: enable DHCPv6 IP address configuration. If enabled, switches will operate as DHCPv6 clients and its IP address will be defined by the DHCPv6 server available at the VLAN of this interface;
- DHCPv6 Rapid Commit: enable the Rapid Commit function for defining its IPv6 address. If Rapid Commit DHCPv6 is allowed by the DHCPv6 server, this checkbox allows the switch to finish the waiting process when a Reply message with Rapid Commit information is received;
- DHCPv6 Current Lease: For interfaces with DHCPv6 enabled, this field display the IP address obtained by the DHCPv6 server at the VLAN of this interface;
- IPv6 Address: define the static IP address to be used at this interface. Values must be inserted with hexadecimal values, with each field of the address separated with a colon (":") marker. When DHCPv6 is enabled, this address will be used if the DHCPv6 server does not respond to the requests of the switch;
- IPv6 Mask Length: define the number of bits to be used as mask to the IP address, from the most significant bit to the lowest significant bit. Available values are from 0 to 128.

IP routes (Static Routing)

The functionality Static Routing is not a routing protocol, instead it is managed manually by the network administrator to define network IP routes. Note IP Routes manually entered are not updated automatically, the administrator must reconfigure it after changes on the network.

Static IP routing works differently depending on the L3 license activation. If the license is not active, S20 will only route packets to gateways in the same VLAN. If the license is active, it can also perform inter-VLAN routing. IP Routes (Static Routing) is useful for a controlled network, which the IP address from terminals are fixed and well known. The following parameters must be configured to establish a IP route manually.

- Network: define network IP address of destination route. IPv4 values must be inserted in dotted decimal notation, and IPv6 values must be inserted with hexadecimal values, with each field of the address separated with a colon (":") marker;
- Mask Length: define the number of bits to be used as mask to the IP address, from the most significant bit to the lowest significant bit;
- Gateway: define the IP address of the gateway/router. IPv4 values must be inserted in dotted decimal notation, and IPv6 values must be inserted with hexadecimal values, with each field of the address

separated with a colon (":") marker. Gateway and Network addresses must be at the same IP version;

- Next Hop VLAN: used only if IPv6 route is requested. Define the VLAN ID of the interface associated to the Gateway. The VLAN IDs allowed range from 1 to 4,095.

To exemplify an IP Route configuration when Layer 3 licensing is activated, the figure below illustrates a network topology with both S20s working as router where is desired to establish a communication between the two IEDs.

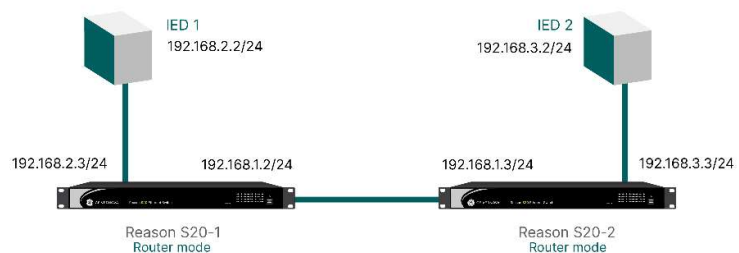


Figure 12: IP routing example

To make sure the messages from IED 1 are delivered to IED 2 using static routing, the network administrator must enter the following route in Reason S20-1:

- Network: 192.168.3.0
- Mask Length: 24
- Gateway: 192.168.1.3

In the other hand, to make sure the IED 2 messages are delivered to IED 1, the following route should be configured in Reason S20-2:

- Network: 192.168.2.0
- Mask Length: 24
- Gateway: 192.168.1.2

Note the Network parameter for IPv4 addresses should end with 0, as shown above.

2.3 NTP Synchronization

The NTP (Network Time Protocol) is a networking protocol that can be used to synchronize the internal clock of S20 over packet-switched data networks, in addition to IEEE 1588v2. The NTP works in a client-server mode, and the time accuracy is within a few milliseconds referred to the UTC time. The current version (NTP version 4) is standardized by RFC 5905. Some functions, such as syslog and password expiration, use time to timestamp the messages.

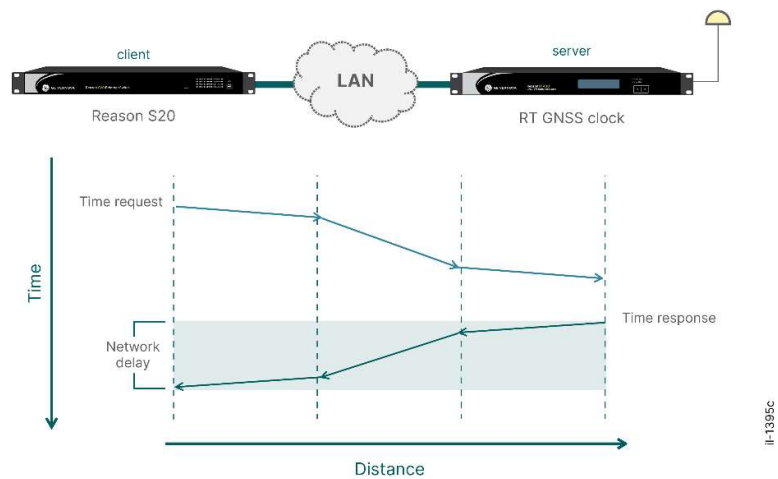


Figure 13: NTP Time Protocol mechanism

In NTP menu, the user can configure up to five NTP time servers to be used as source of time to synchronize the switch internal clock. Lower index of server means higher priority on usage. If a higher priority server does not respond, next index server will be requested.

In addition, the user may choose to enable/disable the NTP server operation and choose the NTP stratum upon the conditions of source of time.

NTP Configuration menu is located at Settings > System > NTP.

NTP Configuration

Configuration related to NTP client operation, where up to five NTP time server may be configured:

- **Mode:** this field is used to enable/disable the NTP time synchronization function. By default, it is disabled. To enable, select Enabled in the Mode list and then configure a valid IP address server. Note if the NTP is enabled, the PTP System Time will be forced to disabled, even if it was previously enabled. The PTP System Time may be once again enabled (manually) if the NTP mode is disabled.
- **Server:** These fields (Server 1 to 5) specify to which NTP servers the switch must send NTP time requests, in a client-server mode. IPv4 values must be inserted in dotted decimal notation, and IPv6 values must be inserted with hexadecimal values, with each field of the address separated with a colon (":") marker.

When using NTP synchronization, be sure NTP server is reachable by the switch. The PING command performed by the switch can be used to check.

NTP Master Configuration

Configuration related to S20 operation as NTP server. S20 can operate as authoritative NTP server based on IEEE1588, NTP client or none source of time (based on manual settings, not synchronized to other source of time). NTP server accepts up to 50 NTP requisition per second (normally represents 50 NTP clients), answering requests from any VLAN that has a known IP registered on the switch IP interfaces.

- **Mode:** Enable/Disable the switch as NTP Server. The NTP server may be based on three different time sources, which are in order of priority: NTP client, PTP adjust system time or manual configured settings. In summary:
 - If NTP client is enabled the NTP will be the source of time to NTP Server.
 - If NTP client is disabled, check whether PTP is being used to adjust the system time by going to “PTP > Adjust System Time”. If PTP adjust system time is enabled, the PTP is being the source of time to NTP Server.
 - In case both the NTP and PTP adjust system time are disabled, the manually configured date/time will be used as source of time to NTP Server.
- **Stratum:** Sets the lowest acceptable output stratum value. Possible values are 1-15, considering the following conditions:
 - When PTP is enabled as time synchronization source, the output stratum follows the configured value.
 - When NTP is enabled as time synchronization source, the output stratum value will be the largest between the input stratum+1, and the configured value.
 - When no time synchronization source is available (NTP client and PTP adjust time disabled, or with them enabled but equipment is not locked), the output stratum is set to 16 (unsynchronized)

The user can also configure the NTP server settings through CLI, as commands below:

```
S2024# configure terminal
```

```
S2024(config)# ntp ?
```

```
master  Configure the switch to act as an authoritative NTP server
server  Configure NTP server
```

```
S2024(config)# ntp master ?
```

```
stratum  distance from the clock source
```

To monitor the NTP status including servers and clients through CLI, use the following command:

```
S2024# show ntp status
```

2.4 Time Configuration

The internal clock of Reason S20 may be synchronized by, in order of priority, NTP, IEEE 1588v2 time protocols or manual configuration of date/time settings. In addition, when using the equipment in other regions the Time Zone and Daylight Saving Time (DST) may be set to correct the internal clock.

Time Configuration menu is located at Settings > System > Time.

Date/Time Configuration

This field allows the user to manually configure the system date/time.

Possible settings for month, date, year, hours and minutes. The “synchronize” button pulls the date/time from the web browser and apply the it to S20 system time. Note the “synchronize” button should only be used in cases where both NTP and PTP are not being used to synchronize the system time.

Time Zone Configuration

This field allows the configuration of the Time Zone, which has a list with where all time zones allowed, and the Acronym that can be used to define it. Possible configurations are as follows.

- Time Zone: define time zone to be used in the internal clock. Allowed values are displayed at the list;
- Acronym: define an acronym to the selected time zone. Allowed acronym size is up to 16 characters.

Daylight Saving Time Configuration

This field allows the configuration of Daylight Saving Time. When used, the internal clock will consider the time zone plus the offset configured in minutes. It is possible to choose if the DST will be used only once or will be recurring at all years. By default, DST (Daylight Saving Time) is disabled. Possible configurations are as follows.

- Daylight Saving Time: enable or disable the DST function. If enabled, the following must be configured;
 - Recurring DST configuration:
 - Week: select the week of the month that the DST should begin (if at Start Time Settings) or end (if at End Time Settings);
 - Day: select the day of the week that the DST should begin (if at Start Time Settings) or end (if at End Time Settings);
 - Month: select the month when the DST should begin (if at Start Time Settings) or end (if at End Time Settings);
 - Hours: select the hour of the day when the DST should begin (if at Start Time Settings) or end (if at End Time Settings);
 - Minutes: select the minute of the hour when the DST should begin (if at Start Time Settings) or end (if at End Time Settings).

- Non-Recurring DST configuration:
 - Month: select the month when the DST should begin (if at Start Time Settings) or end (if at End Time Settings);
 - Date: select the day of the month when the DST should begin (if at Start Time Settings) or end (if at End Time Settings);
 - Year: select the year when the DST should begin (if at Start Time Settings) or end (if at End Time Settings);
 - Hours: select the hour of the day when the DST should begin (if at Start Time Settings) or end (if at End Time Settings);
 - Minutes: select the minute of the hour when the DST should begin (if at Start Time Settings) or end (if at End Time Settings).
- Offset: set the offset that will be applied at the internal clock at the DST period, in minutes. This value will be added at the internal clock during the DST.

2.5 Log

The log function makes sure all events from the operating system are recorded in a non-volatile memory, either by the switch itself or dedicated log servers. In many cases, such logs are required for analysis purposes, as it keeps stored running routines, changes of configuration or physical connections information, such as active Ethernet ports.

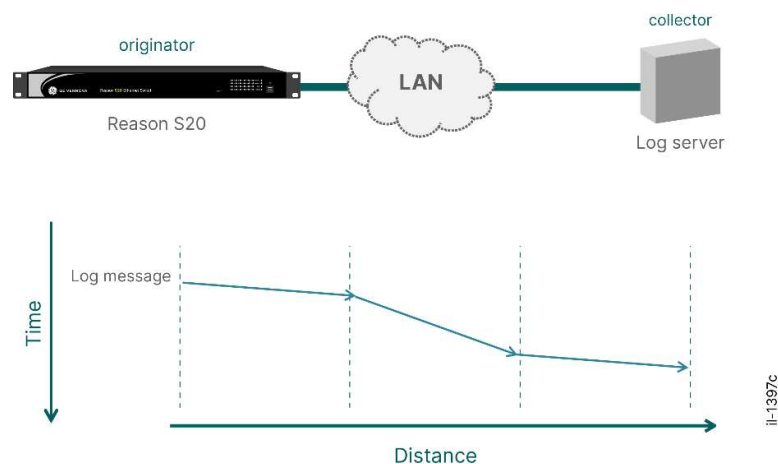


Figure 14: NTP Syslog Message Basics

For computer usage, the log file format (known as syslog) is standardized according to RFC 5424. This RFC does not specify the transport layer protocol. UDP protocol usage for syslog applications is defined in RFC 5426, and this document specifies that at least the 514 UDP port must be used for syslog applications. Other ports, if applicable, should be configurable.

Reason S20 can store log messages internally in a non-volatile memory and send it to two dedicated log servers. Using the internal memory, the S20 can store more than 2048 log messages (circular buffer) and all types of categories registered. To download or visualized messages stored internally, refer to monitoring section.

To configure up to two remote log servers, refer to the following settings.

System Log Configuration menu is located at Settings > System > Log. The following instructions are applied for both Server 1 and Server 2.

Server Mode

This field is used to enable/disable the send of Log messages to a remote server. By default, it is disabled. To enable, select Enabled in the Mode list and then configure a valid IP address server.

Server Address

This field defines the network IP address of the Log server which will receive log messages. Only IPv4 values are supported and IP address must be inserted in dotted decimal notation.

If there is a log server configured at the switch, be sure that the Reason S20 IP address is configured at the Log server, and it is capable to receive Log messages at UDP port 514.

Syslog Level

This list allows the user to select which severity level of log messages will be used as a filter. Reason S20 syslog level is divided in 4 categories: error (severity 3), warning (severity 4), notice (severity 5) and informational (severity 6). Severity levels are defined in RFC 5424 document. When choosing higher severities levels, Reason S20 will send all messages of lower levels plus the severity level selected. Thus, choosing informational severity level means all log messages will be sent to the remote log server. In the other hand, choosing error severity level the remote log server will just receive the error messages.

3 Ports Settings

The Ethernet ports are the connection between the Physical Layer and the Data Link Layer. The Layer 2 functions occur mainly at the Data Link Layer.

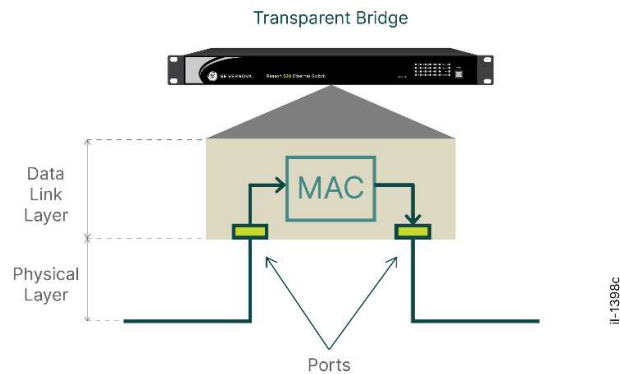


Figure 15: Ports at a Transparent Bridge

As the operation of an Ethernet switch must be as a transparent bridge, it has to deal with the physical medium where all packet data flows and the end nodes of an Ethernet network, which are the clients of the transmitting data.

For copper connections, Reason S20 can be configured to perform automatic negotiation or the port speed may be manually defined. Even when using the automatic speed and transmission mode, it is possible to define which speed and mode will be preferred when connected to an equipment. By default, the switch is configured to auto negotiate and prefer the full capacity (i.e., 1 Gbps for gigabit ports in full-duplex mode or 100 Mbps for fast Ethernet ports in full-duplex mode), however it is user-configurable.

For optical connections, the speed is pre-defined by the SFP hardware thus it can be either 100 Mbps or 1 Gbps. Besides, optical ports cannot operate in a half-duplex mode. For this reason, optical ports can be only configured as disabled or operating in its specified speed, in a Full-Duplex mode.

Port Configuration menu is located at Settings > Ports.

The first column "Port" lists all switch ports. The second column is available to define a "description" for each port if necessary. The third column "Link" displays the status of a given link. Red color means link down, and green color means link up. The fourth column, display the current speed for those ports with link up.

Speed Configured

This field allows configuring the speed at a given port. Port speed configuration will depend on the port type (electrical or optical), and possible options are as follows.

- **Disabled:** disable the port, that is, turn communication off at that port;

To meet cyber security standards, ports that are not been under use must be disabled.

- **Auto:** enable port speed auto negotiation;

- **10Mbps HDX:** enable port speed to 10 Mbps in half-duplex mode;
- **10Mbps FDX:** enable port speed to 10 Mbps in full-duplex mode;
- **100Mbps HDX:** enable port speed to 100 Mbps in half-duplex mode;
- **100Mbps FDX:** enable port speed to 100 Mbps in full-duplex mode;
- **1 Gbps FDX:** enable port speed to 1 Gbps in full-duplex mode;

Advertise Duplex (Adv Duplex)

To configure the link partner advertisement of communication mode from each port when Speed Configure is **Auto**. By default, all full-duplex mode ports detected will advertise its partners of the duplex capacity.

- **Fdx checkbox:** enable advertising link full-duplex is supported;
- **Hdx checkbox:** enable advertising link half-duplex is supported;

Advertise Speed (Adv speed)

This field allows configuring link partner advertisement of communication speed when Speed Configure is defined as **Auto**. By default, all port capacity (10/100/1000 Mbps) will advertise its partners of all capacity (up to 1 Gbps).

- **Speed 10 checkbox:** enable advertising 10 Mbps speed is supported;
- **Speed 100 checkbox:** enable advertising 100 Mbps speed is supported;
- **Speed 1000 checkbox:** enable advertising 1 Gbps speed is supported;

Maximum Transmission Unit (MTU)

This field gives the possibility to configure the maximum transmission unit (MTU), in other words it is the size of the largest network layer protocol data unit that can be communicated through a single Ethernet port. Transmissions with sizes higher than specified in this field are discarded. The size must be configured between 1518 and 10056 byte packets.

Excessive Collision Mode

Collisions may happen when port is operating in half-duplex mode, where there is the possibility of two hosts send transmission frames at the same time, generating collisions at the physical and link layer. After 16 collisions, Reason S20 performs the Excessive Collision Mode, which by default discarded the frames, but options are:

- **Discard:** discard the frame after 16 collisions at the port;
- **Restart:** restart backoff algorithm after 16 collisions at the port.

Frame Length Check

Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If "frame length check" is enabled, frames with payload size less than 1536 bytes are evaluated and if the EtherType/Length field doesn't match the actually payload length they are dropped.

If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame).

Far End Fault Indication (FEFI)

Optical ports support FEFI to disable the port communication in case one fiber loses communication. FEFI is enable by default, and in case is disabled, S20 will still identify loss of fiber communication in Rx ports and disable Tx communication accordingly.

4 Switch Security

Cyber Security is a common topic nowadays, and as Ethernet technology is being widely used in automation systems, the importance of network security has increased over the years. Equipment involved with network automation tasks are designed to be aware of cyber security.

When it comes to switches, management and access security must be evaluated. This section describes basic security configurations, related to management access control and interfaces protocol available.

Following cyber security standards, Reason S20 has a set of security features as follows. To configure Security Switch settings, refer to Settings > Security > Switch.

4.1 User & Password

Multiple users accounts are possible to be created where each user has its specific password and privilege levels. The passwords are encrypted using SHA-2 and must have at least 8 characters including lower/uppercase alphabetic, numeric and special non-alphabetic (e.g. #, \$, @, &). Non-valid characters are: ? and space.

By factory, the Reason S20 password for admin user is the equipment serial number (numbers only) but it must be changed after first login. Each user can change its own password, and admin accounts can change anyone's password.

Attempts to log-in (either successful or failed) are stored in a persistent flash memory syslog. After three failed log-in attempts, the account gets lockout and must wait 1 minute to retry new three attempts.

By default, passwords also expire after 6 months. This option is also user-configurable, and it may be disabled or the expiration period changed. The password expiration uses as reference the date of internal clock in the moment the configuration is saved. Thus, it is recommended to configure the system time before creating new user accounts.

- **Password Expiration** : Enabled/disabled. By default, it is enabled and the expiration period must be configured.
- **Expiration Period** : Defines the period to expire the password in months. Default value is 6 months, and allowed values are from 1 to 120 months.

When configuring a new user, the name password and privilege level must be defined. Up to 15 privilege levels are possible, as described in the following subsection.

- **User Name:** the user name that will be used by this user. Allowed values are letters, numbers and underscore. Maximum user name size is 31 characters;
- **Password:** the password that will be used to identify this user. Password must have at least 8 characters including lower/uppercase alphabetic, numeric and special non-alphabetic (e.g. #, \$, @, &). Maximum password length is 31 characters;
- **Password (again):** repeat password as previously.
- **Privilege Level:** choose the privilege level for the user account. Possible values are from 0 to 15. Only one privilege level is allowed per user.

Default user to access and configure the equipment is the admin user with a privilege level 15. By factory, admin user password is the equipment serial number (numbers only) but it must be changed after first login.

Lastly, by default idle users are logged-out automatically which is configurable through the protocol used to establish the communication. By default, SSH and Telnet connections have a 10 minutes time-out while HTTP/HTTPS has 60 minutes time-out.

4.2 User Privilege Level

Reason S20 can have different privilege levels for each selected user. Up to 16 privilege levels are available, been 0 the lowest privilege level and 15 the highest. Each user has one single privilege attached to its account, and any user can see other users privilege levels. To define what functions a user can read/write, a list of functions is available and each functionality can be classified as desired by admin. By default, three privilege levels are set:

- Level 5: ready-only user (guest);
- Level 10: read and write user (standard user);
- Level 15: read, write and software management user (administrator).

For the following descriptions of this manual, the privilege level 15 is considered as an admin user account.

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5 ▼	10 ▼	5 ▼	10 ▼
Debug	15 ▼	15 ▼	15 ▼	15 ▼
DHCP	5 ▼	10 ▼	5 ▼	10 ▼
DHCPv6_Client	5 ▼	10 ▼	5 ▼	10 ▼
Diagnostics	5 ▼	10 ▼	5 ▼	10 ▼
EVC	5 ▼	10 ▼	5 ▼	10 ▼
IP	5 ▼	10 ▼	5 ▼	10 ▼
IPMC_Snooping	5 ▼	10 ▼	5 ▼	10 ▼
JSON_RPC	5 ▼	10 ▼	5 ▼	10 ▼
JSON_RPC_Notification	5 ▼	10 ▼	5 ▼	10 ▼
LACP	5 ▼	10 ▼	5 ▼	10 ▼
LLDP	5 ▼	10 ▼	5 ▼	10 ▼
Loop_Protect	5 ▼	10 ▼	5 ▼	10 ▼
MAC_Table	5 ▼	10 ▼	5 ▼	10 ▼
Maintenance	15 ▼	15 ▼	15 ▼	15 ▼
MVR	5 ▼	10 ▼	5 ▼	10 ▼
NTP	5 ▼	10 ▼	5 ▼	10 ▼
Ports	5 ▼	10 ▼	1 ▼	10 ▼
Private_VLANs	5 ▼	10 ▼	5 ▼	10 ▼
PTP	5 ▼	10 ▼	5 ▼	10 ▼
QoS	5 ▼	10 ▼	5 ▼	10 ▼
RMirror	5 ▼	10 ▼	5 ▼	10 ▼
Security	5 ▼	10 ▼	5 ▼	10 ▼
sFlow	5 ▼	10 ▼	5 ▼	10 ▼
Spanning_Tree	5 ▼	10 ▼	5 ▼	10 ▼
System	5 ▼	10 ▼	1 ▼	10 ▼
UDLD	5 ▼	10 ▼	5 ▼	10 ▼
UPnP	5 ▼	10 ▼	5 ▼	10 ▼
VCL	5 ▼	10 ▼	5 ▼	10 ▼
VLAN_Translation	5 ▼	10 ▼	5 ▼	10 ▼
VLANs	5 ▼	10 ▼	5 ▼	10 ▼
XXRP	5 ▼	10 ▼	5 ▼	10 ▼

Figure 16: List of group to be classified with privilege levels (default config)

Group Name column shows all functions families allowed to be used in the privilege level settings.

- **Configuration Read-only** : select the privilege level number which will be allowed to only read configuration parameters.
- **Configuration/Execute Read/write** : select the privilege level number which will be allowed to read and write configuration parameters.
- **Status/Statistics Read-only** : select the privilege level number which will be allowed to only read status and statistics parameters.
- **Status/Statistics Read/write** : select the privilege level number which will be allowed to read and write status and statistics parameters.

User privilege level should be the same or greater than the Privilege Level assigned to a function to have access at that group.

4.3 Authentication Methods

There are three authentication methods available to access S20: local, RADIUS or TACACS+, been the last two remotes. It is possible to select an authentication type for each of the access protocols: console interface (USB), telnet, SSH and HTTP can have different authentication methods each.

When the local authentication is chosen. the user database (username, password and privilege levels) will be stored at the switch's internal memory, and can be accessed and managed when setting the switch. In

this case, the administrator must have access to the interfaces available, e.g., Ethernet connection or USB interface connection.

When using remote authentication method, either RADIUS or TACACS+ servers, it is required a server which stores and manages the users accounts. To connect to the remote server, a hostname and password (key) must be properly configured in AAA section.

Possible configurations for Authentication Method are as follows.

- **Authentication Method Configuration** : define how the user will be authenticated when accessing through each interface (console, SSH, Telnet or HTTPS). First column is the main method. After a timeout of the main method of authentication, the method selected at the second column will be tried. Finally, after the timeout of the second chance, it will be tried to authenticate the user by the method selected at the third column.
 - **Methods:** select the three authentication methods:
 - **Local:** authentication of this client will be done locally through equipment database;
 - **Radius:** authentication of this client will be done remotely through a Radius server;
 - **Tacacs:** authentication of this client will be done remotely through a TACACS+ server;
 - **No:** authentication is disabled in this client and login is not possible.
- **Command Authorization Method Configuration** : define how the user will be authenticated when using the CLI (Command Line Interface) when accessing from console, SSH or Telnet.
 - **Method:** select the authentication method of this client. Allowed methods are:
 - **Tacacs:** authentication of this client will be done remotely through a TACACS+ server;
 - **No:** authentication is disabled in this client and login is not possible.
 - **Cmd Lvl:** allow all commands of this client with privilege level higher than the Cmd Lvl value. That is, this value will be the lowest Privilege Level required to use the CLI interface. Valid values are from 0 to 15;
 - **Cfg Cmd:** enable configuration commands at this interface.
- **Accounting Method Configuration** : define how the user will be authenticated when doing users' accounting (console, SSH or Telnet).
 - **Method:** select the authentication method of this client. Allowed methods are:
 - **Tacacs:** authentication of this client will be done remotely through a TACACS+ server;
 - **No:** authentication is disabled in this client and login is not possible.

- **Cmd Lvl**: enable accounting of all commands of this client with privilege level higher than the Cmd Lvl value. That is, this value will be the lowest Privilege Level required to do accounting. Valid values are from 0 to 15;
- **Exec**: enable exec (login) accounting at this interface.

4.4 Telnet/SSH Protocols

Telnet and SSH (Secure Shell) protocols are available to access the Reason S20. By default, Telnet is disabled and SSH enabled, but they can be enabled/disabled if desired. By security means, the use of Telnet should be avoided and SSH preferred if CLI through Ethernet is necessary. The possible configurations is as below:

SSH/Telnet Configuration

- **SSH Mode**: enable/disable the SSH protocol.
- **SSH Max Connections**: Defines the maximum number of concurrent SSH client connections (from 1 to 20). CLI command is *"ip ssh max-connections"*.
- **SSH Timeout (minutes)**: The SSH Timeout specifies the timeout interval from an inactive session for USB/SSH connections. When the interval elapses without keyboard activity, the timeout occurs and the user has to authenticate again. Allowed values are in the range 0 through 1440, default being 10. The value 0 disables the session timeout. CLI command is *"ip ssh timeout"*.
- **Telnet Mode**: enable/disable the Telnet protocol.
- **Telnet Max Connections**: Defines the maximum number of concurrent Telnet client connections (from 1 to 20). CLI command is *"ip telnet max-connections"*.
- **SSH Timeout (minutes)**: The Telnet Timeout specifies the timeout interval from an inactive session for Telnet connections. When the interval elapses without keyboard activity, the timeout occurs and the user has to authenticate again. Allowed values are in the range 0 through 1440, default being 10. The value 0 disables the session timeout. CLI command is *"ip telnet timeout"*.

In case of using "Max Connections", admins should always be able to connect either by having a reserved session or disconnecting another user. In this last case, the first non-admin session is disconnected, if none, the oldest admin session.

SSH Authorized Keys

The SSH Authorized Keys specifies the SSH keys that can be used for logging into the user account without a password.

4.5 HTTP/HTTPS Protocols

As the web interface is an easy and intuitive way to access the switch settings, the HTTPS protocol is available and enabled by default. HTTP is also available but disabled by default, as it should be avoided and HTTPS preferred. In case HTTP is enabled, it is recommended to keep HSTS header (automatic redirect) also enabled so the browser can identify that a secure connection can be established automatically.

Howsoever, it is highly recommended to keep both HTTP and HTTPS protocols disabled once the S20 is properly configured and ready to be placed in operation. As SSH and Telnet are also recommended to be disabled, the USB local interface (using CLI commands) may be used to reenables Web Interface communication.

The HTTP / HTTPS configuration is as follows:

- **HTTPS:** select if HTTPS should be enabled or not, by default it is enabled. Automatic redirect can only be enabled if HTTPS is enabled too.
- **HTTP:** select if HTTP should be enabled or not. By default it is disabled.
- **Max Connections :** Defines the maximum number of concurrent HTTP/HTTPS client connections (from 1 to 20). CLI command is "*ip http max-connections*".
- **Automatic Redirect :** select if HTTP connections should be automatically redirected to HTTPS connections, using the HSTS header.
 - **Enabled:** HSTS header enabled;
 - **Disabled:** HSTS heard disabled.
- **HTTP/S Timeout (minutes) :** The HTTP/S Timeout specifies the timeout interval from an inactive session for web interface connections. When the interval elapses without keyboard activity, the timeout occurs and the user has to authenticate again. Allowed values are in the range 0 through 1440, default being 60. The value 0 disables the session timeout. CLI command is "*ip http secure-timeout*".
- **SSL Configuration:** Specify the SSL configuration used to negotiate a connection with a remote client.
 - **Custom:** For services that need customized cipher suites.
 - **Secure:** For services that do not need backward compatibility, provide a higher level of security. This configuration is compatible with Firefox 27, Chrome 30, IE 11 on Windows 7, Edge, Opera 17, Safari 9, Android 5.0, and Java8.
 Protocol: TLS v1.2
 Cipher suite: ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-

RSA-AES128-GCM-SHA256:ECDSA-AES256-SHA384:ECDSA-AES256-SHA384:ECDSA-AES128-SHA256:ECDSA-AES128-SHA256

- **Default:** For services that do not need compatibility with legacy clients (mostly WinXP), but still need to support a wide range of clients. It is compatible with Firefox 1, Chrome 1, IE 7, Opera 5 and Safari 1. This is the default option.

Protocols: TLS v1.2, TLS v1.1, TLS v1

Cipher suite: ECDHE-ECDSA-CHACHA20-POLY1305:ECDSA-AES128-GCM-SHA256:ECDSA-AES256-GCM-SHA384:ECDSA-AES128-SHA256:ECDSA-AES256-SHA384:ECDSA-AES128-SHA256:ECDSA-AES128-SHA:ECDSA-AES256-SHA384:ECDSA-AES256-SHA:ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDSA-DES-CBC3-SHA:ECDSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:IDSS

- **Compatible:** This is the old cipher suite that works with all clients back to Windows XP/IE6. It should be used as a last resort only.

Protocols: TLS v1.2, TLS v1.1, TLS v1, SSL v3

Cipher Suite: ECDHE-ECDSA-CHACHA20-POLY1305:ECDSA-AES128-GCM-SHA256:ECDSA-AES128-GCM-SHA256:ECDSA-AES256-GCM-SHA384:ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:KEDH+AESGCM:ECDSA-AES128-SHA256:ECDSA-AES128-SHA:ECDSA-AES128-SHA:ECDSA-AES256-SHA384:ECDSA-AES256-SHA384:ECDSA-AES256-SHA:ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:ECDSA-DES-CBC3-SHA:ECDSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES-DES-CBC3-

SHA:HIGH:SEED:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5!
 PSK:!RSAPSK:!aDH:!aECDH:!EDH-DSS-DES-CBC3-
 SHA:!KRB5-DES-CBC3-SHA:!SRP

- **Certificate Maintain** : select which mode should be used to maintain HTTPS certification. Only allowed when Mode is disabled.
 - **None**: no action to maintain certification will be done;
 - **Delete**: delete certification;
 - **Upload**: upload the certification. If allowed, the PassPhrase, Certificate Upload and File Upload fields will appear. Possible values are as follows.
 - **PassPhrase**: type the pattern that will be used for encrypting the certification;
 - **Certificate Upload** : select certification upload method. Possible modes are Web Browser and URL. Possible configurations are as follows:
 - **Web Browser** : certificate upload is done via Web Browser. When using this method, it is necessary to upload a valid Web Browser file to do certification upload at the File Upload row;
 - **URL**: certificate upload is done through a given address. When using this method, it is necessary to type the URL to be used at the URL row, using the following methodology:
 <protocol>:// [<username>[:<password>]@]<host>[:<port>] [/<path>];
 - **Generate**: generate the certification. If allowed, Certificate Algorithm field will appear. Possible values are as follows.
- **Certificate Status**: displays information of the status of the HTTPS actual certification at the switch. Possible values are as follows.
 - **Switch secure HTTP certificate is presented**: there is a certification stored in HTTPS database;
 - **Switch secure HTTP certificate is not presented**: there is no certification stored in HTTPS database;
 - **Switch secure HTTP certificate is generating...** : switch is generating a certification to be stored in HTTPS database.

4.6 Access Management

Access can be restricted to a determined VLAN or IP address range. For each group of VLAN and IP address range, the type of communication protocol enabled may be chosen: HTTP/HTTPS, TELNET/SSH and SNMP protocol for remote monitoring.

By default it is disabled, meaning any user from any IP address or VLAN through any access protocol can access the equipment. If enabled, this

menu allows controlling the VLAN, IP range and protocol. The maximum number of filters to apply at Access Management is 16.

If access management is **enabled**, at the **Add New Entry** gives the possibility to insert a new filter to be applied at the access interfaces.

- **Delete:** click at the button to delete the filter at the row;
- **VLAN ID:** specify the VLAN identifier allowed to access management interfaces. Allowed values are the VLAN allowed values (from 1 to 4,095);
- **Start IP Address:** specify the lowest IP address allowed to access management interfaces. IP address must be inserted in dotted decimal notation;
- **End IP Address:** specify the highest IP address allowed to access management interfaces. IP address must be inserted in dotted decimal notation;
- **HTTP/HTTPS:** enables, if checked, the host to access the switch through HTTP and HTTPS protocol at the configured VLAN and the specified range of IP addresses;
- **SNMP:** enables, if checked, the host to access the switch through SNMP protocol at the configured VLAN and the specified range of IP addresses;
- **Telnet/SSH:** enables, if checked, the host to access the switch through Telnet or SSH interface at the configured VLAN and the specified range of IP addresses.

5 Simple Network Management Protocol (SNMP)

The SNMP protocol was created in the mid 1990's to increase management information allowed by network devices to send to workstations. Creating a protocol to send standardized information over IP networks to a server has increased network maintenance and diagnostics capability. There are dozens of RFC documents related to SNMP, such as the RFC 1157 (A Simple Network Management Protocol) or RFC 3418 (Management Information Base (MIB) for the Simple Network Management Protocol). When using this protocol, it is important to list relevant RFC documentation to the application.

5.1 SNMP Fundamentals

Reason S20 supports the three SNMP versions v1, v2c and v3, and RFC 3584 standardized that all versions can coexist in a network. Whilst SNMPv1 networks can include SNMPv3 or SNMPv2c protocols, the capabilities of the SNMPv1 agents are not the same. When using different SNMP versions, make sure that the SNMP manager understands all used versions of the protocol. Among other, the general information and management available through SNMP is:

- Interface speed and usage;
- Equipment Serial Number and its location;

- CPU and memory usage;
- Internal temperature;
- Link errors;
- Time since last system boot;
- Alarms status;
- Enable/disable management communication protocols: HTTP/HTTPS, SSH and Telnet;
- Configuration file download and upload;
- Firmware upgrade.

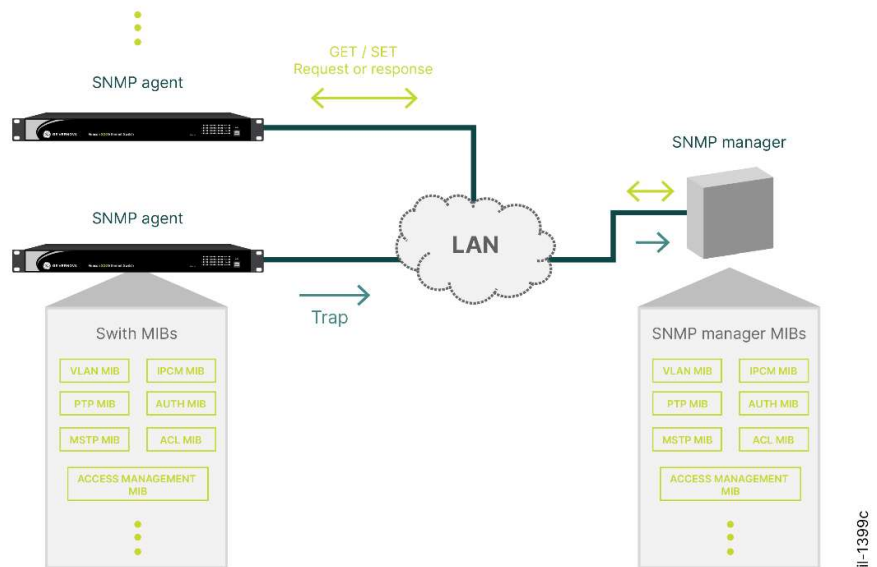


Figure 17: Example of SNMP management architecture

General operation is based on GET and SET requests, done by SNMP manager to the agents. In this operation, the manager will poll information from the agents periodically, apart from the information that is received at the time it occurs. Examples like Link up, STP protocol information or switch Cold Start can be sent by SNMP agents without a request from the server. The last type of operation is called the Trap, and an asynchronous message received from an agent is called Trap message.

When SNMP information must be sent through the network, the agent will search at its own library of SNMP protocol information to search whether the request done by the manager can be satisfied. An Information library is called Management Information Base (MIB). Both manager and agent must have MIB libraries at its own hardware to understand the information exchanged between them. When it comes to Trap messages, there are some MIB libraries that can be set to be sent without the request from the manager.

5.2 SNMP Configuration

SNMP messages are exchanged in an IP network, generally using UDP transport protocol. UDP port 161 is used to send request messages, and UDP port 162 is used for traps.

By default, SNMP is disabled in Reason S20 switches and to change its configuration go to Settings > Security > Switch > SNMP.

System

System menu allows configuring basic SNMP settings and protocol enable. Allowed configuration is as shown below.

- **Mode:** select if SNMP should be enabled or not. Allowed values are **Enabled**, to enable the SNMP protocol usage or **Disabled**, to disable the SNMP protocol usage.
- **Version:** select which version of SNMP should be used. Allowed values are **SNMPv1**, **SNMPv2c** and **SNMPv3**;
- **Read Community :** indicate the community read access string, which will permit SNMP agent access. Used only on SNMPv1 and SNMPv2c versions. SNMPv3 version community information is get at the communities table. Allowed string length is up to 255 and allowed characters are the ASCII characters from 32 to 126 (basically letters, numbers and other characters, such as “-” or “_”);
- **Write Community :** indicate the write community access string, which will permit SNMP agent access. Used only on SNMPv1 and SNMPv2c versions. SNMPv3 version community information is get at the communities table. Allowed string length is up to 255 and allowed characters are the ASCII characters from 32 to 126 (basically letters, numbers and other characters, such as “-” or “_”);
- **Engine ID:** indicates SNMPv3 engine ID. Used only on SNMPv3 version.

Trap

Trap menu allows configuring trap-sending messages throughout SNMP protocol. While SNMP general messages should be requested by an SNMP server, Trap messages are sent automatically when an event occurs (trap messages) or cyclically (inform messages, on SNMPv3). Allowed configuration is as shown below.

- **Global settings:** select if Trap messages sending should be Enabled or Disabled. By default, it is Disabled;

If Trap is enabled, it is necessary to configure which messages should be sent without request of the SNMP server. Using the **Add New Entry** button is possible to insert a new Trap to be applied. When clicked, it will appear the **SNMP Trap Configuration** menu, with the following fields to be configured:

- **Trap Config Name :** indicates Trap configuration name. Allowed characters are the ASCII characters from 33 to 126 (basically letters, numbers and other characters, such as “-” or “_”);
- **Trap Mode:** enable these settings to operate as SNMP Trap messages. Allowed values are Enabled or Disabled;

- **Trap Version**: select SNMP version of Trap messages. Allowed values are SNMPv1, SNMPv2c and SNMPv3;
- **Trap Community**: indicates Trap community name. Allowed characters are the ASCII characters from 33 to 126 (basically letters, numbers and other characters, such as “-” or “_”);
- **Trap Destination Address**: indicates the destination of the Trap messages, that is, the SNMP server responsible for this node. IP address must be inserted in dotted decimal notation;
- **Trap Destination Port**: indicates UDP port used to transport Trap messages. By default this value is 162. Allowed values are from 1 to 65,535 UDP port;
- **Trap Inform Mode**: enable these settings to enable Trap messages operation in inform mode. In this case, Trap messages of this Trap Config Name will be sent cyclically at a given time. Only SNMPv3 supports this mode of operation. Allowed values are Enabled or Disabled;
- **Trap Inform Timeout (seconds)**: indicates Trap Inform operation timeout. By default this value is 3 seconds. Allowed values are from 0 to 2,147 seconds;
- **Trap Inform Retry Times**: indicates how many times a Trap Inform operation will retry sending an inform message. By default this value is 5 times. Allowed values are from 0 to 255 times;
- **Trap Probe Security Engine ID**: enable using engine ID as credentials to SNMP Trap Probes. Allowed values are Enabled or Disabled;
- **Trap Security Engine ID**: indicates engine ID used as credential to SNMP Trap Probes. If Trap Probe Security Engine ID is Enabled, engine ID shown in the System menu is used. Otherwise, value at this field will be used as engine ID;
- **Trap Security Name**: indicates Trap security name. If trap and informs messages are used, it is required to each one have its own security name.

After defining Trap and Inform basic sending and authentication configurations, it is necessary to inform, at the given Trap configuration, which event will send these messages. These settings are done at the SNMP Trap Event field. Allowed configuration is as shown below.

- **System**: enable the Warm Start or Cold Start trap message. The “*” checkbox selects automatically all possibilities;
- **Interface**: enable the Port Up, Port Down and LLDP protocol trap message. None option means no port configured to send trap message, specific option allows the user to select which ports will generate a trap message and all switches selects all ports to generate a trap messages. Link Up, Link Down and LLDP ports can be freely configured;
- **Authentication**: enable the SNMP Authentication Fail message to generate a trap message;
- **Switch**: enable the STP and RMON trap messages to be sent.

Communities

Communities menu allows configuring SNMPv3 communities table. By default, public and private communities are created. To add new communities, click at the Add New Entry button. When clicked, it will appear the following fields to be configured:

- **Delete:** click at the button to delete the filter at the row;
- **Community:** indicates community name to permit access of a SNMPv3 agent. Maximum community name length is 32, and allowed characters are the ASCII characters from 33 to 126 (basically letters, numbers and other characters, such as “-” or “_”). For SNMPv1 and SNMPv2c, community name will be treated as security name.
- **Source IP:** indicates SNMP access source address. IP address must be inserted in dotted decimal notation;
- **Source Mask:** indicates SNMP access source mask address. Mask address must be inserted in dotted decimal notation.

After one of the configurations described before is changed, there are two buttons that allow the user to save or discard the configurations.

- **Save:** save configuration at the Running Config;
- **Reset:** undo changes made locally at the Running Config.

Users

Users menu allows configuring SNMPv3 user configuration. To add new users, click at the Add New Entry button. When clicked, it will appear the following fields to be configured:

- **Delete:** click at the button to delete the filter at the row;
- **Engine ID:** indicates the engine ID used by the user. Engine ID equal to switch engine ID means local user, and different engine ID means remote user. Engine ID number must be inserted in hexadecimal format;
- **User Name:** indicates the name of the user configured at the given engine ID. Maximum community name length is 32, and allowed characters are the ASCII characters from 33 to 126 (basically letters, numbers and other characters, such as “-” or “_”);
- **Authentication Protocol :** select the protocol which will be used to authenticate the user. Possible values are as follows.
 - **None:** No authentication protocol is used on this user;
 - **MD5:** MD5 protocol is used to authenticate this user. Enabling this field allows the switch to create a flag to indicate this protocol usage;
 - **SHA:** SHA protocol is used to authenticate this user. Enabling this field allows the switch to create a flag to indicate this protocol usage.
- **Authentication Password :** the password that will be used to identify this user. Password length for MD5 protocol should be from 8 to 32 characters, and for SHA protocol should be from 8 to 40 characters. Allowed characters are the ASCII characters from 33 to

126 (basically letters, numbers and other characters, such as “-” or “_”);

- **Privacy Protocol**: select the privacy protocol that this entry will participate. Possible values are as follows.
 - **None**: No privacy protocol is used on this user;
 - **DES**: DES protocol is used. Enabling this field allows the switch to create a flag to indicate this protocol usage;
 - **AES**: AES protocol is used. Enabling this field allows the switch to create a flag to indicate this protocol usage.
- **Privacy Password**: the password that will be used to identify this user. Password length should be from 8 to 32 characters. Allowed characters are the ASCII characters from 33 to 126 (basically letters, numbers and other characters, such as “-” or “_”);

After one of the configurations described before is changed, there are two buttons that allow the user to save or discard the configurations.

- **Save**: save configuration at the Running Config;
- **Reset**: undo changes made locally at the Running Config

Groups

Groups menu allows configuring SNMPv3 group table. By default, default_ro_group and default_rw_group are created. To add new group, click at the Add New Entry button. When clicked, it will appear the following fields to be configured:

- **Delete**: click at the button to delete the filter at the row;
- **Security Model**: select security model to be used in that given group. Allowed values are v1, v2c and usm. USM security model is the user-based security model. V1 and v2c security models are reserved for SNMPv1 and SNMPv2c use;
- **Security Name**: select the security name that the group will belong to. Possible values are **public** and **private**, for v1 and v2c security models, and **default_user** for usm security model;
- **Group Name**: indicates the name of the created group. Maximum community name length is 32, and allowed characters are the ASCII characters from 33 to 126 (basically letters, numbers and other characters, such as “-” or “_”).

Views

Views menu allows configuring SNMPv3 views table to select what should appear or not at the OID SNMP tree. By default, default_view is created. To add new view, click at the Add New Entry button and the following field will appear:

- **Delete**: click at the button to delete the filter at the row;
- **View Name**: indicates the name of the created view. Maximum community name length is 32, and allowed characters are the ASCII characters from 33 to 126 (basically letters, numbers and other characters, such as “-” or “_”);
- **View Type**: select if this view should be included at the SNMP OID sub tree or not. Possible values are **included** or **excluded**. Included

means that this view will appear at the OID sub tree and excluded means that this view will not appear at the OID sub tree;

- **OID Subtree:** indicates the OID defining the root of the subtree, to add to the named view. Allowed OID length is 128, and allowed characters are numbers and the "*" character, always preceded by a dot (examples: .1, .2, .*, etc.).

After one of the configurations described before is changed, there are two buttons that allow the user to save or discard the configurations.

- **Save:** save configuration at the Running Config;
- **Reset:** undo changes made locally at the Running Config.

Access

Groups menu allows configuring SNMPv3 access table. By default, default_ro_group and default_rw_group are created. To add new access configuration, click at the Add New Entry button and the following field will appear:

- **Delete:** click at the button to delete the filter at the row;
- **Group name:** select group name to be configured. Group names listed are get from the Groups menu;
- **Security Model:** select security model to be used in the access. Allowed values are any, v1, v2c and usm. Choose any if any security model may be used. USM security model is the user-based security model. V1 and v2c security models are reserved for SNMPv1 and SNMPv2c use;
- **Security Level:** select the security model to be used for the selected group. Possible values are NoAuth, NoPriv, Auth, NoPriv and Auth, Priv. "No" at the beginning means no use of authorization or privacy. Thus, it is possible to choose from no authentication and no privacy, authentication and no privacy and, finally, authentication and privacy security levels;
- **Read View Name:** select the name which will be shown of this MIB when requested current values. Possible values are None, default_view or the name of a given view. None means no view name, default_view means that MIB will be displayed as default_view and, if a view is created, its name typed at the Views menu can be used as MIB's name;
- **Write View Name:** select the name which will be shown of this MIB when potentially set new values. Possible values are None, default_view or the name of a given view. None means no view name, default_view means that MIB will be displayed as default_view and, if a view is created, its name typed at the Views menu can be used as MIB's name;

6 Aggregation Settings

Link Aggregation function is defined by the IEEE 802.3ad standard. The purpose of Link Aggregation is to increase the performance and the availability of network devices with more than one connection, making

parallel links work as if they were a single high performance link. This function is also known as Port Trunking or Port Bundling. The main benefits of using link aggregation are:

- Increased communication capacity;
- Load balance on links;
- Increased communication availability.

Trunking can refer to Trunk port (RSTP protocol), which forwards data of many VLAN-tagged frames or, in this context, to backbone connections. This manual uses the term 'Aggregated-link' when referring to links operating in aggregation.

Nowadays, link speed generally is not the major difficulty when upgrading a LAN. As network devices are getting less expensive, upgrading the devices to a higher speed device is generally possible. Besides, when it comes to redundancy, the aggregation function can have great benefits to a given connection between two stations. As the behavior of two links will be as if they are one, there will be redundancy in the connection between these stations. If one of the links fails, network speed will decrease, but it will continue operating.

When using this function, it is important to know that some features, such as VLANs, STP protocol or CoS operations will operate as if aggregated links are just one port. Thus, the physical loop created when connecting two bridges together will not be detected by the STP protocol, as the aggregation function will logically merge the ports.

The figure below shows an example of the link aggregation between two network devices, and the behavior of the protocol when there is an aggregated link failure.

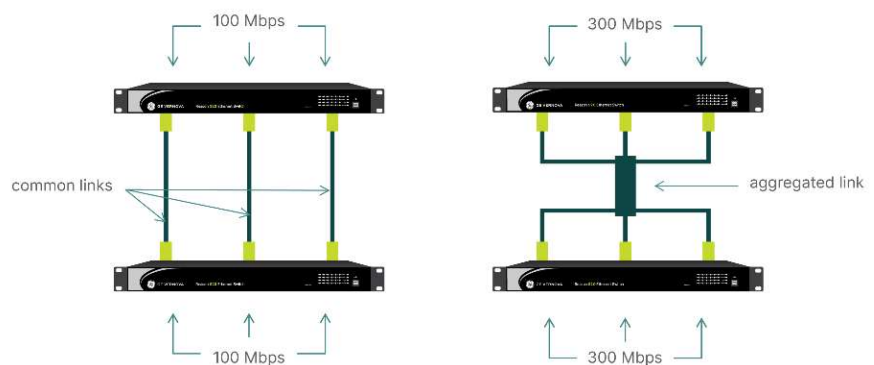


Figure 18: Comparison between common and aggregated links speed

IL-1400

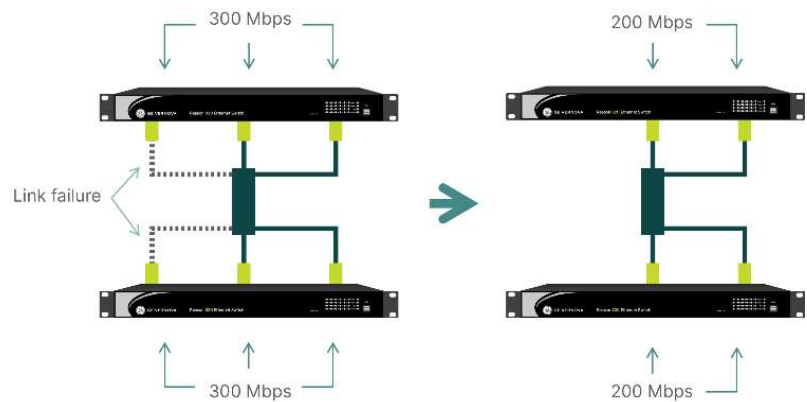


Figure 19: Link failure behaviour of an aggregated link

In aggregated links, load balancing would not be perfect because the way traffic is redirected on links. Thus, if three 100 Mbps aggregated links is used; it is possible that the resulting link is not a 300 Mbps link.

To guarantee operation of Aggregation function, links must operate in full-duplex mode and at the same speed. Thus, different speed ports should not be used as aggregated links.

Care must be taken when configuring Aggregation function in a switch. As the physical topology will create loops in the network, it is recommended to configure both switches before enabling the ports used.

To use this function, both network equipment connected must be aware to perform aggregation. Besides, aggregated ports must be at the same aggregation group ID. Reason S20 can create up to 12 groups, and the maximum allowable ports for one group are the maximum number of ports the switch has.

Aggregation load balancing are performed based in some aspects of the traffic at the ports. Reason S20 can share the links based on the following aspects:

- Source MAC address;
- Destination MAC address;
- IP Address;
- TCP/UDP port number.

This means that traffic from a given source MAC address will be redirected through a given port of the aggregated link. Traffic based on other parameters should use other link. Thus, if there is different bandwidth traffic between end nodes, there will be a non-perfect load balancing. In the end, the apparent link speed will increase, and there will be a redundant path for the traffic of the end nodes. Figure below shows an example of

such behavior, and the method for load balancing used is source MAC address.

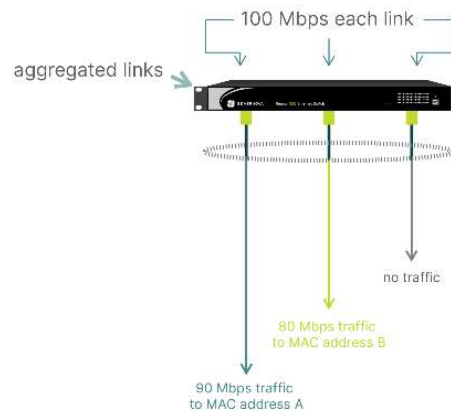


Figure 20: Load balancing in aggregated links

Even though the total speed of the ports is 300 Mbps, there are only 170 Mbps being used and one of the links is not forwarding any traffic. Even though there is one port available, if MAC address A or B requires more bandwidth, the extra traffic will be generated on ports already used.

6.1 Static Aggregation Configuration

Static aggregation will aggregate ports as user defines, without usage of automatic protocols.

Aggregation Static menu is located at Settings > Aggregation > Static.

Aggregation Mode Configuration

This menu contains the settings allowed to be used as filters in the static aggregation mode. At the Hash Code Contributors table, there are four checkboxes that can be selected to enable given parameters as static aggregation filter.

- **Source MAC Address** : traffic balancing will use source MAC address as filter. Source MAC address field at the Ethernet frame will be used to define on which port of aggregation group traffic will be redirected;
- **Destination MAC Address** : traffic balancing will use destination MAC address as filter. Destination MAC address field at the Ethernet frame will be used to define on which port of aggregation group traffic will be redirected;
- **IP Address**: traffic balancing will use IP address traffic as filter. IP addresses at the Ethernet frame will be used to define on which port of aggregation group traffic will be redirected;
- **TCP/UDP Port Number**: traffic balancing will use TCP or UDP port numbers as filter. TCP/UDP port number field at the Ethernet frame will be used to define on which port of aggregation group traffic will be redirected.

Aggregation Group Configuration

This menu allows defining which ports will be at the same group in static aggregation mode. At the table, there are the Group ID column and Port Members columns.

Two ports belonging at the same Group ID means that they will behave as only one port, and MAC address used in traffic flow will be the lowest port number MAC address. Maximum number of group aggregation allowed will be half of total port numbers, that is, minimum aggregation Group must have at least two ports. By default, all ports belong to Normal Group ID. Possible configurations are as follows.

- **Port Members**: select which ports will be member of a given Group ID number. Same group ID ports means that these ports will operate as aggregated ports.

When using aggregated ports, both sides of the traffic path must be configured to operate as Aggregated Static Ports, and both sides must be in the same Group ID. That means to use aggregation function, both switches connected or both nodes must support Aggregation protocol. In addition, they must be configured to use the same Hash Code Contributors and ports connected to be used must belong to the same Group ID number.

After one of the configurations described before is changed, there are buttons that allow the user to save or discard the configurations.

- Save: save configuration at the Running Config;
- Reset: undo changes made locally at the Running Config.

6.2 Link Aggregation Control Protocol (LACP) Settings

Aggregation LACP menu allows configuring dynamic port aggregation on the switch. Link Aggregation Control Protocol will aggregate ports automatically when two Aggregation nodes are connected, and ports connected allow being used in aggregation mode.

Aggregation LACP menu is located at Settings > Aggregation > LACP.

LACP Port Configuration

All allowed configurations are displayed by default. The first column displays port number that is being configured in a given row. Other columns allow configuration of a port as shown below.

- **LACP enabled**: enable LACP protocol usage at the port. Checkbox selected means LACP enabled, and checkbox empty means disabled. Maximum Aggregation groups allowed when using LACP protocol is 32;
- **Key**: indicates the key used at the port, which represents port speed capabilities. Two ports only could be used in aggregated mode if they have same speed capabilities, that is, the same key. If Auto is selected, Reason S20 uses key value 1 to 10 Mbps ports, key value 2 to 100 Mbps ports and key value 3 to 3 Gbps ports. If Specific is selected, user can define port key. In Specific mode, allowed values are integer numbers from 1 to 65,535.

- **Role:** indicates LACP activity rules for use. Active operation means port will transmit frames automatically, and passive operation means port will only transmit messages as response to received LACP messages from the other side of the link. If Active is selected, port will transmit LACP packets each second when operating (port enabled). If Passive is selected, port will not transmit LACP packets until there is no reception of LACP messages from the other side of the link;
- **Timeout:** indicates LACP timeout between transmissions of LACP packets. Fast will allow transmitting LACP messages each second and Slow will allow transmitting LACP messages each 30 seconds.
- **Prio:** indicates port priority to be used by LACP protocol. If LACP partner try to form a larger group than supported by the device, this value will be used to define which ports will be used. Lower priority numbers means higher priority, and group will be created with higher priority ports. Values allowed are integer numbers from 1 to 65,535.

7 Loop Protection

Reason S20 support detection and protection from a network loop in two ways, using spanning tree protocols or using the Loop Protection function. This section shows the Loop Protection function. Refer to next section for spanning tree protocol description.

7.1 Loop Fundamentals

In a network, a loop can be understood as more than one connection paths between endpoints. Typical examples of loop is connecting two switches using more than one port, as occurs in a ring topology, or connecting a port to another port of the same switch. The figure below exemplifies a loop topology.

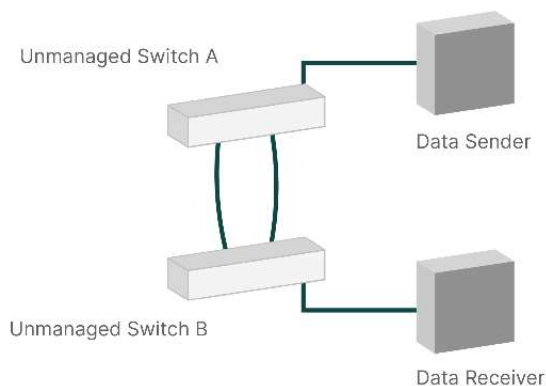


Figure 21: Bridge Loop

In the bridge loop given, there are three main problems:

- Unicast frame duplication;
- Multicast frame flooding;
- Address table non-convergence.

If the Data Sender starts transmitting data to the Receiver, switch A will understand that the Receiver is in two different ports, and thus will send data through both ports. Switch B will map MAC address of the Receiver at two ports and thus will send it from both. This behavior will insert duplicate frames for each data transmitted, which can cause undesirable behavior of nodes, like an application crash.

If the Data Sender starts a multicast communication, the link between the switches would become quickly saturated. As the switch operates as a transparent bridge, multicast frames must be delivered to all ports, except the incoming port. In the example given, switch A will send the multicast to switch B through all ports.

Switch B will execute the switch algorithm and will send the multicast frame to all ports, except the incoming frame port. Thus, the multicast received in one port will be replicated to the other connected port, and so on. Since Layer 2 header does not support a time to live (TTL), every multicast frame will be endless replicated until there is resource exhaustion or a crash happens in the network.

Finally, MAC address table will not converge the actual topology, as the Sender and Receiver port will continuously change. If the Sender starts a communication with the Receiver, switch A and B will view initially that the position of the Receiver is one port, and then another. This behavior will make the switch continuously recalculate its MAC addresses table, leading to traffic loss.

Redundancy might be a requirement in networks. The redundant path is possible due to the usage of redundancy or loop resolution protocols. For loop resolution, the most common is Spanning Tree protocols, and for link redundancy the Link Aggregation protocol.

7.2 Loop Protection

The Loop Protection function is used to prevent loops between one port and another at the same switch, or at ports connected to unmanaged switches, thus interfering in its operation. To prevent problems caused by these situations, the Loop Protection function must be enabled at ports where loop could happen.

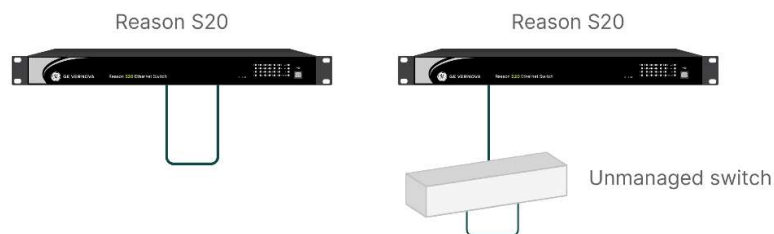


Figure 22: Usage situations for Loop Protection

The function is executed by sending messages throughout the ports that are enabled to send loop detection protocol. If a port that has been enabled

to send loop detection packet receives it, this port will be shutdown, as it will detect a loop in this port.

It is possible to define the repetition time of the packet and the time that a given port will remain off if a loop is detected. Besides, each port can be freely set to have the function enabled and send or not loop detection packets. If a loop is detected, there are three actions allowed:

- Shutdown port;
- Shutdown and log;
- Log only.

If the Log option is enabled, a log server must be configured to send the log messages informing the loop detection of a given port.

7.3 Loop Protection Configuration

This function applies for loop created directly or loop created in unmanaged switches connected in one port of Reason S20. A loop is detected using loop protection messages (PDU messages).

Loop Protection menu is located at Settings > Loop Protection.

General Configuration

This menu shows the settings related to enabling and the times related to this function.

- **Enable Loop Protection** : enable loop protection function. Enable will allow the function to be operating and Disable will shut down loop protection function;
- **Transmission Time**: indicates the interval between each loop protection message sent to the network. Allowed values are from 1 to 10 seconds, and default value is 5 seconds;
- **Shutdown Time**: indicates the period in seconds that the port will be disabled when a loop is detected and port is configured to shut down when this occurs. Allowed values are from 1 to 604,800 seconds, and default value is 180 seconds.

Port Configuration

This menu contains the settings allowed to perform when a loop is detected. The first column displays port number that is being configured in a given row and other columns allow configuration of that port. If one configuration is desired to be applied at all ports, then the row “*” should be used, that is, configuration done in the “*” row will be replied to all ports. Possible configurations are as follows.

- **Enable**: enable loop protection function at the port. Checkbox selected means LACP enabled, and checkbox empty means disabled;
- **Action**: indicates the action to be executed when a loop is detected at the port. Allowed values are as follows:
 - **Shutdown Port**: indicates that port will be disabled when a loop is detected on the port. The period that the port will remain disabled is the period defined at the Shutdown Time field;

- **Shutdown Port and Log** : indicates that port will be disabled when a loop is detected and switch will send a log message to the log server configured at System Log menu. The period that the port will remain disabled is the period defined at the Shutdown Time field;
- **Log Only**: indicates that switch will send a log message to the log server configured at System Log menu when a loop is detected on the port.
- **Tx Mode**: indicates if ports are sending loop protection messages or just listening for looped PDU messages at the network. If Enabled is selected, port will effectively send messages, and if Disabled, port will only wait for looped PDU loop protection messages.

8 Spanning Tree Protocol (STP)

Spanning Tree protocol is a mechanism created to solve the problems that arise when a loop is inserted into a LAN. As shown in the Loop fundamentals section, Ethernet networks were not developed to work in loop topologies. As redundant paths are generally required for most of network applications, several protocols have been developed to solve these problems.

The most common protocol to identify loops is the Spanning Tree Protocol, defined by IEEE 802.1D-2004. In addition, the IEC 61850-90-4 Technical Report specifies that for substation networks, Rapid Spanning Tree Protocol (RSTP) shall be used when looped topologies, such as ring topology, are required at the station level. This chapter will firstly introduce the STP fundamentals and later on explain how to configure it on Reason S20.

8.1 Spanning Fundamentals

This section will firstly introduce the STP fundamentals and later focus on the following protocols specifically:

- STP protocol;
- RSTP protocol;
- MSTP protocol.
- UltraRSTP

The need of a protocol to solve problem of loops in Ethernet networks started at the beginning of the commercial usage. As loops were required for better reliability of networks and loop-free topologies are difficult to maintain, automatic loop detection became a necessity. Therefore, the Spanning Tree protocol was created.

The protocol operates sending and receiving specific packets over the network, to map actual topology and act when required. The packets are

the BPDUs (Bridge Protocol Data Units) packets, and they are structured as shown below.

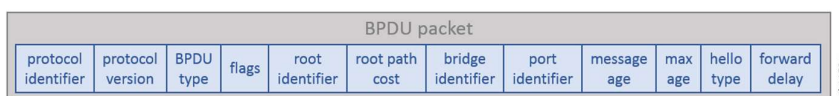


Figure 23: BPDUs Packet

By sending these packets over the network, switches can map physical topology to search for loops and disable them. Thus, the resulting logical topology will be a loop free tree topology. The following figure shows the possible paths for data traffic from IED A to IED B.

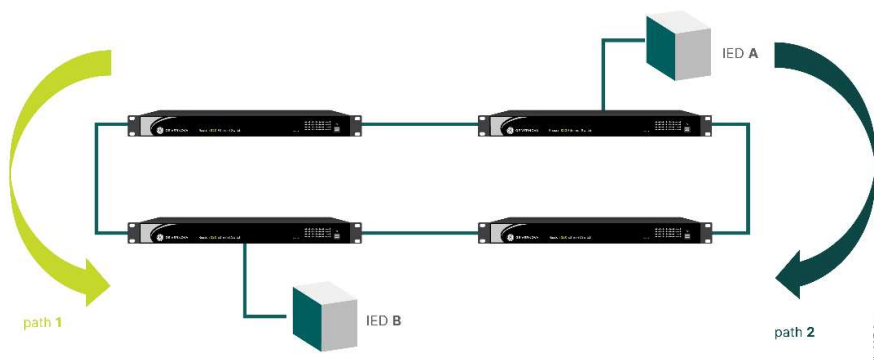


Figure 24: Ring topology LAN and possible paths for data traffic from IED A to B

The protocol works to create a logical topology that resembles a tree. The topology will have a root; branches that extend from it until reaching the leaves. The first step is to define where the root of the tree is, in other words, which will be the root switch. The root switch is the logical center of the topology and the remaining switches will be designed as bridge. After bridges are defined, the ports that are part of this bridge must be defined. They can be root port and designated port. A root port is the port of a designated bridge that leads to the root switch, and designated ports forwards traffic away from the root. If a port is not a designated port or a root port, it will be disabled otherwise will block traffic. There can be only one root port on a switch, and there may be multiple designated ports. To decide which switch will be the root, an election occurs between all Spanning Tree aware switches in a given LAN. Every switch has a bridge identifier, which contains information regarding the switch (generally the MAC address of the first Ethernet port) and the priority of the bridge. Bridges with lower priority number will have preference when the election occurs.

Beyond the bridge identifier, each port of the switch has a port identifier, containing the port number and port priority. If there is a tie in path cost, ports with lower priority number will have preference in the tree.

The path cost is a number that is used to Spanning Tree aware bridges to decide which path should be used as a tree branch. If the port has more speed capacity, the path cost will be lower. The lowest path cost to a bridge will be the path chosen. The following table exemplifies the recommended cost range to be used:

Recommended cost range of the paths:

Table 3: Spanning cost range recommendation

Data Rate	Recommended cost range
10 Mbps	50 – 600
100 Mbps	10 – 60
1 Gbps	3 - 10

The figure below presents an example of these definitions. The number shown is the bridge identifier, and the path costs to the entire physical topology is shown. On the example, all bridges priority and ports priority will be considered the same. Thus, the logical topology will be defined based only on path costs and bridge identifier. Furthermore, it is considered that all switches send and receive BPDUs to map topology and disable active loops

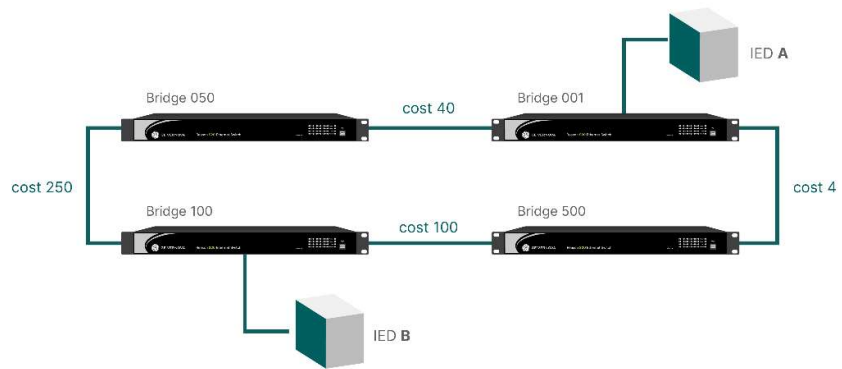


Figure 25: Example of a loop-topology showing bridge

In the example, the lowest bridge identifier is the Bridge 001. Thus, this switch will be the root bridge.

The path that will be used to send data over the network will be defined based on the path cost from the root bridge to the last node. If traffic from IED A to IED B goes through bridges 001 and 500, the total cost will be 104. However, if traffic from IED A to IED B goes through bridges 001, 050 and 100, the total cost will be 290. Thus, the first path will be used. After the election, the active logical topology will be as follows.

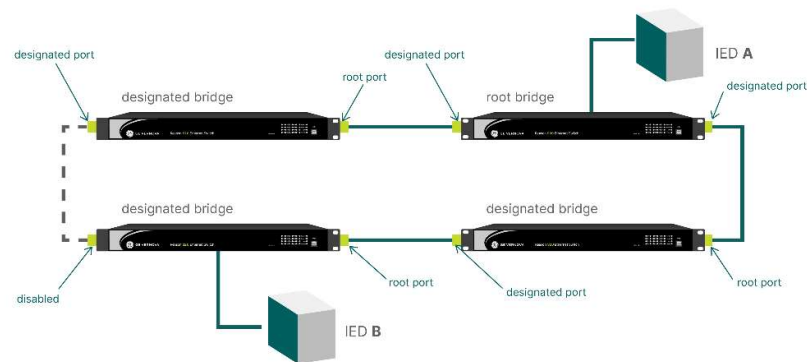


Figure 26: Logical topology after the Spanning Tree protocol was executed

The previous figure also shows how ports are defined as root and designated port. In case the port leads to a loop and it is the end of the tree branch, the port will be disabled. If there is a change in the topology, e.g., one of the branches is disconnected or a switch fails, there will be another election to find a root and the branches in the network. Thus, the physical network topology will have loops, but the logical will not.

When a bridge is initialized, or there is a change in the physical topology, all ports are in disabled state. After initialization, there will be traffic between them to define which ports will be non-designed (blocked) and which will be root or designated. After that, there will be the time to fill the MAC table (to learn all addresses), and then the port will forward traffic as a common switch port. The figure below demonstrates such steps, from the disabled to the forwarding state.

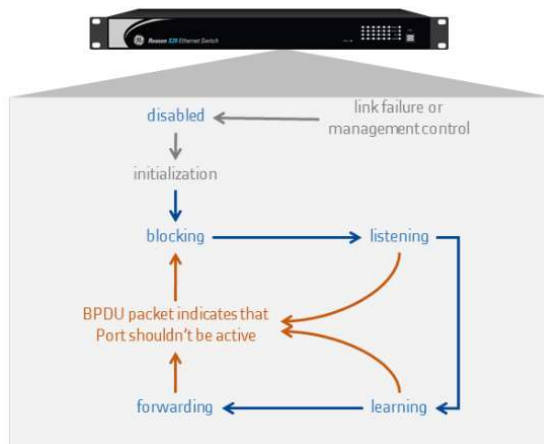


Figure 27: Port states in the Spanning Tree Protocol

Over the years, the protocol has evolved. After the first version of the Spanning Tree Protocol (STP), Rapid STP protocol was created to improve response time. When VLANs were introduced, Multiple STP protocol was created to identify loops inside VLANs. The following sections will describe these protocols, which are available for use in Reason S20.

STP Protocol

STP protocol mechanism was described at the section Spanning Tree fundamentals. However, the STP protocol has some unique characteristics. For start, the next figure illustrates how the ports would behave when

exchanging BPDU packets over the network and the maximum time allowed port changing state.

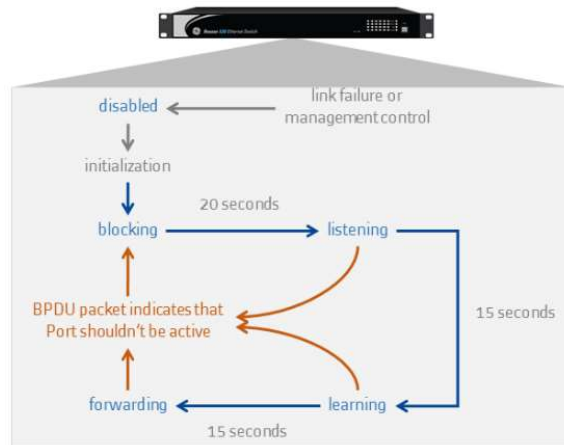


Figure 28: STP protocol mechanism and maximum port changing time

The table below illustrates the port state behavior over the STP protocol.

Table 4: Port State behavior using STP protocol

Port state	Send BPDU	Receive BPDU	Forward frames	Learn MAC addresses
Disabled	No	No	No	No
Blocking	No	Yes	No	No
Listening	Yes	Yes	No	No
Learning	Yes	Yes	No	Yes
Forwarding	Yes	Yes	Yes	Yes

It's important to note that changing from one state to another will occur only after the time to receive packets exceeds. Thus, it is possible that changing from blocking to forwarding state takes up to 50 seconds, considering the maximum time allowed. As conclusion, a topology change will be detected and corrected in dozens of seconds when the STP protocol is used. Generally, these timers are user-configurable, and then it is possible to change period of sending and receiving messages to increase its performance.

By default, Reason S20 is set to detect and correct a topology changing in up to 30 seconds using the STP protocol. The next figures illustrate what are these steps when a path of a given ring topology using STP fails. When there is a link failure or switch failure, each port will pass through all of the STP states until it starts sending packets again.

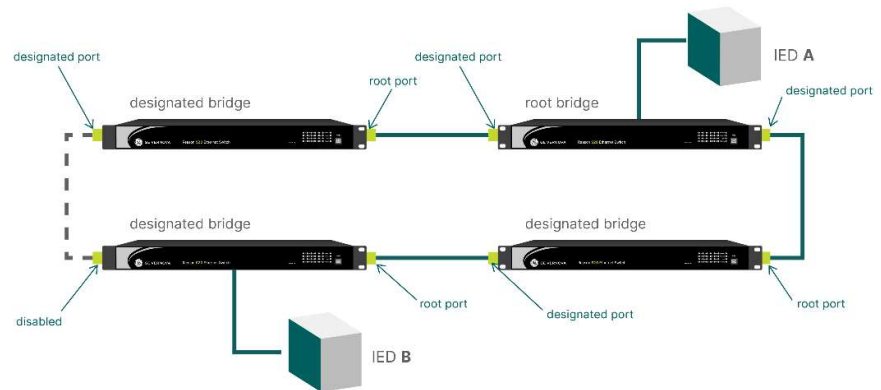


Figure 29: Port states when STP protocol is used in a ring physical topology

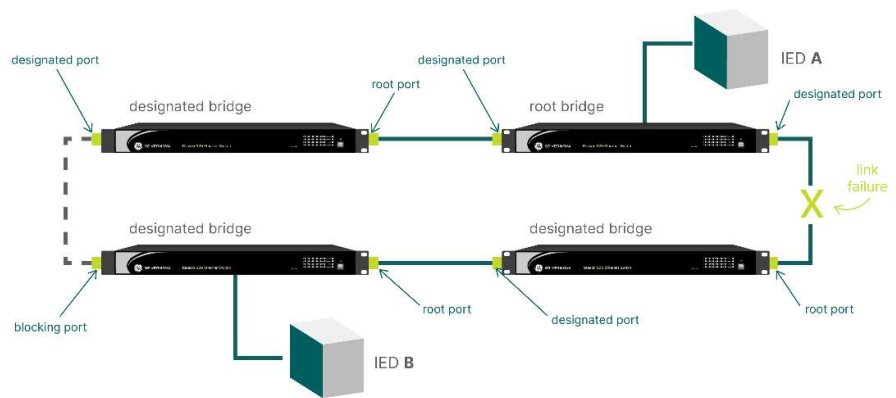


Figure 30: Failure on the designated link of the Spanning tree

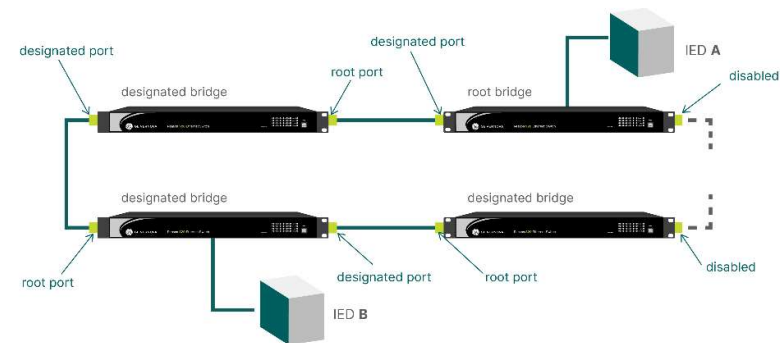


Figure 31: Reconfigured topology after a designated link failure

RSTP Protocol

STP protocol has a limitation regarding the time needed to rebuild a topology when there is a topology change. As shown in the previous section, the protocol waits for its timers to expire and then takes action, causing it to take several seconds to converge to a new topology. A faster protocol was required, leading to the creation of the Rapid Spanning Tree Protocol.

Defined by IEEE 802.1w, RSTP is an evolution from the STP protocol. It uses the same philosophy, such as the election of root bridge, but it has added some new characteristics and concepts to the STP protocol. The figure below shows the expected port behavior when using RSTP.

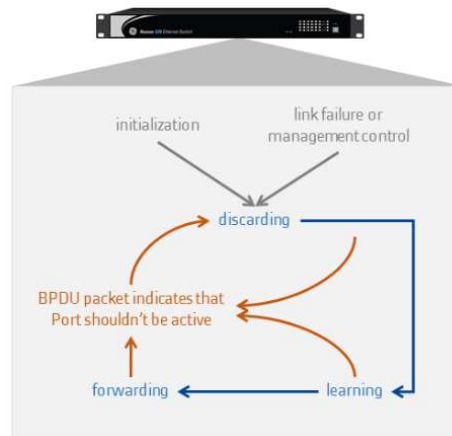


Figure 32: RSTP protocol mechanism

The table below illustrates the port state behavior over the RSTP protocol.

Table 5: Port State behavior using RSTP protocol

Port state	Send BPDU	Receive BPDU	Forward frames	Learn MAC addresses
Disabled	Yes	Yes	No	No
Learning	Yes	Yes	No	Yes
Forwarding	Yes	Yes	Yes	Yes

Compared to the STP protocol, the number of port states has decreased. In STP when a port is disabled, blocking traffic or listening to BPDU packets over the network equates to discarding state in RSTP. Learning and forwarding states remain as explained at the Spanning Tree fundamentals section.

When it comes to port definition, RSTP has changed some aspects from the STP protocol. While in STP there were blocking, disabled, designated and root ports, in RSTP they are defined as alternate, backup, designated and root ports.

Figure below exemplifies a topology after the RSTP protocol has identified all of the loops.

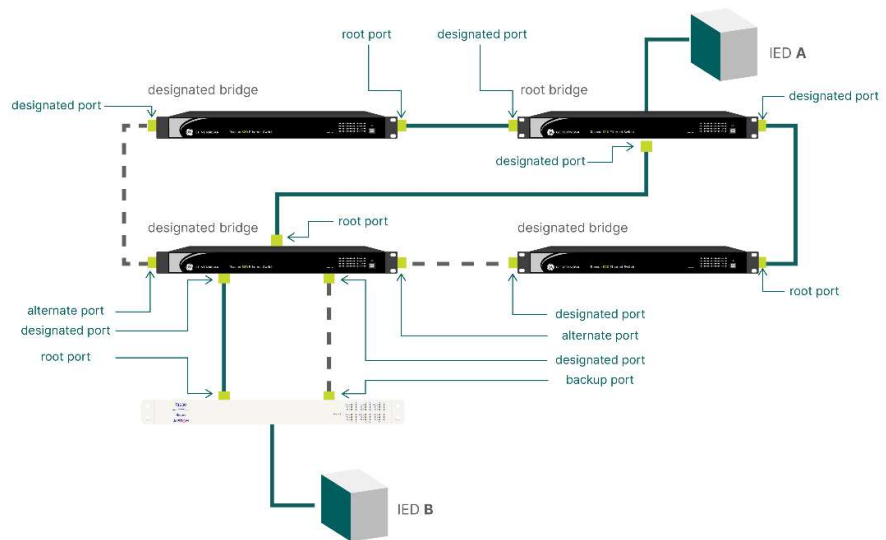


Figure 33: RSTP port status in a loop topology

Besides the difference in port states and definition, there are also two port definitions that are not used in the STP protocol and are used in the RSTP, which are called Edge and Link.

Edge ports are connected to end nodes, e.g., LEDs or computers. Care must be taken when using an LED that is RSTP-aware, as it behaves as a bridge, it ports should not be treated as Edge ports.

Trunk ports are ports connected between switches with RSTP. The figure below shows these port types.

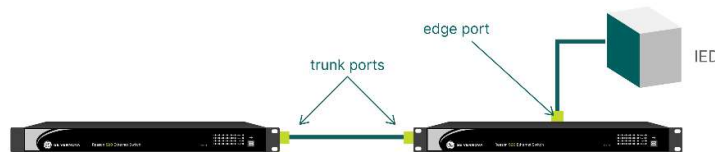


Figure 34: RSTP edge and trunk ports

These definitions are used to increase the RSTP performance, as edge ports do not send or receive BPDU packets, they go from disabled to forwarding state without passing through other states. If an edge port starts receiving BPDU packets, it moves to trunk state and starts being a part of the RSTP protocol.

Each port can also be configured as point-to-point or shared link type. Full duplex ports are considered directly point-to-point links, which makes them change their state to forwarding directly if they are designated port. On the other hand, half-duplex ports are considered shared link ports.

RSTP protocol has changed the way the “flags” field at the BPDU frame is used, when compared to STP protocol. In RSTP the bits are used as follows:

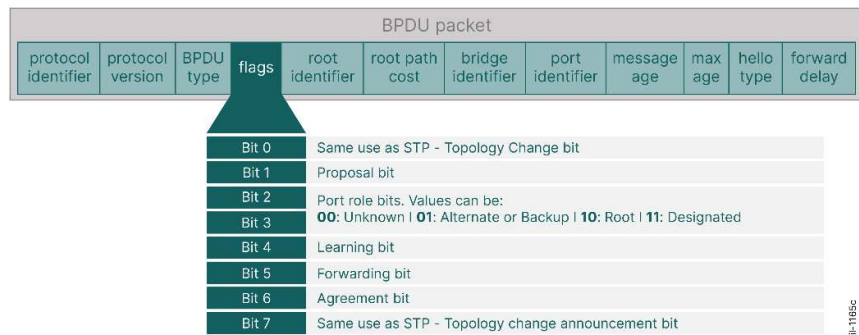


Figure 35: BPDU flag field at RSTP protocol

The change on bits usage was done because the mechanism of transmission of BPDU packets changed. In the RSTP protocol, each bridge in the network can send BPDU packets, and they can also receive BPDU packets from a 'less important' bridge in the topology. Thus, as all of the bridges can send BPDU, it is faster to detect a link failure. In case of receiving a BPDU packet from an inferior bridge, it assumes that the connection to the root has been lost and a reconfiguration of the topology is needed.

Finally, in the RSTP protocol each bridge that is in the topology starts sending BPDU packets based on the 'hello time' of the frame's transmission. RSTP aware bridges can send BPDU without receiving it from a root bridge. If the bridge stops receiving BPDU packets from designated or root bridges three times in a row, it will assume it has lost the connection to the bridge and then a reconfiguration at the ports should be started. By default, Reason S20 sends a 'hello time' message every 2 seconds.

MSTP Protocol

Multiple Spanning Tree protocol (IEEE 802.1s) is an enhancement of the RSTP protocol, developed to be used in environments with VLANs. When using this protocol, all spanning tree information is contained in single BPDU packet, thus reducing traffic and ensuring that the MSTP protocol is compatible with other spanning tree protocols.

The main improvement related to RSTP is the possibility to create regions of spanning tree, mapped to defined VLANs, making spanning tree convergence faster.

Instead of calculating the spanning tree for all VLANs, MSTP allows grouping a set of VLANs in instances, and these instances can run inside a region. Switches that are set to run the protocol need to find their neighbors, which are also running MSTP.

This concept defines three main characteristics that allow bridges to become a member of the same region:

- MSTI configuration name;
- MSTI configuration revision;
- VLANs mapped to the MSTI.

It is defined that bridges are at the same region if they have the same configuration name, revision and the same VLANs mapped.

The figure below shows an example of the MSTP instance regions.

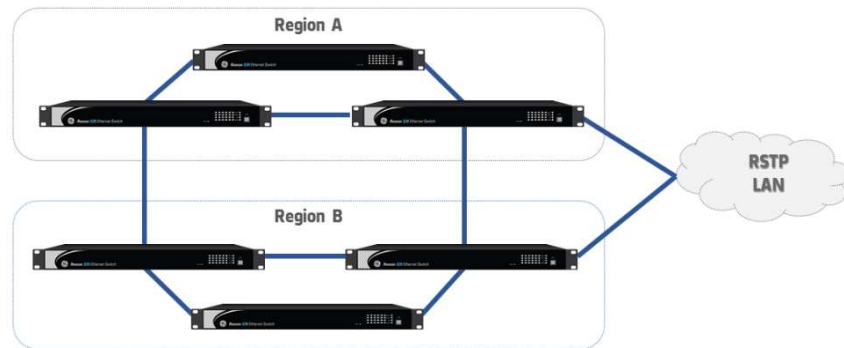


Figure 36: MSTP regions and legacy RSTP LAN connection

Each region will have its own root switch, as it behaves as a separate spanning tree to the others. Also, there will be a switch that will be elected as the regional root, which will allow regions to be connected to each other. The figure below exemplifies these bridges in regions A and B.

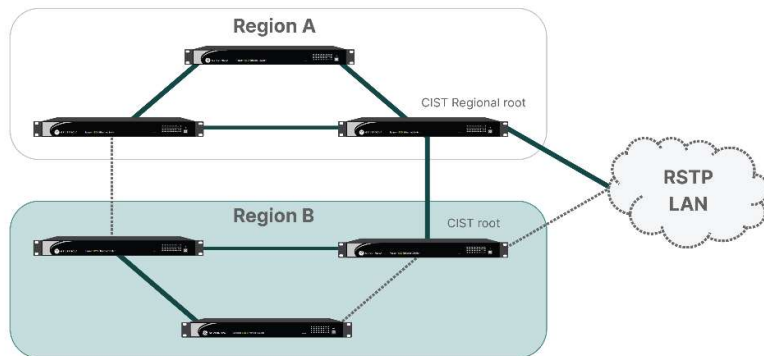


Figure 37: CIST roots an MSTP regions and legacy RSTP LAN

The Common Internal Spanning Tree (CIST) root bridge is the root of the internal spanning tree, which is limited to each region. The regional root is the main root of all regions interconnected.

In a macroscopic view, all regions in the MSTP protocol behave as bridges in a common Spanning Tree LAN. Thus, RSTP convergence will be easier as internal loops created at the regions will be solved independently. Besides, a change in the topology inside a region will not affect all bridges, as it will be limited to its own region. The figure below shows how RSTP and STP bridges will behave when connected to regions created by the MSTP protocol.

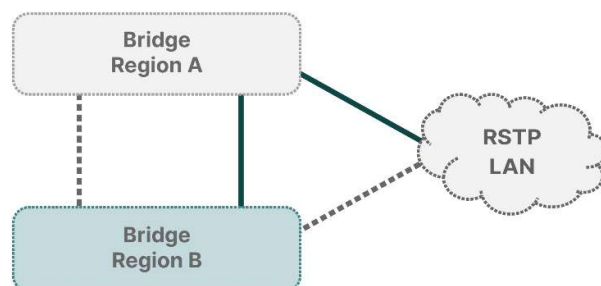


Figure 38: MSTP regions behaviour using RSTP protocol

UltraRSTP

UltraRSTP is a GE approach to improve the standard RSTP fault recovery times performance, by implementing a hardware interruption which notifies the network fault. Please refer to advisory notice GER-4848 if using SFP Transceiver copper RJ45 Part Number GLC-T-BI (order code SFP1GCU01K).

With UltraRSTP, Reason S20 performs fault recovery time around 5 ms per hop, reducing packets loss while maintaining interoperability with others standard RSTP devices. Reason S20 supports UltraRSTP natively and as it is performed by hardware, no extra configuration other than the standard RSTP is needed.

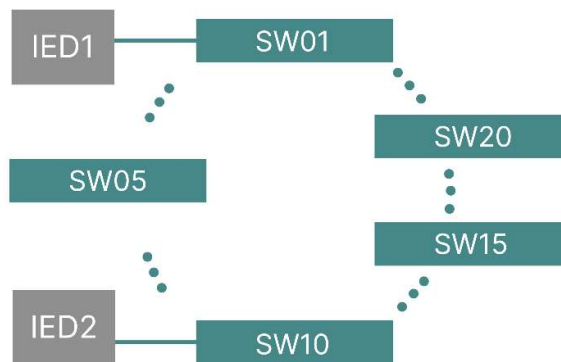


Figure 39: Network fault recovery using GE Reason S20s

8.2 Bridge Settings

The Bridge Settings menu allows configuring basic topics of the STP usage. It is divided in Basic and Advanced Settings tables. Possible configurations are as follows.

Basic Settings

- Protocol Version**: select the Spanning Tree protocol to be used. Possible values are STP, RSTP and MSTP protocols. Protocol set in this field will be the protocol used in this switch to solve loops in a given LAN. If lower protocol is the only available at the network, the switch will use lower protocol instead of the configured in this field. The MSTP protocol is the highest level protocol, RSTP is the intermediate and STP is the lowest level protocol. By default the RSTP protocol is selected;
- Bridge Priority**: indicates bridge priority to be used in the root bridge election. Only one bridge is the root bridge in the spanning tree protocols, and all nodes will be connected to the root bridge. Lower numbers of bridge priority mean higher priority bridge, that is, more reliable bridge to be the root of the spanning tree hierarchy. Lower value available is 0 and maximum value available is 61,440;
- Forward Delay**: indicates the delay that will be used in STP bridges to change its blocking state to forwarding state. This delay is only

used when STP protocol is being used. Allowed values are integer numbers from 6 to 40 seconds, and the Max Age field depends on this value to be defined;

- **Max Age:** indicates the maximum age time of information transmitted by the switch when it is the Root Bridge. This delay is only used when STP protocol is being used. Allowed values are integer numbers from 6 to 40 seconds, and the Max Age field depends on the Forward Delay as follows:

$$\text{Max Age} \leq 2 \times (\text{Forward Delay} - 1)$$

- **Maximum Hop Count:** indicates the initial value of remaining bridges for MSTI instances information generation at the boundary of an MSTI region. Thus, this value defines how many bridges can belong to a given region, as it limits the number of bridges that Root Bridge can distribute BPDU information to. This information is only used when MSTP protocol is being used. Allowed values are integer numbers from 6 to 40 hops (bridges);
- **Transmit Hold Count:** indicates maximum BPDU packets that can be sent per second at the ports allowed to participate in the Spanning Tree protocol network. Allowed values are integer numbers from 1 to 10 BPDU packets per second.

Advanced Settings

- **Edge Port BPDU Filtering :** indicates if Edge ports (explicitly configured as Edge ports in the CIST Ports menu) will transmit and receive BPDU packets. Checkbox selected means that Edge ports will not receive nor transmit BPDU data, and checkbox empty means that Edge Ports could receive and transmit BPDU information;
- **Edge Port BPDU Guard :** indicates if Edge ports (explicitly configured as Edge ports in the CIST Ports menu) will change its state to Trunk port automatically when a BPDU packet is received. Checkbox selected means that Edge ports will change its state automatically to Trunk when a BPDU packet is received at the port, and checkbox empty means that ports will not change its Edge state;
- **Port Error Recovery :** indicates if a port in Error state (which will be disabled by the protocol) will be enabled automatically after a given time. Checkbox selected means that ports in error state will wait until the Port Error Recovery Timeout expires to be enabled, and checkbox empty means that port will not be activated automatically after it becomes in Error state;
- **Port Error Recovery Timeout :** indicates timeout to be applied in the Port Error Recovery function. Allowed values are integer numbers from 30 to 86,400 seconds.

8.3 MSTI Mapping Configuration

MSTI Mapping Settings menu allows configuring regions to be used by MSTP protocol. It is divided in Configuration Identification and MSTI Mapping tables. Possible configurations are as follows.

To create a Region in MSTP protocol, all bridges at a given Region must have the same Configuration Name, Configuration Revision and MSTI-to-VLAN mapping. This last field means that VLANs in all switches in a given region must be at the same MSTI identifier number region

Configuration Identification

- **Configuration Name** : indicates the name that identifies the MSTI region. All Bridges at the same region should have the same Configuration Name. By default, configuration name at a given switch is the MAC address of the switch. Maximum configuration name is 32 characters;
- **Configuration Revision** : indicates the revision of the Configuration Name that identifies the MSTI region. All Bridges at the same region should have the same Configuration Revision. By default, configuration revision at a given switch is 0. Allowed values are integer numbers from 0 to 65,535.

MSTI Mapping

- **MSTI**: shows MSTI instance identifier given row of the table. An MSTI instance, when used, will be understood as the region in the MSTP protocol. Up to 7 instances are supported by Reason S20;
- **VLANs Mapped** : indicates the VLAN identifiers that are mapped to a given MSTI instance. By default, all instances are empty, meaning no use of MSTI. Allowed values are the VLAN range values (from 1 to 4,095). It is possible to insert specific VLAN identifiers separated by comma (for instance, 1,2,10,40), a range of VLAN identifiers using the “-” character (for instance, 10-40), and a meshed specific and range VLAN identifiers (for instance, 1,2,10-40).

8.4 MSTI Priorities Configuration

MSTI Priorities Settings menu allows configuring bridge priority to be used by MSTP protocol. It is allowed to configure in this field the CIST priority and MSTI priority.

CIST priority field is the default instance, which matches with the instance used by STP and RSTP protocols. Thus, this is the value of priority used in these protocols. CIST priority field is interlocked with the Protocol Version configured in the Bridge Settings menu, that is, configuring it at the Bridge Settings menu will change its value in the MSTI Priorities menu, and the same if it is changed at the MSTI Priorities menu.

MSTI priority field is the value used by the bridges that supports MSTP protocol to elect the root bridge in a given region.

If one configuration is desired to be applied at all instances, then the row “*” should be used, that is, configuration done in the “*” row will be replied to all instances. Possible configurations are as follows.

- **MSTI:** shows MSTI instance identifier given row of the table. The first row displays the CIST instance, which is the default instance used by STP and RSTP protocols. An MSTI instance will be understood as the region in the MSTP protocol. Up to 7 instances are supported by Reason S20;
- **Priority:** indicates bridge priority to be used by MSTP protocol. To define the root of the instance (the region root switch), this priority is used as one of the parameters. Priority number plus MSTI instance number and switch's MAC address will be used as the Bridge Identifier parameter in the MSTP network. Lower priority numbers mean higher priority, Values allowed are from 0 to 61,440.

8.5 CIST Ports Configuration

CIST Ports Settings menu allows configuring ports parameters to be used in the Spanning Tree function. This menu is divided in two tables, one for CIST Aggregated Port Configuration and another for CIST Normal Port Configuration. If aggregation function is being performed by the switch, the first table will be used to configure specific parameters for aggregated ports.

If one configuration is desired to be applied at all instances, then the row “*” should be used, that is, configuration done in the “*” row will be replied to all instances. Possible configurations are as follows.

CIST Aggregated Port Configuration

- **Port:** shows the aggregated ports to be configured at this row;
- **STP Enabled:** enable STP function at the port. Checkbox selected means STP enabled, and checkbox empty means disabled;
- **Path Cost:** indicates the path cost value that will be announced by the port to other bridges. Lower path costs mean higher port speed, and they are chosen to forward traffic at the expenses of higher path costs. Allowed values are Auto and Specific. If Auto is selected, path costs will be calculated based on port speed capabilities as recommended at the 802.1D standard. If Specific is selected, path cost used will be the path cost defined by user at the field allowed in the Path Cost column. Allowed path costs values are integer values from 1 to 200000000;
- **Priority:** indicates the priority of the port. If there are two paths between Bridges with the same path cost, the priority field will be used to choose which port should forward traffic. Lower values mean higher priority for the port. Allowed values are integer numbers from 0 to 240;
- **Admin Edge:** indicates status flag of the Edge operation when port is initialized. Allowed values are Non-Edge and Edge. Non-Edge means that Edge operation flag will be initialized with value equal 0,

and Edge means that Edge operation flag will be initialized with value equal 1;

- **Auto Edge:** enable Auto-Edge port detection at the port. This checkbox allows the switch to detect if a port is an Edge or Trunk spanning tree port automatically. Checkbox selected means Auto-edge detection enabled, and checkbox empty means disabled;
- **Restricted:** enables Root guard functions. If it is desired to control ports to not propagate topology changes or not to be root ports, to guarantee that that ports are not in the main catenet of the logical topology, Root guard functions should be enabled. Possible values are as follows:
 - **Restricted Role:** enable Root guard function. This checkbox allows the port to guarantee that the port will not be a Root port, even if it is the best path to the root. Checkbox selected means that the port will not operate root port, and checkbox empty means port could be selected as root port;
 - **Restricted TCN:** enable the port to not propagate notifications and topology changes received in that port to other ports. This can be used to ports connected to networks that change frequently. Checkbox selected means that the port will not propagate topology change and notification messages, and checkbox empty means port will propagate these messages;
- **BPDU Guard:** enable the port to operate in BPDU Guard mode. This function causes the port to disable itself if a BPDU message is received in that port, as could happen if a non-STP bridge is looped in the Spanning Tree network. Ports operating as Edge ports are not affected by this setting. Checkbox selected means that the port will disable itself if a BPDU packet is received, and checkbox empty means port will not disable itself in that case;
- **Point-to-point:** indicates if port is connected to a switched full-duplex LAN (point-to-point LAN) or a shared medium LAN. Allowed values are Auto, Forced True and Forced False. Auto selection means that switch will detect automatically if full-duplex operation is allowed or not, forced true means port will always operate as Point-to-point connection and forced false means port will always be considered as a shared medium. Point-to-point connections have a transition to forward state faster than shared medium LAN connection.

CIST Normal Port Configuration

- **Port:** shows the aggregated ports to be configured at this row;
- **STP Enabled:** enable STP function at the port. Checkbox selected means STP enabled, and checkbox empty means disabled;
- **Path Cost:** indicates the path cost value that will be announced by the port to other bridges. Lower path costs mean higher port speed, and they are chosen to forward traffic at the expenses of higher path costs. Allowed values are Auto and Specific. If Auto is selected, path costs will be calculated based on port speed

capabilities as recommended at the 802.1D standard. If Specific is selected, path cost used will be the path cost defined by user at the field allowed in the Path Cost column. Allowed path costs values are integer values from 1 to 200000000;

- **Priority:** indicates the priority of the port. If there are two paths between Bridges with the same path cost, the priority field will be used to choose which port should forward traffic. Lower values mean higher priority for the port. Allowed values are integer numbers from 0 to 240;
- **Admin Edge:** indicates status flag of the Edge operation when port is initialized. Allowed values are Non-Edge and Edge. Non-Edge means that Edge operation flag will be initialized with value equal 0, and Edge means that Edge operation flag will be initialized with value equal 1;
- **Auto Edge:** enable Auto-Edge port detection at the port. This checkbox allow the switch to detect if a port is an Edge or Trunk spanning tree port automatically. Checkbox selected means Auto-edge detection enabled, and checkbox empty means disabled;
- **Restricted:** enables Root guard functions. If it is desired to control ports to not propagate topology changes or not to be root ports, to guarantee that that ports are not in the main catenet of the logical topology, Root guard functions should be enabled. Possible values are as follows:
 - **Restricted Role:** enable Root guard function. This checkbox allow the port to guarantee that the port will not be a Root port, even if it is the best path to the root. Checkbox selected means that the port will not operate root port, and checkbox empty means port could be selected as root port;
 - **Restricted TCN:** enable the port to not propagate notifications and topology changes received in that port to other ports. This can be used to ports connected to networks that changes frequently. Checkbox selected means that the port will not propagate topology change and notification messages, and checkbox empty means port will propagate these messages;
- **BPDU Guard:** enable the port to operate in BPDU Guard mode. This function causes the port to disable itself if a BPDU message is received in that port, as could happens if a non-STP bridge is looped in the Spanning Tree network. Ports operating as Edge ports are not affected by this setting. Checkbox selected means that the port will disable itself if a BPDU packet is received, and checkbox empty means port will not disable itself in that case;
- **Point-to-point:** indicates if port is connected to a switched full-duplex LAN (point-to-point LAN) or a shared medium LAN. Allowed values are Auto, Forced True and Forced False. Auto selection means that switch will detect automatically if full-duplex operation is allowed or not, forced true means port will always operate as Point-to-point connection and forced false means port will always be considered as a shared medium. Point-to-point connections

have a transition to forward state faster than shared medium LAN connection.

8.6 MSTI Ports Configuration

MSTI Ports Settings menu allows configuring CIST parameters to each MSTI instance. A given port can operate as a CIST port for many MSTI instances, if this port belongs to more than one region. Thus, it can operate in forwarding state in a given MSTI instance and in blocking state for another MSTI. MSTI menu allows the user to configure each MSTI instance of the switch.

By default it will appear the Select MSTI field at this menu. MSTI field has a list of all MSTI regions allowed to be created in Reason S20. Select the desired MSTI instance and then press Get button. When Get button is pressed, it will appear the MSTI Aggregated Ports Configuration and the MSTI Normal Ports Configuration tables.

If one configuration is desired to be applied at all instances, then the row “*” should be used, that is, configuration done in the “*” row will be replied to all instances. Possible configurations are as follows.

MSTI Aggregated Ports Configuration

- **Port:** shows the aggregated ports to be configured at this row;
- **Path Cost:** indicates the path cost value that will be announced by the port to other bridges in the same MSTI instance. Lower path costs mean higher port speed, and they are chosen to forward traffic at the expenses of higher path costs. Allowed values are Auto and Specific. If Auto is selected, path costs will be calculated based on port speed capabilities as recommended at the 802.1D standard. If Specific is selected, path cost used will be the path cost defined by user at the field allowed in the Path Cost column. Allowed path costs values are integer values from 1 to 200000000;
- **Priority:** indicates the priority of the port. If there are two paths between Bridges with the same path cost, the priority field will be used to choose which port should forward traffic. Lower values mean higher priority for the port. Allowed values are integer numbers from 0 to 240.

MSTI Normal Ports Configuration

The configuration options for normal ports are the same as for aggregated ports.

9 IP Multicast (IPMC)

IP communication, just as Ethernet communication, allows the devices in a network to send packets to a single host or to all hosts, in unicast or broadcast transmission, respectively. There are several applications that have a logical architecture of one sender to a set of receivers, such as PMU

applications. To fill that kind of applications, the IP Multicast (IPMC) transmission is used

Be aware when using distinct layer protocols with the Multicast transmission mechanism. There are layer 2 and layer 3 multicast possibilities when it comes to power system basic communication.

Phasor Measurement Units use UDP protocol to send data throughout the network. Thus, in this context, multicast messages are messages sent to an IP address inside a range of IP addresses defined as multicast addresses.

GOOSE, Sampled Values and PTP messages are mapped directly at the Ethernet frame, and the Multicast mechanism is assured by its MAC address destination. This means these messages cannot be directly routed (e. g., they cannot be transmitted in their original form over WANs), and they are sent to a MAC address, which is not the end node MAC address, but the multicast MAC address.

As may be expected, unicast transmission is from one sender to a specific receiver. In broadcast, the message is sent to all receivers in the subnet. Using multicast filters, the equipment that is not expecting these messages will not receive it, different from the broadcast transmission where broadcast messages are forwarded to all nodes in each LAN. Without multicast filtering, multicast messages are sent just as broadcast messages.

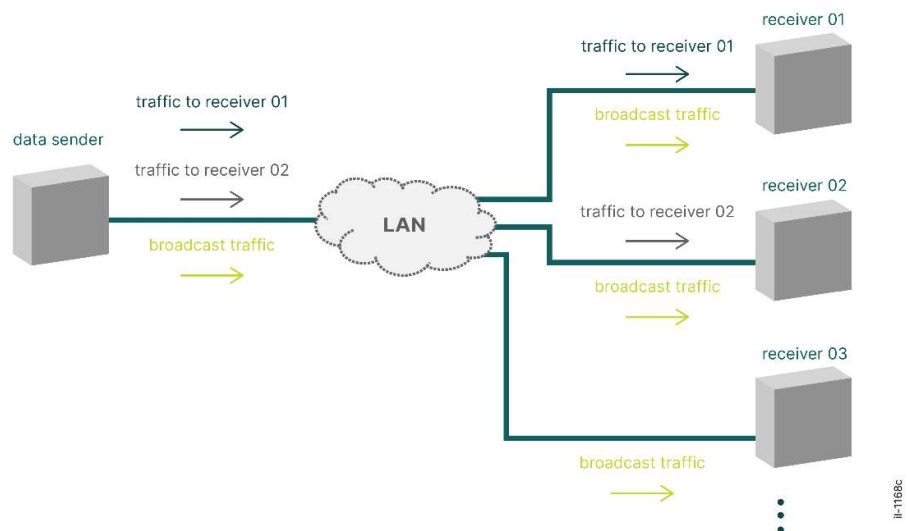


Figure 40: Unicast and Broadcast communication

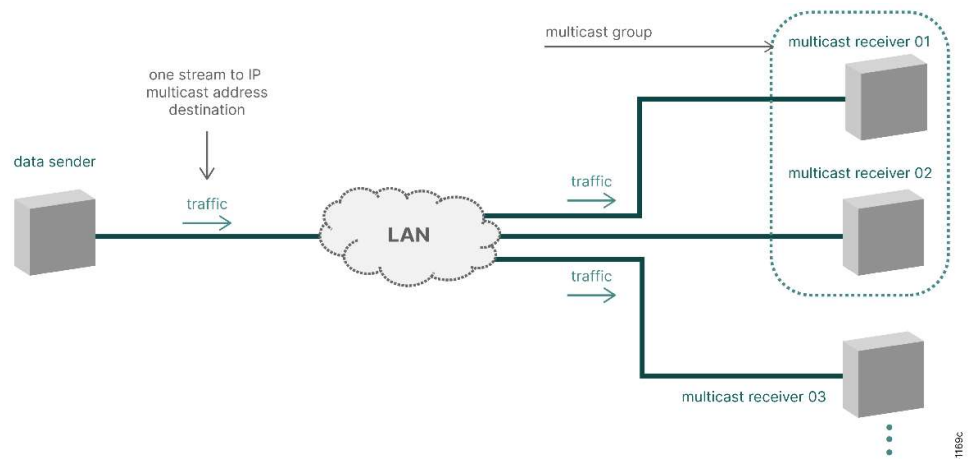


Figure 41: Multicast communication

The IPMC profile menu allows configuring the profile to be used in IP multicast streams, which will be used by IGMP or MLD snooping as the filter rules to be applied at the multicast IP traffic receiving. IPMC Profile menu are located at Settings > IPMC Profile.

The IPMC menu allows configuring basic setting to do IP multicast functionality. IGMP Snooping is related to IPv4 environments and MLD Snooping is related to IPv6. IPMC menu are located at Settings > IPMC.

9.1 IPMC Profile

IPMC Profile Table


Profile Table menu allows the user to perform basic configuration at IPMC profile definition. These profiles will be used at IGMP and MLD protocols to define which group to enjoy at the multicast group. Allowed configurations are as follows.

- **Global Profile Mode**: indicates if profiles at the table should be enabled or not. Filtering functions will only be performed if profiles are enabled. Reason S20 allows up to 64 profiles to be created. Possible values of this field are Enabled or Disabled. Enabled means filtering profile allowed to be executed, and disabled means no filtering profile will be done.

IPMC Profile Table Setting





Indicates which profiles are created. By default, no profile is configured at the switch. If a new profile is required, click at the Add New IPMC Profile button. When clicked, it will appear the following fields to be configured:

- **Delete**: click at the button to delete the profile at the row;

- **Profile Name**: indicates the name to be used by the profile, which must be unique at the network. Allowed values are alphanumeric characters, and maximum name length is 16 characters;
- **Profile Description**: indicates additional description of the configured profile. Allowed values are alphanumeric characters, and maximum name length is 64 characters;
- **Rule**: allows entering in the IPMC Profile Rule Settings, by clicking at the  button. When clicked, it will appear the following fields to be configured:
 - **IPMC Profile Rule Settings**: Indicates which rules are created at the profile. By default, no rule is configured at the profiles created. If a new rule is required, click at the Add Last Rule button. When clicked, it will appear the following fields to be configured:
 - **Profile Name & Index**: shows the name of the profile configured at the Profile Name field at IPMC Profile Table Setting menu and an index number identifying each rule. Each added rule has an incremental decrease index, starting at index 1 and ending in index 64. Higher index numbers (that is, first created rules) have higher priority on lookup, and the highest priority is performed to the first rule created, which has index number 1;
 - **Entry Name**: indicates which entry would be used at this profile rule. Entries are created at the Address Entry menu and allow creating names and IP Multicast address ranges to be used at profile rules. Allowed values are the entries created. If no entry is required, the "-" character means no entry used by this rule;
 - **Address Range**: indicates the IP multicast address range allowed to be used by the selected entry. Entries are created at the Address Entry menu and allow creating names and IP Multicast address ranges to be used at profile rules. If no entry is selected, the "~" character means no entry selected;
 - **Action**: indicates group learning action allowed to be executed by this rule. After receiving join or report messages from a given group, switch will compare if IP address range is compatible with the allowed range of this rule. If IP multicast address message received match with allowed IP multicast address range, this field will specify which action would be performed. Possible values are Deny and Permit. By default, the Deny option is selected. Deny action means messages from a group at the allowed address range should be dropped, and Permit action means that messages from a group at the allowed address range should be learned;
 - **Log**: indicates logging preference after receiving join or report messages from a given group with the allowed IP address range of this rule. Possible values are Disable and

Enable. By default, the Disable option is selected. Disable logging means information from a group at the allowed address range will not be logged, and Enable logging means information from a group at the allowed address range will be logged.

After a rule is created, it will be displayed four icons at the last column of the IPMC Profile Rule Settings table. Their usage is as follows:

-  - Insert New Rule Button: allows adding a new rule in higher level index, click at this button. Created rule will be inserted at the index number of the row where the button was clicked. It can be used to add higher priorities rules after creating other ones;
-  - Delete Rule Button: allows deleting the rule at the row;
-  - Move Rule to higher levels: allows managing rules created by moving a given index rule to higher index rule levels;
-  - Move Rule to lower levels: allows managing rules created by moving a given index rule to lower index rule levels.

Address Entry

Profile Table menu allows the user to create entries to be used at the profiles created in the Profile Table menu. These entries are used in the profiles used at IGMP and MLD protocols to define which group to enjoy at the multicast group. By default, no entry is configured at the switch. If a new entry is required, click at the Add New Address (Range) Entry button. When clicked, it will appear the following fields to be configured:

- **Delete:** click at the button to delete the entry at the row;
- **Entry Name:** indicates the name to be used by the entry, which must be unique at the network. Allowed values are alphanumeric characters, and maximum name length is 16 characters;
- **Start Address:** indicates the first address of the addresses range allowed in this entry. Allowed values are IPv4 or IPv6 multicast group addresses. IPv4 addresses must be entered in dotted decimal format, and IPv6 addresses must be entered in hexadecimal format with a colon (":") separating each field;
- **End Address:** indicates the last address of the addresses range allowed in this entry. Allowed values are IPv4 or IPv6 multicast group addresses. IPv4 addresses must be entered in dotted decimal format, and IPv6 addresses must be entered in hexadecimal format with a colon (":") separating each field.

9.2 IGMP Snooping

Internet Group Management Protocol (IGMP) was designed in the end of 1980's (first version by RFC 1112) to fulfill the requirement of using multicast transmission over IP networks (more specifically, IPv4 networks). The

second version of the protocol was defined at RFC 2236 and its last version is the IGMPv3, defined at RFC 3376.

In internet context, common applications that require multicast transmission are video and audio streaming. When it comes to power systems communication, IGMP protocol can be used when there is multicast communication between Phasor Measurement Unit (PMU) and the Phasor Data Concentrator (PDC).

The IGMP snooping mechanism is shown in the figure below.

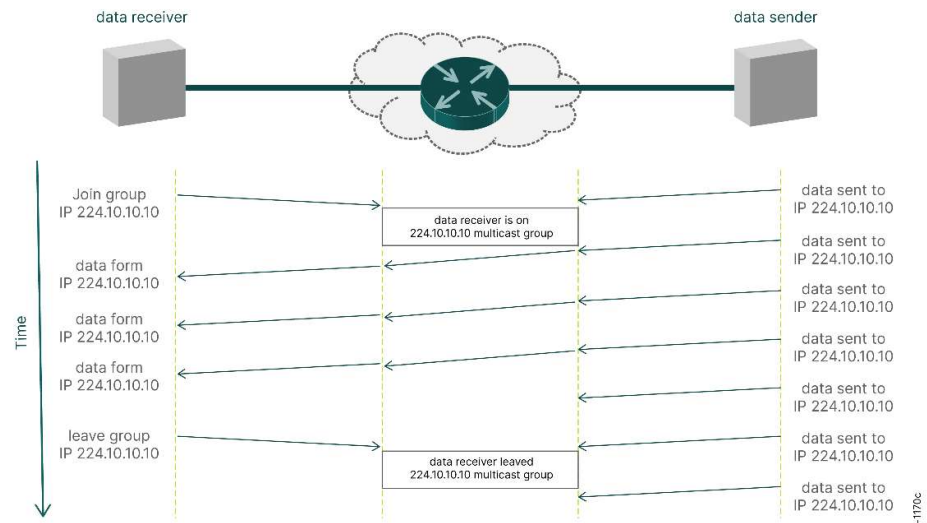


Figure 42: IGMP protocol mechanism

When a receiver wants to join an IP multicast group, it sends a “join group” message to the network, where the routers will mark the incoming IP address and interface to the group. After the receiver becomes a member of the desired multicast group, it starts receiving data. It can be observed the sender will send data to a determined IP address which will not be the address of the receivers, but a “virtual IP address” that matches to the multicast IP address. To stop receiving data, the receiver sends a “leave group” message to the routers at the network.

A range of the IP addresses which is used only for multicast is defined. When the routers in the network receive a frame addressed to these IP addresses, they route the frames based on multicast groups. Multicast IP addresses can be:

- 224.0.0.1 – “All host” address;
- 224.0.0.2 – “All multicast routers” address

At the IGMP protocol, there are two addresses which are used by the protocol and cannot be used as a multicast address:

- From 224.0.0.0 to 239.255.255.255 (Class D address);
- 224.0.0.0 and 224.0.0.255 addresses are reserved for network protocols;
- 224.0.0.0 and 238.255.255.255 addresses are private addresses and cannot be routed;

Reserved addresses cannot be used as IP multicast addresses. In addition to the addresses shown above, there are common services, such as PTP multicasting and NTP multicasting, that have specific addresses. Be sure that they're not used when configuring an IP Multicast group at the network.

IGMP snooping function is performed by the switches by reading the IP header field of the incoming packets. If the switch cannot handle IGMP snooping, multicast IP communication is forwarded as broadcast transmission. Inspecting the IP header data at the port that is connected to IGMP server, the switch can check if the packets are from IP multicast groups. If so, the switch can do a smart forwarding decision, delivering the data only to the interfaces connected to the multicast group, and save bandwidth in other Ethernet interfaces.

When there are many switches, such as LAN, the IGMP snooping will effectively save bandwidth, as only the paths related to the multicast group will forward the data. Paths between switches that are not member of the multicast group will not receive its packets.

The figure below shows how IP multicast transmission happens through IGMP snooping capable switches, routers and common switches. Orange lines mean traffic through the path, and blue lines mean that there is no traffic at the path. It has been considered all equipment is member of the same VLAN.

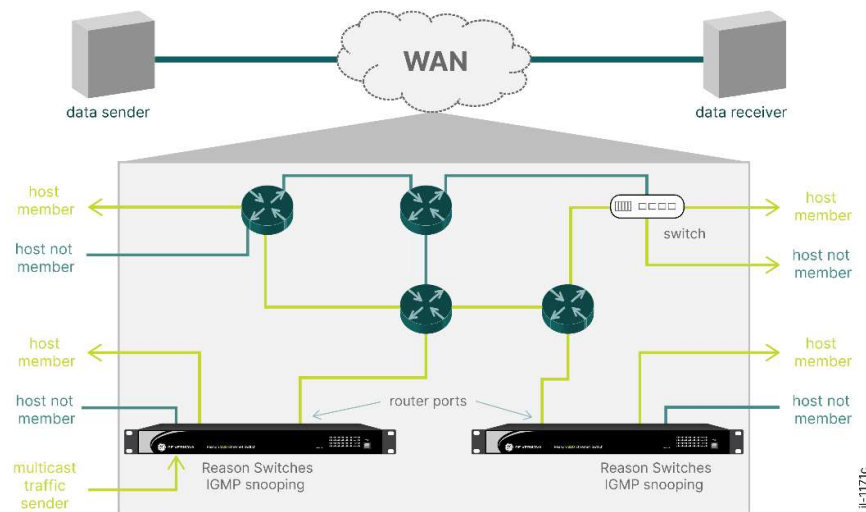


Figure 43: IGMP Snooping at a given LAN

IGMP snooping function is associated to the VLAN at Reason S20. If there is no VLAN usage at the network, the IGMP Snooping VLAN must be configured to operate at VLAN ID (VID) "1".

If IGMP multicast protocol is used, be sure that all equipment at the Local or Wide Area Network have support to IGMP protocol, and be sure that they have support to the same version of IGMP. Reason S20 has support to IGMPv1, IGMPv2 and IGMPv3 protocols.

Basic Configuration

IGMP Snooping Configuration

- **Snooping Enabled** : enable IPMC Snooping function at the switch. Checkbox selected means function enabled, and checkbox empty means disabled;
- **Unregistered IPMCv4 Flooding Enabled** : enable unregistered IPMCv4 traffic flooding at the switch. This function only takes effect if IGMP Snooping is enabled. Unregistered traffic flooding is the unknown multicast traffic, and if enabled, this function will forward these packets as general purpose packets. Checkbox selected means function enabled, and checkbox empty means disabled;
- **IGMP SSM Range** : indicates Source-Specific Multicast (SSM) range. SSM function is used when multicast listener should receive packets from a given source only, and not all multicast sources at a given LAN, improving security and reducing network demands. SSM address will allow SSM-aware hosts and routers to run SSM services. Address must be entered in a dotted decimal format, and mask length is represented as mask length bits;
- **Leave Proxy Enabled** : enable IGMP leave proxy, to avoid forwarding unnecessary leave messages to the router side port. Checkbox selected means function enabled, and checkbox empty means disabled;
- **Proxy Enabled** : enable IGMP proxy, to avoid forwarding unnecessary join and leave messages to the router side port. In this mode switch will operate to the router side as a host, exchanging host leave and join messages. Checkbox selected means function enabled, and checkbox empty means disabled.

Port Related Configuration

- **Port** : shows the ports to be configured at this row;
- **Router Port** : enable IGMP Snooping router port. Router port is the port at the switch that is connected to multicast messages source (the layer 3 multicast devices or IGMP querier), that is, the source side LAN port. Checkbox selected means port selected is the router port;
- **Fast Leave** : enable port's multicast snooping fast leave process. If enabled, switch will stop sending multicast data to a given client as soon as the Leave message is received from client. Otherwise, switch would wait the Multicast source Membership Query message to be answered by the client. Checkbox selected means function enabled, and checkbox empty means disabled;
- **Throttling** : indicates the maximum multicast number groups allowed in the port. Possible values are Unlimited and a range from 0 to 10. Unlimited means that there is no limit for group belonging in that port, and numbers shows maximum multicast group numbers allowed.

If one configuration is desired to be applied at all ports, then the row “*” should be used, that is, configuration done in the “*” row will be replied to all ports.

After one of the configurations described before is changed, there are buttons that allow the user to save or discard the configurations.

- **Save:** save configuration at the Running Config;
- **Reset:** undo changes made locally at the Running Config.

VLAN Configuration

This menu allows configuring VLAN based IGMP Snooping. By default, no VLAN is configured at the switch. If a new VLAN specific IGMP entry is required, click at the Add New IGMP VLAN button. When clicked, it will appear the following fields to be configured:

- **Delete:** click at the button to delete the VLAN entry at the row;
- **VLAN ID:** specify the VLAN that is expected for receiving in multicast frames from the address at this entry. Allowed values are the VLAN allowed values (from 1 to 4,095);
- **Snooping Enabled:** enable IPMC Snooping function for this entry. Checkbox selected means function enabled, and checkbox empty means disabled;
- **Querier Election:** enable VLAN at this entry to participate of the querier election. If enabled, this VLAN entry can win querier election and be selected as a path to the multicast source to be used by multicast clients. Checkbox selected means function enabled, and checkbox empty means disabled;
- **Querier Address:** indicates IPv4 address as source address used in querier election. Querier election will define which router or IGMP Snooping switch will forward traffic if they share the same segment based on its IP address: the lowest IP address device will win querier election and then will forward traffic. If not set, IPv4 address used will be the IP address of the management interface of the switch. Allowed values are in the IP version 4 (IPv4) address range, and values must be configured in dotted decimal format;
- **Compatibility:** indicates which IGMP version this entry should be compatible to. Allowed values are IGMP-auto, Forced IGMPv1, Forced IGMPv2 and Forced IGMPv3. By default, IGMP-auto is selected, which means switch will define itself protocol running at the VLAN. Forced IGMP values allow user to configure explicitly which version entry should use;
- **PRI:** indicates priority (PCP bits at the Ethernet frame) of the IGMP control frames at the network, to prioritize or not these messages at the switch, redirecting it to a given queue. At the network, switch will send PCP value to other devices embedded at the frame. Allowed values are the PCP range values, from 0 to 7;
- **RV:** indicates the robustness variable value for use in the network by this entry. This field allows tuning of the expected loss of data on a given network. Networks that lose many packets should have this number increased. RV value must not be equal to 0 or 1. By

default, its value is set to 2. Allowed values are integer numbers from 2 to 255;

- **QI (sec)**: indicates the Query Interval to be used between general queries of this entry. These general queries messages are exchanged between IGMP interfaces to all of them have knowledge about the multicast group. Allowed values are integer numbers from 1 to 31,744 seconds. By default, query interval is set to 125 seconds;
- **QRI (0.1 sec)**: indicates the Query Response Interval, which is the maximum time that clients can take to answer to a general query message. Allowed values are numbers from 1 to 31,744 tenth of seconds. By default, query interval is set to 100 (which means 10 seconds);
- **LLQI (0.1 sec)**: indicates the Last Listener Query Interval of this entry. LLQI timer indicates the maximum time allowable by a client to answer to the querier. When this timer is expired, querier and snoopers at the network will stop sending multicast data to this client. By default, query interval is set to 100 (which means 10 seconds);
- **URI (sec)**: indicates the Unsolicited Report Interval of this entry. This timer indicates the time between repetitions of a host's initial report of a membership in a group. Allowed values are integer numbers from 1 to 31,744 seconds. By default, query interval is set to 1 second.

After one of the configurations described before is changed, there are buttons that allow the user to save or discard the configurations.

- **Save**: save configuration at the Running Config;
- **Reset**: undo changes made locally at the Running Config.

Port Filtering Profile

This menu allows configuring filtering condition to be applied at the ports based on the IPMC profile. IPMC profiles used are the profiles added at the IPMC Profile menu.

- **Port**: shows the ports to be configured at this row;
- **Filtering Profile**: indicates which profile can be selected to be used by this port. Allowed values are the profile names configured at the Profile Table at the IPMC Profile menu. The “-” field means no filtering profile being applied to this port.

9.3 MLD Snooping

Multicast Listener Discovery (MLD) is a part of ICMPv6 protocol. It was defined at the RFC 2710 (version 1) and then upgraded to version 2 through RFC 3810. Its usage is much like IGMP, but instead of multicast transmission over IPv4 networks, MLD works over IPv6 networks. Protocol mechanism is like IGMP. To be part of a group that is receiving a multicast data from a sender, the MLD receiver must send a “join group” message, which must be understood by MLD-aware hosts and routers at

the network. If it wants to stop receiving data, then a “leave group” message must be sent.

MLD snooping can be understood, from an application point of view, as IGMP snooping for IPv6 networks.

When using this feature as multicast transmission function, all equipment at the network (routers, switches) must be capable to read the IP packet headers and inspect its multicast group. In case of layer 2 switches, multicast transmission benefits can only be obtained if the switch can handle MLD snooping function. If not, multicast messages will be treated as broadcast messages. Thus, all members of the LAN (or VLAN) will receive data, instead of only multicast members.

A range at the IP addresses which is used only for multicast is defined. Routers at the network, when receiving a frame addressed to these IP addresses, will route the frames based on multicast groups. Multicast IP addresses can be:

- FF00::/8 address block is reserved for multicast;

Like at the IGMP protocol, there are addresses which are defined and cannot be used as a multicast address:

- FF01::1 – “All nodes in local interface” address, used by hosts;
- FF02::2 – “All in local link” address, used by hosts;
- FF02::5 – “All nodes in local site” address, used by routers.

Reserved addresses cannot be used as IP multicast addresses. In addition to the addresses shown above, there are common services, such as PTP multicasting and NTP multicasting, that have specific addresses. Be sure that they are not used when configuring an IP Multicast group at the network.

Basic Configuration

The IGMP snooping configuration may be used as reference to configure the MLD snooping, but using IPv6 syntaxes.

10 MAC Table

10.1 MAC Table Fundamentals

Ethernet switches operate in a context of transparent bridge packet switching, which is a fundamental concept in Ethernet packet switching. There are some topics, thus, that must be matched by Ethernet switches, which are

- Each station (host) attached to a transparent bridge has a globally unique address (MAC address);
- A bridge has an interface connected to all LANs that the bridge belongs to;

- The bridge has information to reach all stations that it is connected to;
- A bridge operates in promiscuous mode, in which it receives all frames at all interfaces, regardless the destination address;

There are some additional features that a switch must perform, such as:

- Packet filtering;
 - If the source MAC address of a given packet is attached at the interface where it was received, the packet will be discarded by the switch.
- Multicast forwarding
 - A multicast addressed frame must be forwarded to all interfaces except the incoming frame interface

If one of these concepts is violated, the network would not work properly.

Reason S20, by default, are set to operate as a transparent bridge, i.e., as a common switch.

An example of the Ethernet frame is shown in Figure 35 below.



Figure 44: Ethernet frame

As can be seen, the destination and source addresses are attached directly at the Ethernet frame. Thus, a switch must be able at least to handle these fields to perform its main function, being a transparent bridge in a packet-switching network environment.

If a host needs to send data to another host in a switched LAN, it will forward traffic from its own NIC (Network Interface Card) to the interface that it is connected at the switch. Then, the switch will map the incoming MAC address in a table, mapping to an interface. Continuing this process, the switch will map all hosts to reach all stations connected to it. Note that, for this operation, it is assumed that there is no duplication at the hosts addressing, that is, there is different MAC addresses to each host. Figure 36 exemplifies the MAC table at a given LAN.

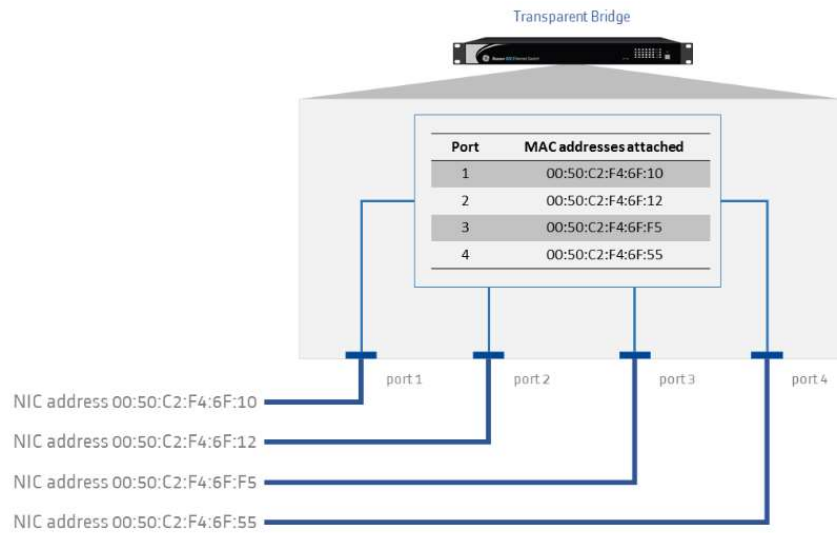


Figure 45: Address a table at a given Switch

As the switch knows where the hosts are, incoming data to a mapped host will be redirected through the interface where the destination is attached, and no data will be sent to other interfaces, as shown below. If there is incoming data to a host not mapped as destination, the switch may flood the ports connected to other switching equipment or drop the packets.

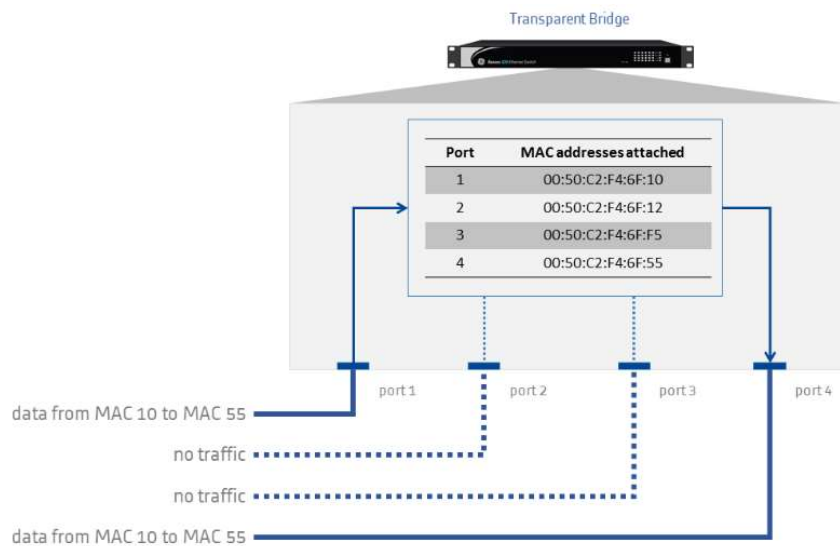


Figure 46: Forwarding traffic in an Ethernet switch

As networks are not static and hosts can be connected and disconnected any time, the switch must inspect its own MAC table to update it. This is called aging of the MAC table and it is performed by the switch verifying MAC addresses at the incoming and outgoing data packets. If a mapped MAC address stops receiving or sending data, the switch will discard its address on the MAC table. Thus, processing time for inspecting the address table is decreased and performance of the switch is increased. It is possible, for security reasons, to restrict the access to a switch's LAN by manually inserting MAC addresses of the allowed hosts at a given

interface. In this case, the port will operate in secure mode, and the equipment will only forward traffic from set MAC addresses and will drop data from MAC addresses which are not set. Thus, it is possible to limit LAN access only by MAC addresses. The following figure shows how MAC access management works in the switch.

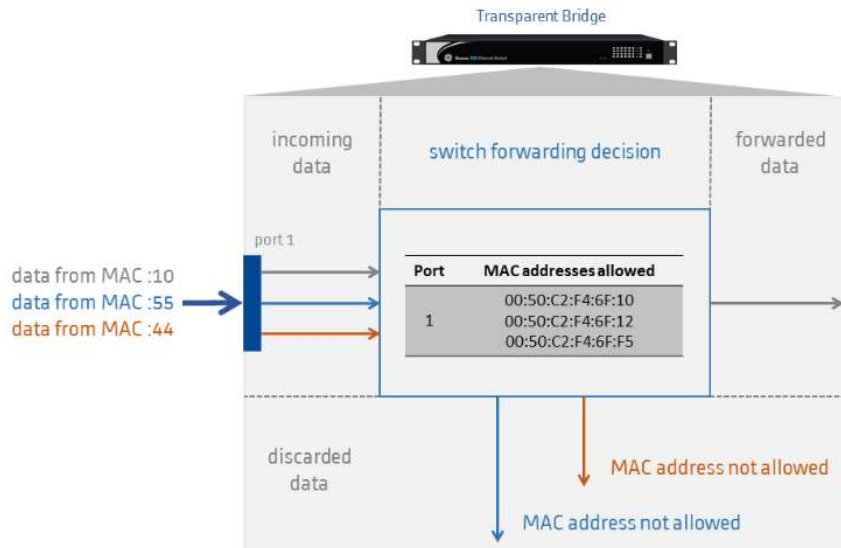


Figure 47: LAN access restriction with MAC address configuration

10.2 MAC Table Configuration

MAC table menu is meant to configure the MAC address entry of Reason S20, which can have up to 8192 entries in total considering the dynamic and static entries. It allows configuring aging time of MAC addresses learned, mode of operation and allowed MAC addresses to ingress at the switch local interface.

MAC Table menu is located at Settings > MAC Table.

Aging Configuration

This function allows the switch to automatically discard a learned MAC after the aging time of this entry expires. Possible configurations are as follows.

- **Disable Automatic Aging** : disable automatic aging function. Checkbox selected means Aging configuration disabled, and checkbox empty means enabled;
- **Aging Time**: indicates the time that entries will expire. Allowed values are integer values from 10 to 1,000,000 seconds;

MAC Table Learning

MAC Table Learning menu allows configuring switch's behavior at the MAC learning process, that is, if switch will use filters configured to limit access to the LAN or not. Each port can have its MAC learning function selected separately. Possible configurations are as follows.

- **Auto**: select to allow the learning process to start as soon as frame is received. If MAC address is not known, port will learn MAC

address source or destination and will insert it at the Address table entry;

- **Disable:** select to disable the learning process. If MAC address is not known, port will not learn MAC address source or destination to insert it at the Address table entry;
- **Secure:** select to allow the learning process to start only if frame received is from a MAC configured at the Static MAC Table Configuration. If MAC address is not configured, port will drop the frame.

If ports are configured as Secure mode, make sure that Management link used to configure and monitor switch is included. If not, switch's configuration will be accessible only by serial interface at USB connection (Local interface).

Static MAC Table Configuration

The static MAC table can contain up to 64 entries. Note if ports are configured as Secure mode, make sure that Management link used to configure and monitor switch is included. If not, switch's configuration will be accessible only by serial interface at USB connection (Local interface).

- **Delete:** click at the button to delete the MAC address at the row;
- **VLAN ID:** specify the VLAN that is expected for receiving in frames from this MAC address. Allowed values are the VLAN allowed values (from 1 to 4,095);
- **MAC Address:** specify the MAC address number of the entry allowed. Values must be inserted in hexadecimal format, and each octet must be separated by the "-" signal;
- **Port Members:** specify which ports allow ingress of frames from this MAC address. Checkbox selected means port allowed to receive frames from this MAC address, and checkbox empty means port not allowed.

11 Virtual LAN (VLAN)

11.1 Legacy LAN Technology

In packet switching networks, a LAN can be understood as the physical connection between hosts (equipment that uses the LAN to communicate to each other) and switching equipment (switches) that will deal with exchanging data from hosts.

If a company with many departments (many types of data traffic) would like to segregate its LAN, for management purposes and to maintain LAN performance, it would use different LAN infrastructure for each department. All traffic between them should be routed. This issue would not be a problem if the hosts were static, which is not a common behavior. There are new people joining the LAN, mobile users, and new changes in organization infrastructure and so on.

As an example, imagine the organization shown in below. Departments A and B are located in different rooms, and each department's LAN is physically separated from each other.

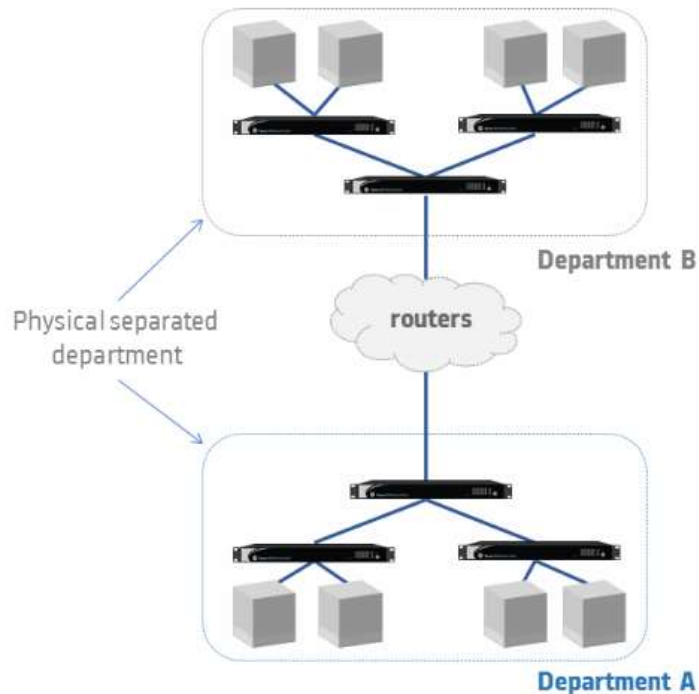


Figure 48: Different LAN from different departments

Now imagine there is a need to increase Department A hosts, but there is no space at the department's room, the new host would stay at Department B's room. With legacy VLAN-unaware equipment, this increase at Department A's LAN size would be done as shown below.

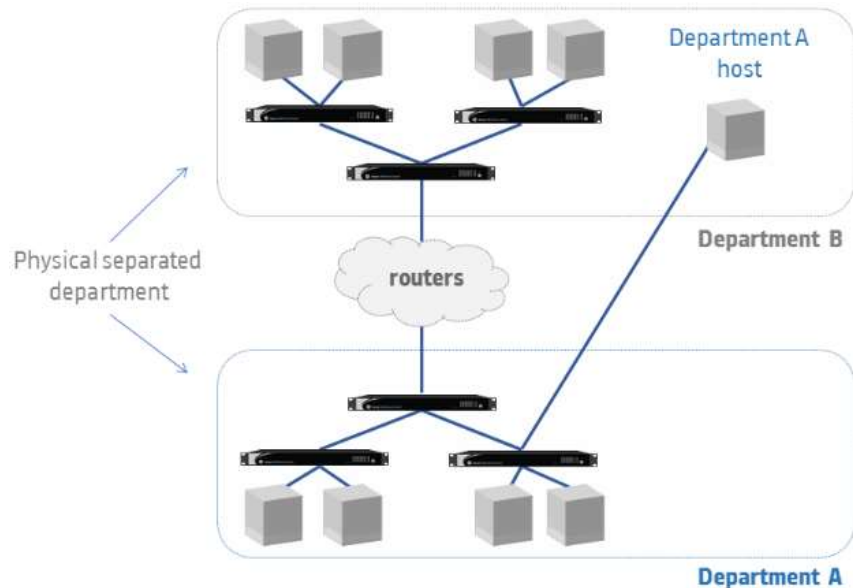


Figure 49: Addition of new hosts to the legacy VALN-unaware equipment

This demonstrates that changes and increases in a VLAN unaware network would create problems, since it would be required to change all physical installations in the network. The VLAN mechanism was created in this context.

In the modern power system communication, using only legacy equipment to transmit IED communication through VLAN unaware equipment could create problems at many points. One of them could be that traffic segregation of GOOSE, Sampled Values and PTP messages would be done through different physical LAN installation. This option would likely be unacceptable due to installation costs and maintenance difficulties.

11.2 Virtual LAN Basics

Virtual LAN technology allows separating the network through logical and physical networks. With VLAN information, it is possible to create logical networks based on its usage instead of its physical installation, thus enabling much more flexibility on it.

In the example given, if VLAN technology is used to segregate traffic from the different departments, the physical topology could be as demonstrated below. The figure shows that installation issues would decrease, as hosts can be attached at any VLAN-aware switch at the LAN.

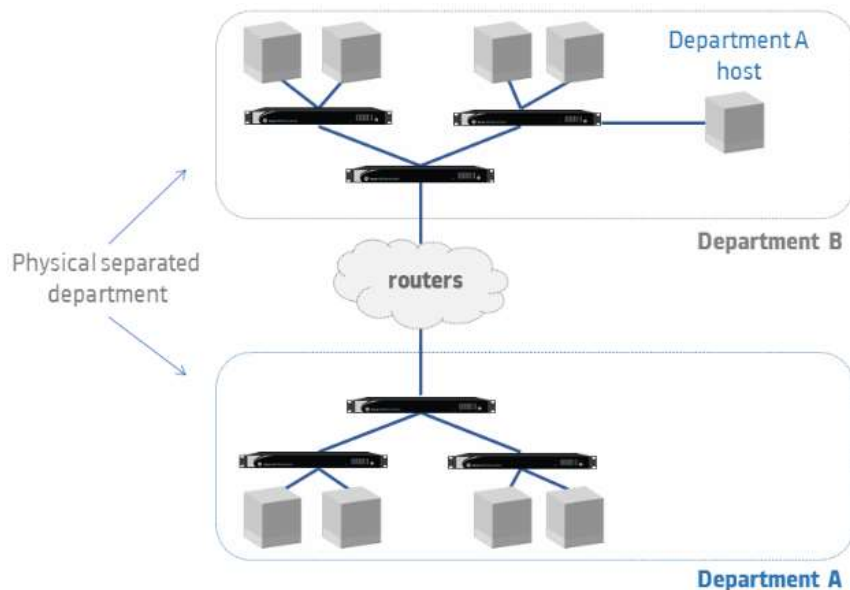


Figure 50: Adding new VLAN-aware hosts

Besides the physical installation, VLAN mechanism will make the hosts see each other as if they were at the same physical LAN, as shown in the next figure. Thus, there is no more dependency on the equipment connections. With VLAN, it is possible to logically group hosts or messages with common interests.

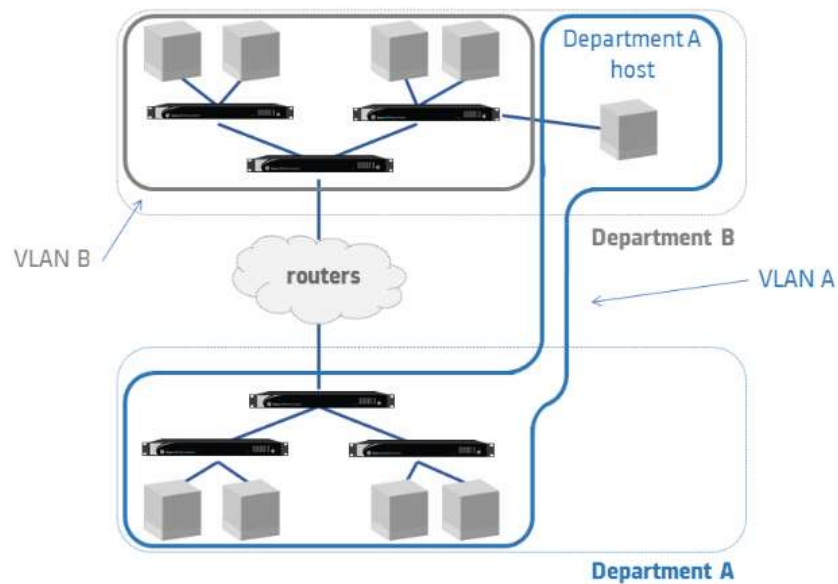
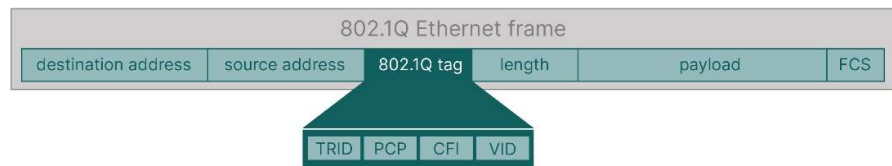


Figure 51: VLAN segregation in different departments

Traffic segregation through Virtual LAN (VLAN) is standardized by IEEE 802.1Q document. The standard added 4-bytes in the Ethernet frame, where information about the logical LAN which the host (or message) belongs to. Figure below shows an Ethernet frame and its 802.1Q tag position



H-1184c

Figure 52: 802.1Q Ethernet frame

The information at 802.1Q tag is divided in 4 fields:

- TPID (Tag Protocol Identifier): 16-bit length, this field presents VLAN protocol and will be equal to 0x8100;
- PCP (Priority Code Point): 3-bit length, this field presents the priority of the packet at the network;
- CFI (Canonical Format Unit): 1-bit length, this field is always set to 0 in Ethernet communication;
- VID (VLAN Identifier): 12-bit length, this field shows explicitly VLAN number identifier which the frame belongs to. It is also called VLAN tag.

VLAN tag usage can have many concepts in its background. Actually, there are many VLAN tag types, used in different environments, and with specific standards related. As example, C-tag, S-tag and I-tag can be cited. Description given in this manual applies to Customer tag (C-tag), the most common VLAN usage in power system communication. As Reason S20 main application is be a path to interconnect IED equipment in power systems communication, information contained in this manual should be enough to use the equipment. If application of switch requires the usage of specific VLAN for trunk links, where S-tag is used, service VLAN tag (S-tag) is also supported by Reason S20.

VID number is the number that explicitly defines which VLAN the incoming packet belongs to. There are, in theory, 2^{12} (4,096) possibilities of numbers, as this is a 12-bit field. Besides, there are two VID numbers that are reserved:

- VID = 0xFFFF is reserved and must not be used;
- VID = 0x000 means Priority-tagged frame. This frame is not associated with any VLAN identification, but explicitly shows the priority of the packet.

When using VLAN mechanism, be aware that there is no 0xFFFF VLAN usage.

By default, Priority-tagged frames (VID = 0x000) will be mapped to native VLAN ID (VID = 0x001) and will have its priority information removed at the outgoing frame.

11.3 LAN in Modern Power System Communication

Virtual LAN technology allows separation of traffic in through logical and physical networks. In power system communication, where is expected IEC-61850 messages with different priority and usage, there will be only one physical path for each IED and the packets must be separated logically. Traffic segregation is particularly important in modern power system communication as it is expected that multicast traffic will flow in the network. GOOSE, Sampled Values and Precision Time Protocol messages are multicast messages, and all of them can be mapped directly at Ethernet frame, in other words, they are layer 2 protocol communication. As these messages traffic mechanism is multicast, by default the switch will flow them throughout its interfaces, except the incoming messages. When using VLAN traffic segregation, multicast messages are forwarded only onto the VLAN that the multicast message belongs to. Thus, GOOSE, Sampled Values and PTP traffic will flow separately from each other. Finally, as the traffic is separated, IED equipment that expects to receive only GOOSE messages will not have its network interface interrupted by Sampled Values data, for example.

An example of expected VLAN traffic segregation is shown below. Note that a ring physical topology is used only for example propose, as it is a common physical network topology in power system communication. Before refer to the figure, there are a few assumptions:

- Merging Unit is the GOOSE and Sampled Values messages supply, and it is a slave clock of PTP synchronization protocol;
- PTP grandmaster clock synchronizes PTP-aware equipment, and do not receive GOOSE or Sampled Values data;
- IEDs do not synchronize themselves through PTP protocol. Both of them expect to receive GOOSE messages from the Merging Unit and only one of them expects to receive Sampled Values;
- There are 3 VLAN configured at the equipment involved: One for PTP traffic, other for Sampled Values traffic and another one for GOOSE messages traffic.

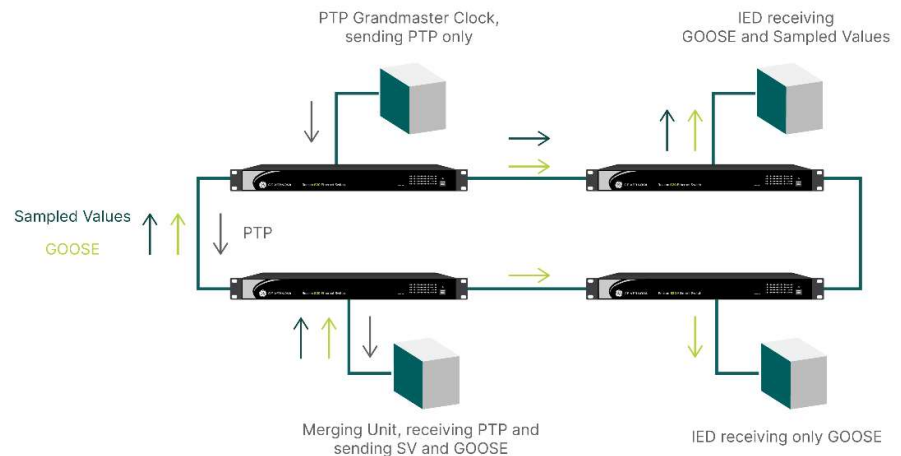


Figure 53: Typical topology in power system communication environment

The logically network the switches do when using VLAN traffic segregation is shown below.

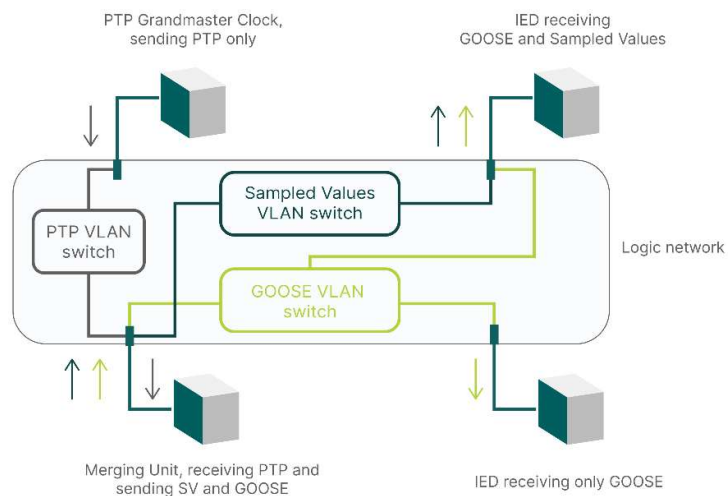


Figure 54: Logical topology of typical power system communication environment

IEC 61850 documents recommend to use different methods of redundancy at Station and Process communication bus. For simplification, these redundancy requirements are not shown nor discussed in this chapter.

11.4 IEEE 802.1Q Switch operation concepts

In previous sections, it could be understood what is VLAN and what is expected using packets with VLAN information. This section will demonstrate the basics of the switch operation when dealing with 802.1Q frames, which applies to Reason S20. Next figure shows data traffic flow inside the switch.

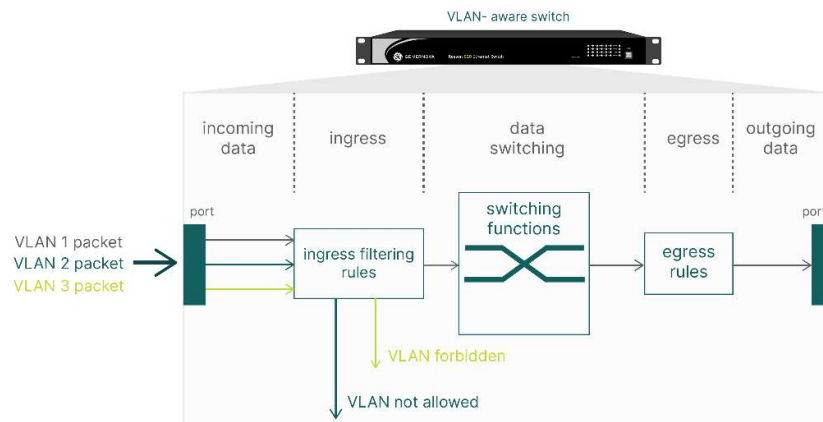


Figure 55: Traffic flow inside an 802.1Q switch

As can be seen, there is no management in the incoming data, switch will receive everything the host is sending. The forwarding decision, then, is based on the ingress filtering rules applied. Ingress rules will define:

- Which VLAN frames are acceptable;
- If VLAN untagged frames are allowed;

If incoming frame is from a not allowed VLAN, it will be discarded. Besides, if the packet is a priority-tagged frame or an untagged frame, ingress filtering rules will map the frame to the VLAN which the port is a member.

802.1Q switches always operate in VLAN mode. When incoming frames have no VLAN information or applications does not require VLAN usage, switch will encapsulate the frame on an 802.1Q frame and egress rules will define if the frame will be sent with or without VLAN information.

When a frame is allowed to be forwarded, switching functions will check which VLAN the frame is member of and it will be forwarded based on the ports that are member of this VLAN. MAC table will, then, forward traffic as the hosts are mapped when unicast communication is used. In broadcast and multicast transmissions, the switch will flood only VLAN ports that are member of the broadcast/multicast incoming frame VLAN.

At the end of the process, egress rules will determine if the switch will maintain or discard VLAN information.

If it is required to maintain 802.1Q, all frames will leave the switch tagged including those which have come without tag information, which will leave the switch with the Port VLAN identifier (PVID) of the incoming port. 802.1Q frames will leave the switch as it comes.

If it is required to discard all 802.1Q information on the frame, then all frames will leave the switch untagged, including those which have come with tag information.

Besides the egress filtering of 802.1Q frames, Reason S20 has a third option on the egress filtering: discard information only from PVID frames. If used, untagged frames that were tagged on PVID will leave the switch untagged, and tagged frames will leave the switch tagged. Thus, tagged and untagged frames can leave the switch as they come.

11.5 Reason S20 Operation

The Reason S20 is a VLAN-aware equipment and its operation allows the use of traffic segregation as transparent bridge, using 802.1Q tagging. When using VLAN function, there are some terms and definitions that must be understood to a correct configuration.

Reason S20 operates only in VLAN-aware mode, which all traffic is treated in a VLAN concept. Tagged VLAN will be redirected to the VLAN it belongs, and untagged traffic will be redirected to the VLAN set in Port VLAN. At the egress, by default, untagged incoming frames will be forwarded without VLAN tag, as it has come to the switch.

Port Operation Mode

Operation mode can be defined as Access, Trunk or Hybrid port.

Access port is used when legacy equipment is connected. Legacy equipment may be VLAN-unaware equipment and customer VLAN tag equipment, such as IEDs equipment. These ports will tag untagged ingress traffic with the VLAN Port number and forward the traffic into this VLAN. When incoming frames have VLAN information, the frame will be directed to the specified VLAN. At the egress, the tag used internally by the switch to direct untagged frames will be removed

Access ports are always defined as C-Ports, permit tagged and untagged incoming frames. All frames are untagged at the egress. Only VLAN port is allowed to traffic. Forbidden VLAN at the ports and egress tagging is user configurable.

Trunk ports accept VLAN tagged frames from many VLAN. These ports permit the ingress of VLAN-tagged frames and will maintain its tag in the egress. Otherwise, the user must configure which VLAN the trunk port will accept or not. These ports can be member of more than one VLAN, limited by maximum number of VLAN permitted (4,095 VLAN). Incoming data from a not allowed VLAN will be discarded at the ingress process in the switch. By default, Trunk ports allow to traffic all VLAN range (1 – 4,095). Trunk ports are generally ports connected to switches or IED that send data to

more than one VLAN, such as merging units (one VLAN for GOOSE data and another one for Sampled Values data).

Trunk ports are always defined as C-Ports and permit tagged and untagged incoming frames. Allowed and Forbidden VLAN at the ports and egress tagging is user configurable. When using equipment that allow much VLAN traffic, such as IED receiving Sampled Values and GOOSE messages at the same network interface, port type of the connection point of the IED to the switch should be considered trunk port.

Hybrid ports allow the user to configure all parameters at a given port, as ingress filtering, port VLAN (in case of untagged frame), allowed and forbidden VLAN. Hybrid ports can permit, if desired, the ingress of packets from a given VLAN that is not a member nor is a forbidden VLAN.

Hybrid ports allow users to configure all possible treatment the switch will perform in the VLAN, such as Port VLAN, Port type, Ingress filtering, Ingress Acceptance, Egress Acceptance and Allowed and Forbidden VLAN configurable.

Port Type Concept

In addition to operation mode, there is the port type concept that must be understood. Port types can be set to be Unaware, C-Port, S-Port and S-Custom-Port types.

Unaware port is used for legacy equipment connection. These ports do not consider incoming frames VLAN information, and all incoming frames are classified at port VLAN number. On frame's egress, port VLAN tag is removed.

Customer tag port (C-Port) is a port that deals with C-tagged frames. These are common tagged frames, such as incoming GOOSE messages. Thus, when using equipment that sends tagged-frames, this is the port type that needs to be used. Incoming frames with VLAN information will be directed to the VLAN, and priority-tagged or untagged frames are directed to Port VLAN.

Service tag port (S-Port) is a port that expects to deal with double-tagged frames. Double-tagged frames are frames that have a C-tagged frame inside other VLAN tag, which is the service VLAN tag. S-tag frames are used by switching equipment at the network to create a VLAN to transport tagged frames. Only switching equipment use this frames. Thus, if S-tag is required, be sure that the S-port is connected to other switching equipment, e. g., another switch.

Custom Service tag port (S-Custom-Port) is used in environments that traditional S-tag does not fulfill the requirements of the network. This port behaviour is much like S-port, except that the expected Ethertype field in the Ethernet frames of custom S-port is defined at the switch, that is, the Ethertype field in the frame should be configured manually at the switch. These ports can be used at applications where non-conventional switching equipment is used, to allow some interoperability to them.

There are some concepts on the treatment of untagged frames, ingress and egress filtering on the switch and the VLAN range that a port can be member as explained below.

Port VLAN parameter is the VLAN that the switch will use if incoming traffic is untagged. All frames “inside” the switch are tagged-frames, and untagged incoming frames will be internally tagged in the VLAN defined at Port VLAN.

Ingress filtering and acceptance can be configured by user, when the port selected permits. If port ingress filtering is used, port can select if it will accept tagged or untagged frames. If not used, the switch will perform its function in promiscuous mode, that is, all incoming data will be received. Egress filtering and acceptance can be configured by user, when the port selected permits. When used, the switch can be configured to untag all egressing frames, tag all egressing frames and untag (cut VLAN information of the frame) PVID frames. If untag all is used, then frames will always egress the switch without VLAN information, including the ones which have come with VLAN information. If tag all is used, then frames will always egress the switch with VLAN information, including these ones which have come without VLAN information. In that case, untagged incoming frames will be encapsulated in an 802.1Q frame with PVID identification. Finally, if untag PVID is used, then only frames with PVID identifier will have their VLAN information discarded, and all of the others VLAN identifiers will be maintained.

Attention is required when using meshed VLAN and VLAN-unaware equipment in the same port. If the application imposes this, use different VLAN identifiers in VLAN-aware equipment from PVID number, which will be used only for VLAN-unaware equipment, and then choose untag PVID at the egress tagging. If the same identifier is used on both VLAN-aware and unaware equipment, all frames with PVID (send to the VLAN-aware and unaware hosts) will have its 802.1Q information discarded.

Allowed and forbidden VLAN are concepts used to define which VLAN (or which VLAN ID range) the port will be a member of. Trunk and Hybrid ports can be members of as many VLAN as it is possible. Thus, such ports can receive data from all of the allowed VLAN configured. Besides, as it is desirable to explicitly define of which VLAN the port must not be a member, there is the forbidden concept. In this concept, the port will allow any VLAN to be a member, except for the forbidden ones. This last concept is particularly useful if there are too many VLAN whose port should be a member and a few that should not be member. Thus, all of the VLAN accepted and a short list of the ones that are not accepted can be configured. In power system applications, for instance, such a concept can be used to guarantee that Sampled Values data do not leave the process bus, thus increasing station bus bandwidth security.

11.6 VLAN Configuration

VLAN menu allows configuring virtual LAN segments to segregate broadcast domains. VLAN information is mapped directly at the Ethernet

frame, and it is standardized by IEEE 802.1Q. VLAN is the main way to segregate traffic from station and process bus at Reason S20. Sampled Values, GOOSE, PTP, MMS and other messages can be segregated from each other using VLAN, increasing performance on its usage in power system applications.

VLANs menu is located at Settings > VLANs.

Global VLAN Configuration

Global VLAN Configuration menu contains basic configurations used by VLAN function. These configurations are the allowed access VLANs and the Ethertype that can be used for S-custom ports.

- **Allowed Access VLANs** : indicates the VLAN identifiers allowed when port Mode is Access. By default, only VLAN ID 1 is allowed in ports configured as Access ports. If required, it can be added VLAN identifiers. Allowed values are the VLAN range values (from 1 to 4,095). It is possible to insert specific VLAN identifiers separated by comma (for instance, 1,2,10,40), a range of VLAN identifiers using the “-” character (for instance, 10-40), and a meshed specific and range VLAN identifiers (for instance, 1,2,10-40);
- **Ethertype for Custom S-ports** : indicates Ethertype allowed (in addition to 802.1Q defined 0x8100 Ethertype) to ingress if port is configured as S-Custom-Port. When a frame has the Ethertype configured at this field, it will be classified to the VLAN ID embedded at the frame or, if no VLAN ID is embedded, it will be classified to the Port VLAN identifier. Values must be inserted in hexadecimal format.

Port VLAN Configuration

Port VLAN Configuration menu contains allowed per port configurations used by VLAN function. This menu allows configuring all VLAN settings at a given port. Port operation mode, allowed VLAN identifiers, VLAN filtering rules are examples of the configuration that this menu allows to be done. If one configuration is desired to be applied at all ports, then the row “*” should be used, that is, configuration done in the “*” row will be replied to all ports. Possible configurations are as follows.

- **Port**: shows the port to be configured at this row;
- **Mode**: indicates the mode of port operation. This field will define fundamental behavior of the port. Allowed values are as follows:
 - **Access**: indicates that port will operate as an access port. This is normally used by end stations, that is, VLAN-unaware equipment. Main characteristics of these ports are:
 - **VLAN Identifier Ingress process** : untagged frames are forwarded to the Port VLAN identifier VLAN, and tagged frames are forwarded to the VLAN that is embedded at the frame;
 - **Filtering ingress process** : both tagged and untagged frames are accepted, but frames that do not belong to the Allowed Access VLANs field or belong to the Forbidden VLANs field are discarded;

- **Egress process** : all frames will have its VLAN identifier removed, that is, access ports only egress untagged frames.
- **Trunk**: indicates that port will operate as a Trunk port. This is normally used by bridges connection or IED equipment that receives frames from multiple VLAN at the same port. For instance, Merging Unit sending Sampled Values and GOOSE messages throughout the same Ethernet interface should be connected to a Trunk port, as it will receive both VLAN messages. Main characteristics of these ports are:
 - **VLAN Identifier Ingress process** : untagged frames are forwarded to the Port VLAN identifier VLAN, and tagged frames are forwarded to the VLAN that is embedded at the frame;
 - **Filtering ingress process** : ingress process filtering will depend on the Egress tagging field configuration. A trunk port can accept both tagged and untagged frames if Egress tagging is set to Untag only frames with Port VLAN identifier. In this case, frames that do not belong to the Allowed VLANs field or belong to the Forbidden VLANs field are discarded. A trunk port can accept only tagged frames if Egress tagging is set to Tag all frames at the egressing process. In this case, frames that do not belong to the Allowed VLANs field or belong to the Forbidden VLANs field are discarded;
 - **Egress process** : egress behavior will depend on the Egress Tagging field configuration. A Trunk port can be set to Untag only frames with Port VLAN identifier (that is, untagged frames leave the switch untagged and tagged frames leave the switch tagged) or to Tag all frames.
- **Hybrid**: indicates that port will operate as a hybrid port. This is the most flexible port mode, as Hybrid ports allow configuring every process on the VLAN function. Main characteristics of these ports are:
 - **VLAN Identifier Ingress process** : untagged frames are forwarded to the Port VLAN identifier VLAN, and tagged frames are forwarded to the VLAN that is embedded at the frame;
 - **Filtering ingress process** : it is possible to define if only tagged, only untagged or if both tagged and untagged frames would be acceptable. Besides, frames that do not belong to the Allowed Access VLANs field or belong to the Forbidden VLANs field are discarded. Ingress Acceptance filtering does not depend on the egress Tagging process;
 - **Egress process** : egress behavior will depend on the Egress Tagging field configuration. A Hybrid

port can be set to Untag only frames with Port VLAN identifier (that is, untagged frames leave the switch untagged and tagged frames leave the switch tagged) or to Tag all frames. Egress Tagging filtering does not affect Ingress Acceptance filter.

- **Port VLAN:** Define the VLAN number (1 to 4095) from each Ethernet port.
- **Port Type:** Define the type form each port, as follow:
 - **Unaware:** indicates that port will operate as unaware in the ingress process. These ports will classify all frames to the Port VLAN identifier, independent of having VLAN identifier or not;
 - **C-Port:** indicates that port will operate as C-port in the ingress process. These ports will classify untagged frames to the Port VLAN identifier and will forward tagged frames to the VLAN embedded at the frame. At the egress process, C-Ports forward tagged frames (if configured to) with C-tag VLAN identifier;
 - **S-Port:** indicates that port will operate as S-port in the ingress process. These ports will classify untagged frames to the Port VLAN identifier. Tagged frames with Ethertype 0x8100 or 0x88A8 will be forwarded to the VLAN embedded at the frame. At the egress process, S-Ports forward tagged frames (if configured to) with S-tag VLAN identifier;
 - **S-Custom-Port:** indicates that port will operate as S-custom-port in the ingress process. These ports will classify untagged frames to the Port VLAN identifier. Tagged frames with Ethertype 0x8100 or with the value configured at the Ethertype for Custom S-ports will be forwarded to the VLAN embedded at the frame. At the egress process, S-Ports forward tagged frames (if configured to) with S-tag VLAN identifier;
- **Ingress Filtering :** enable frames ingress filtering function. If enabled, frames classified to a VLAN that port is not member is discarded. Thus, only Allowed VLANs identifiers and identifiers that do not belong to the Forbidden VLANs frames will be accepted. Checkbox selected means ingress filtering enabled, and checkbox empty means disabled;
- **Ingress Acceptance :** indicates ingress acceptance rules to be applied if Ingress Filtering is enabled. Allowed values are Tagged and Untagged, Tagged Only and Untagged Only, and possible configuration are as follows:
 - **Tagged and Untagged :** means that port will accept both tagged and untagged frames (respecting the Allowed VLANs and Forbidden VLANs rules);
 - **Tagged Only:** means that port will accept only tagged frames (respecting the Allowed VLANs and Forbidden VLANs rules). Untagged frames will be discarded;

- **Untagged Only**: means that port will accept only untagged frames, which will be forwarded to the Port VLAN identifier VLAN. Tagged frames will be discarded;
- **Egress Tagging**: indicates egress tagging rules to be applied at frame egress process at the port. Allowed values are Untag Port VLAN, Tag All and Untag All, and possible configuration are as follows:
 - **Untag Port VLAN**: means that all VLAN identifiers will remain as it ingress at the switch except VLAN identifiers equal to the Port VLAN number. If VLAN Identifier (VID) of the frame at the egressing queue is equal to Port VLAN, switch will remove VID and frame will be forwarded as untagged frame. Other VID numbers are not affected and are forwarded with their VLAN identifier tag;
 - **Tag All**: means that all frames at the egressing queue will be forwarded as tagged frame, including frames that had entered at the switch as untagged;
 - **Untag All**: means that all frames at the egressing queue will be forwarded as untagged frame, including frames that had entered at the switch as tagged;
- **Allowed VLANs**: indicate the VLANs a port can become a member of. Access ports have this field disabled, and these ports can only be member of the Allowed Access VLANs identifier VLAN. Trunk and Hybrid mode ports can be member of many VLAN, and this field specifies all VLAN that these port modes can be member of. Allowed values are the VLAN range values (from 1 to 4,095). It is possible to insert specific VLAN identifiers separated by comma (for instance, 1,2,10,40), a range of VLAN identifiers using the "-" character (for instance, 10-40), and a meshed specific and range VLAN identifiers (for instance, 1,2,10-40). By default, Trunk and Hybrid ports are members of all VLAN range (1 - 4,095);
- **Forbidden VLANs**: indicate the VLAN a port cannot become a member of. Access, Trunk and Hybrid mode ports can be configured to refuse many VLAN identifier traffic, and this field specifies all VLAN that these port modes cannot be member of. Allowed values are the VLAN range values (from 1 to 4,095). It is possible to insert specific VLAN identifiers separated by comma (for instance, 1,2,10,40), a range of VLAN identifiers using the "-" character (for instance, 10-40), and a meshed specific and range VLAN identifiers (for instance, 1,2,10-40). By default, all ports have this field empty, meaning that there is no VLAN restriction.

12 Quality of Service (QoS)

Quality of service function is used to guarantee traffic priority when LAN (or VLAN) network is congested. There are several ways to separate prioritized traffic from general purposes traffics, Reason S20 supports QoS function at the CoS and DSCP bits, for layer 2 and layer 3 communication respectively.

Thus, this chapter will focus on the CoS (Class-of-Service) bits usage, over 802.1Q Ethernet frames, which is one type of QoS. As shown in the VLAN chapter, 802.1Q frames include a 3-bits field for determination of the priority of that marked VLAN packet. Differentiated Services Code Point (DSCP) over IP traffic is also supported by Reason S20 as explained in this chapter.

12.1 QoS Basics

Consider the network capacity is oversized, as shown below, all incoming data is processed and forwarded. The data packets can be understood as Ethernet frames to be processed by the switch. Besides, this philosophy can be extrapolated to other layering protocols.

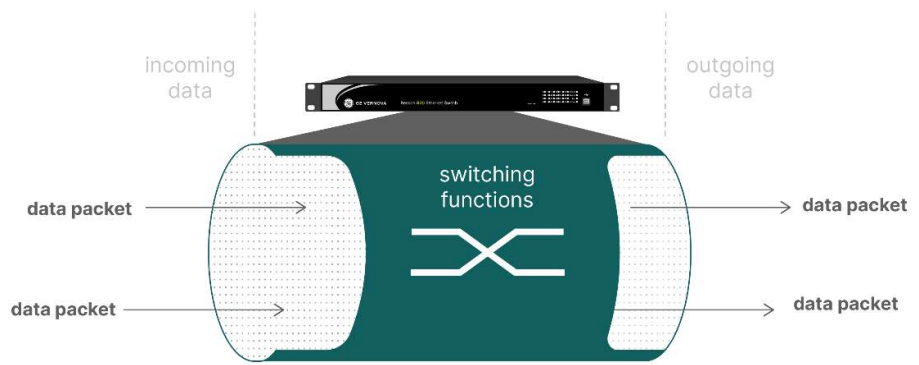


Figure 56: Traffic in an oversized

If there are sporadic small time peaks on incoming data, the switch stores packets that could not be delivered in an internal buffer and then, when the peak traffic ends, data is forwarded and buffer memory gets empty. Besides, if incoming data traffic increases for a time higher than the buffers inside the switch can support, then there will be data lost.

At power system communication, there is a wide use of connectionless communication protocols, that is, protocols that does not guarantee the delivery of sent data. NTP time protocol, as an example, uses UDP transport protocol. GOOSE and Sampled Values protocols are mapped directly at Ethernet frame and use multicast transport mechanism, thus being connectionless protocols. PTP protocol can be mapped directly at Ethernet, as GOOSE and Sampled Values, or at UDP, as NTP protocols. In this situation, to guarantee that higher priority data will not be lost, some quality at the network services should be provided.

Where traffic cannot be dropped, it must use some Quality-of-Service (QoS) mechanism to ensure that data will not be lost. This mechanism will guard a part of its bandwidth to be used only by these messages. General traffic will be stored in a queue to be forwarded, and higher priority traffic will have different queue to be stored before it is forwarded. When forwarding data, the switch will deliver firstly higher priority data, and will forward remaining traffic after high priority data queue is empty. If lower priority data reach its bandwidth, there will be lost of data, but the higher priority data will not be affected, as it has guarantee of bandwidth. Figure below shows an example of such situation.

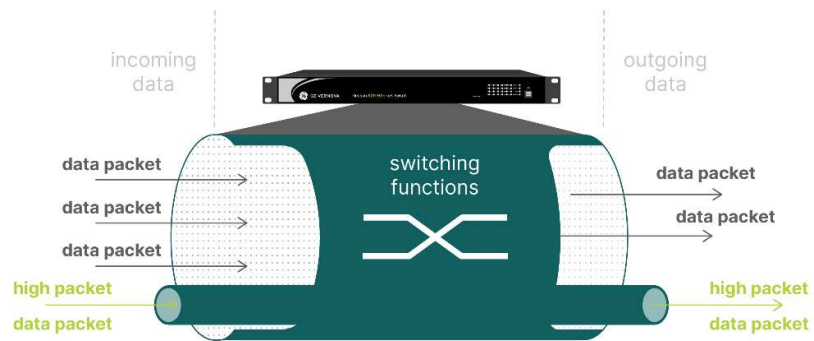


Figure 57: Network with prioritization of traffic

At data link layer, there are the Priority bits in 802.1Q frame that can be used. At network layer, DSCP information in IP protocol header can also be used, and so on.

Class-of-Service (CoS) bits of QoS

First development of a standard to incorporate traffic prioritization started at the IEEE 802.1p standard, which nowadays is inside the IEEE 802.1Q standard. At the last one, there is a 3-bit length field, the class-of-service bits (CoS), that is used to set which priority the network should use for this frame. Next figure shows the 802.1Q and CoS bits, called Priority Code Point (PCP).

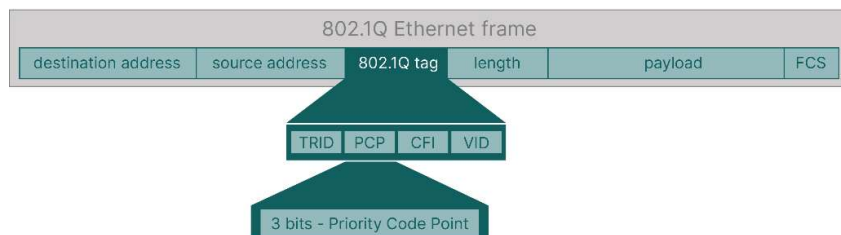


Figure 58: CoS bits inside and 802.1Q frame

There is a general agreement that QoS term is referred to means that equipment guarantee quality at determined kind of traffic in a given network. Thus, Quality of Service can be performed in different layers and different ways. Besides, the CoS term which is one of the QoS mechanism, the one that uses the priority information inside the 802.1Q Ethernet frame. At this manual, the term QoS is used as means that the network performs quality at determined service and CoS is used as a way to implement QoS in a given LAN by inspecting 802.1Q frames.

As this is a 3-bit field, there is the possibility to use eight values of priority, from 0 to 7. 802.1Q standard shows how these bits should be used to ensure prioritization to traffic, shown in the figure below.

One important point is that the value 1 is the lowest priority mark. Legacy equipment, which does not support 802.1Q frames, is understood as priority number 0. Priority 0, at the standard, is mapped as Best-effort quality, above the number 1. This ensures that legacy equipment traffic would not be always treated as background traffic when mixed to 802.1Q aware equipment. In addition, even though priority 7 is the highest, it is not recommended to use this prioritization in traffic that does not belong to network control or management.

Table 6: CoS Traffic Priority

Priority	Acronym	Traffic Type
1 (Lowest priority)	BK	Background
0 (Default)	BE	Best Effort
2	EE	Excellent Effort
3	CA	Critical Applications
4	VI	"Video", < 100 ms latency and jitter
5	VO	"Voice", < 10 ms latency and jitter
6	IC	Internetwork Control
7 (Highest priority)	NC	Network Control

Besides, IEC 61850-90-4 Technical Report recommend mapping the CoS bits as shown below. In addition, the document specifies the usage of priority High for Sampled Values data and priority Medium or High for synchronization messages. MMS messages, which are used by IED communication in power system and other traffics over TCP/IP networks should use priority to Low or Medium, according to the technical report.

Table 7: CoS classification as recommended by IEC 61850-90-4

Priority	QoS	Typical Application
7	Critical	Network management (using VLANs)
6	High	GOOSE messages used for tripping and inter tripping
5	Medium	GOOSE messages used for interlocking merging units
4	Medium	GOOSE messages used for other purposes
3	Medium	Substation Automation (using VLANs)
2	Normal	Engineering (using VLANs)
1	Normal	Quality of Supply metering
0	Normal	Security systems, meters, IP cameras.

The queue description given below is known as a strict priority queue. By default, Reason S20 operate in the Strict Priority Queue mode. If a given LAN needs to dynamically prioritize traffic which there is higher classes transmission, but no stop on transmission in the lower classes traffic, then the port shaping or WRED functions can be used.

One important point using CoS bits is that traffic prioritization will be linked to the VID (VLAN ID) of the frame. Thus, this QoS mechanism will prioritize traffic from one VLAN over another. As there is traffic prioritization related to the VLAN, this mechanism assumes that data at the given VLAN must be prioritized.

IED equipment, in power system communication, should send packets containing VLAN and priority information. This way, as they send packets classified to determined CoS, the switch will by default queue the packet in CoS defined queue. If all IED are correctly configured to send GOOSE, Sampled Values and PTP messages, the switch will classify the packets by default, with no need for QoS configurations.

If core networking equipment has some philosophy on traffic prioritization of CoS values that is different from the edge equipment, it is possible to re-map the frames to a given CoS at the switch. There are several applications

there is a need to change incoming frame CoS to adapt it to the network. Thus, incoming frame from a given CoS will be stored in another CoS queue, and forwarded with the new CoS values.

If application requires the switching equipment to be able to inspect the type of traffic to prioritize them, it is possible to map messages to a determined CoS value, and then there will be effectively traffic prioritization defined by traffic type, not by VLAN. It is possible to prioritize traffic based on Ethertype, UDP or TCP transport protocol, and so on.

Differentiated Service Code Point (DSCP)

The use of specific field at the IP headers was standardized at RFC 2474 document. It specifies the usage of a 6-bit length field, the Differentiated Service Code Point (DSCP) bits that are used to set which priority the network should use for incoming IP frames. Note that, while CoS bits are mapped in data-link layer, DSCP is used at network layer, thus at IP communication environment. Such environment includes NTP and PTP protocols (if mapped to UDP transport) but they are not allowed to GOOSE or Sampled Values data. Figure below shows the IP header and DSCP bits



Figure 59: IP Header frame and Differentiated Service Code Point explained

The Type-of-Service (ToS) byte has two sub groups, one is the Differentiated Service Code Point (DSCP) bits with 6-bit length field that allows the IP header to carry prioritized information of the incoming data. In addition, there are two remaining bits, the Explicit Congestion Notification (ECN) defined in the RFC 3168 document.

ECN allows the IP packets to carry information if the packet has suffered congestion at data traffic. Thus, as there is marking at the packet that it suffered from congestion at the path between sender and receiver, the sender can adjust its bandwidth to the network to avoid data lose. This mechanism makes QoS more reliable, as there will be notification of congestion at the packet, and then the hosts can adjust themselves to prevent losing data. Otherwise, the only way to verify if the network was congested was losing packets.

If core networking equipment has some philosophy on DSCP values that is different from the edge equipment, it is possible to re-map the frames to a given DSCP at the switch. There are several applications where there is a need to change incoming frame DSCP to adapt it to the network. Thus, incoming frame from a given DSCP will be marked as a new DSCP value and will be forwarded with this new DSCP value.

GE Reason S20 QoS Capabilities

GE Reason S20 allows the user to apply QoS in network applications at layer 2 protocols. For layer 3 applications, DSCP-based QoS is also supported. There are two types of QoS available:

- CoS values QoS;

- Direct CoS value at 802.1Q frames;
- Protocol Mapping to CoS;
- DSCP mapping to CoS.
- DSCP values QoS.

As shown in the previous sections, VLAN tagged frames always carry information of packet prioritization. Thus, quality of service is guaranteed to higher priority VLAN identification over lower values, as each CoS value has a specific queue at forwarding decision.

If IED equipment sends priority information correctly at the frames that are sent throughout the network, then Reason S20 will perform its QoS functions without need to configuration, as default configuration ensures that CoS value is queued correctly. This means also to IP communication sending DSCP bits value, which is informing the IP network equipment its priority over the network. Thus, if there is no legacy equipment without CoS capabilities, configuration might not be necessary. In addition, strict priority is generally enough to ensure QoS services. Thus, using weighted queues or WRED congestion detected should be clearly understood before using, as these mechanisms increase network complexity.

QoS configuration is applied when legacy equipment is connected as it does not allow prioritization itself. Besides, strict priority can be changed to weighted queues, or early congestion detection can be obtained over IP protocols with WRED function when network simulations show that network performance can be increased without increasing network bandwidth.

By default, ports are classified to queue 802.1Q non-compliant packets at CoS priority number 0 (best-effort service) and uses CoS information from incoming 802.1Q frames to queue at the given CoS value queue. Besides, tag classification can be enabled to change which queue will be used by incoming data with CoS information. Each port has independently classification, enabling the user to remark CoS value independently at each port. At packet egress processing, it is possible to remark the CoS value at the packets from a given queue, thus enabling incoming data to be re-mapped with another CoS value as illustrated in the figure below.

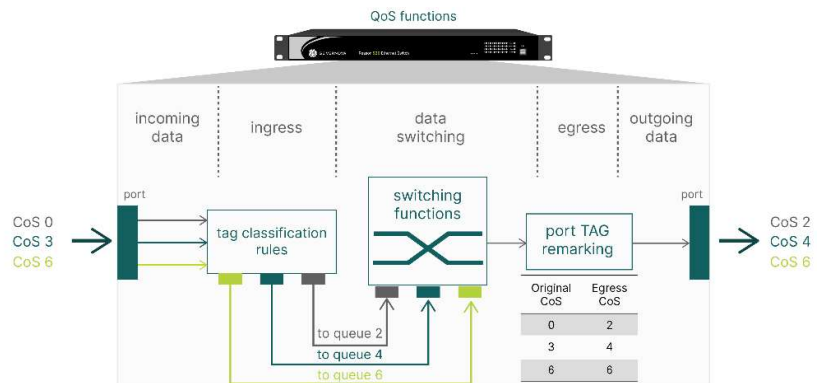


Figure 60: CoS queues and remarking functions

Besides, it is possible to configure port incoming traffic to guarantee class of service by limiting bandwidth at a given port, thus saving processing at ports which hosts such IED or low priority networks are connected. This

function is called Queue Policing. In addition a flow control can be used to send paused frames instead of discarding them. This function is called Port Policing at Reason S20.

By default, Reason S20 queues are scheduled and forwarded as strict priority mode, that is, only if higher CoS queues are empty a given CoS queue will start forwarding traffic. This ensures that higher priority queues will always forward traffic before lower ones. Besides, it is possible to change the egress schedule queues and port behavior to forward traffic based in average traffic, to guarantee that average traffic at a given queue or port will be reliable. These functions are allowed only for 0 to 5 priorities CoS queues, and are divided in Port Scheduler and Port Shaping functions. CoS 6 and CoS 7 priorities queues operate only in strict priority mode. Port scheduler functions allow the user to set a weight value to prioritize some of them based on average calculations. Thus, at instantaneous point of view there will be some transmission of lower queues traffic, but the average traffic of higher CoS queues will be higher and based on its weight at the transmission. To limit bandwidth at a given port, based on the weight and configurations at port scheduler, there is the Port Shaping function. When using strict priority mode, port and queue policing would perform these functions.

If IP packets that traffic in the switch carry information of priority at DSCP bits, the switch can process higher priority IP packets to ensure less delay at transmission of them over lower priorities packets. By default, this function is disabled.

If enabled, DSCP-based QoS will perform its functions much like CoS bits do, been also possible to enable DSCP independently at each port of the switch, classify each priority in a specific queue for forwarding decisions and then translate the incoming DSCP value to another before egressing the packet, as shown below.

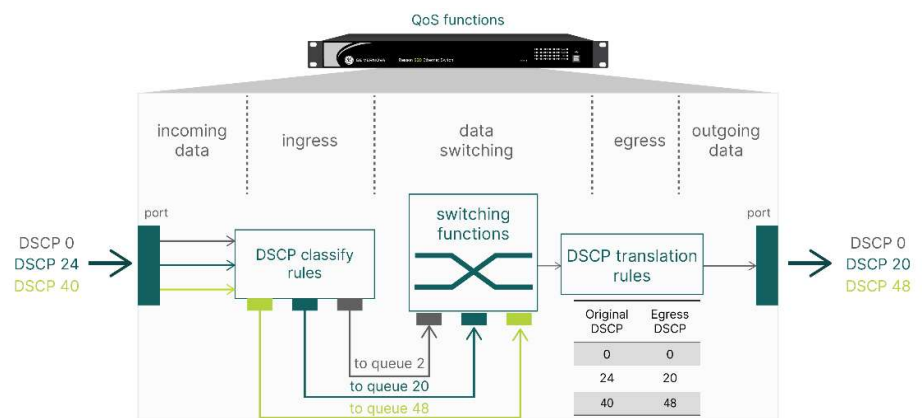


Figure 61: DSCP queues and translation functions

As explained in previous sections, it could be desired to do a relationship between DSCP and CoS values, to mix IP and 802.1Q priority mechanisms and increase its performance over the network. At Reason S20 this function is called DSCP classification, and it is possible to do a direct mapping of DSCP values to each CoS possible values. By default, all DSCP priorities are classified as CoS 0 (best-effort service).

If there is no direct VLAN-mapped priority or IP DSCP mechanism specified at a given LAN, the switch can search for traffic or addresses involved to map them as a specific QoS queue (CoS value and DSCP value), making a real traffic-prioritized function. If, for any reason, IED or hosts at a given network do not allow to configure specific messages to the VLAN, this mechanism can be used to ensure types of message prioritization over other ones.

Reason S20 can perform protocol-to-CoS mapping over several filters, where there is the freedom to select which ports will be filter designed. To schedule traffic in specific queues, Reason S20 uses the following methods:

- Destination MAC address;
- Source MAC address;
- VLAN parameters:
 - Untagged frames to CoS queue;
 - Specific tagged frames to CoS queue;
 - A range of tagged frames to CoS queue;
- CoS and DEI values;
- Frame type:
 - Specific Ethertype to CoS queue;
 - Specific LLC parameters to CoS queue;
 - SNAP PID value to CoS queue;
 - IP packets (both IPv4 and IPv6).
 - Specific or a range of source IP addresses to CoS queue;
 - Specific or a range of source and destination TCP ports to CoS queue;
 - Specific or a range of source and destination UDP ports to CoS queue;
 - Specific or a range of DSCP value to CoS queue.

Thus, if Sampled Values and GOOSE messages are in the same VLAN, it is possible to prioritize one of them over another using its Ethertype, MAC address destination and so on. Besides, for NTP protocol, it is possible to prioritize it using its UDP port to redirect this traffic to a specific CoS queue. There are several ways to do traffic priority services if CoS bits of the incoming data cannot be directly used. Reason S20 allows up to 256 rules at the QoS Control list, which perform this function.

One major QoS function is the prevention of over flux of messages in a given port, which can occur at unicast, broadcast or multicast transport mechanisms. These functions are called Storm policers, and can be performed by Reason S20. Each port can be configured independently to limit bandwidth in Unicast, Multicast and Broadcast messages.

Finally, if strict priority has not the performance required at a given LAN, then Weighted Random Early Detection (WRED) function can be used as a method to discard frames based on previous assumptions. To choose which frame could be dropped in this mechanism it is used the DEI bits in an 802.1Q frame. Thus, packets with DEI 0 are never chosen to be dropped, and packets with DEI 1 are drop-eligible packets. It is allowed to choose up to 3 queues to have congestion detection, from 0 to 5 priorities CoS

queues. CoS 6 and CoS 7 priorities queues cannot be used. The selection of the queues to be used for congestion detection is made at the ingress port classification, where each port is classified at a drop precedence level (DPL), between 0 and 3. DPL equal 0 means that these packets cannot be lost and DPL level 1, 2 or 3 mean that packets are eligible to be dropped. Enabling a queue will permit the switch to perform the WRED function at that queue. There are, then, four fields that must be configured so the WRED can be executed correctly: Minimum Threshold, Maximum Drop Probability 1, 2 and 3.

Minimum Threshold field represents the average filling level of the queue which the switch will start dropping frames randomly. Frames with DEI = 1 in the queue will be drop-eligible packets. Thus, before there is congestion at the network, the switch will drop frames to prevent congestion, after the average load of a given queue is extrapolated.

Maximum Drop probability fields specify the maximum drop probability of a given traffic on the queue to be dropped. Thus, if the average filling level of a given queue gets closer to 100%, the drop probability will get closer to the drop probability specified. The selections of the DP levels are made at the port classification, where each port has a specific DPL (drop precedence level) which can be used. DPL equal 0 means that no packet should be used at the election, and 1, 2 or 3 will select which queue will be used by the port with thresholds configured at the maximum DP levels.

12.2 Port Classification

Port Classification menu allows configuring basic QoS ingress classification at a given port. If one configuration is desired to be applied at all ports, then the row “*” should be used, that is, configuration done in the “*” row will be replied to all ports.

- **Port:** shows the ports to be configured at this row;
- **CoS:** indicates CoS that will be used the ingress process. These ports will classify untagged frames to the CoS class configured at this field and will forward tagged and priority-tagged frames to the CoS queue embedded at the PCP bits in the 802.1Q frame. By default, all untagged frames are classified to the CoS 0 queue, which means lowest priority class-of-service for that packets. Also, by default there is a one-to-one mapping of CoS and PCP bits. Allowed values are the PCP bits range values (from 0 to 7);
- **DPL:** indicates the Drop Precedence Level to be used in the ingress process. These ports will classify untagged frames to the DPL class configured at this field and will forward tagged and priority-tagged frames to the DPL embedded at the frame. DPL level 0 means that packet cannot be dropped, and level 1, 2 and 3 means that packet can be dropped randomly based on the WRED threshold. By default, all untagged frames are classified to the DPL 1. Allowed values are from 0 to 3;
- **PCP:** indicates PCP that will be used the ingress process. These ports will classify untagged frames to the PCP class configured at this field and will forward tagged and priority-tagged frames to the

PCP queue embedded at the PCP bits in the 802.1Q frame. By default, all untagged frames are classified to the PCP 0 queue, which means best-effort class-of-service for that packets. Allowed values are the PCP bits range values (from 0 to 7);

- **DEI:** indicates the Drop Eligible flag to be used in the ingress process. These ports will classify untagged frames to the DEI class configured at this field and will forward tagged and priority-tagged frames to the DEI embedded at the frame. DEI level 0 means that packet cannot be dropped, and level 1, means that packets are allowed to be dropped. By default, all untagged frames are classified to the DPL 0. Allowed values are 0 and 1;
- **Tag Class.:** indicates classification mode to be used by the port. Tag Class field is a hyperlink that allows accessing QoS Ingress Port Tag Classification, where it is allowed to configure a PCP-to-QoS queue at each port independently. This configuration is only applied in tagged or priority-tagged frames, that is, frames with PCP information. Possible values are Disabled and Enabled. Disabled means that PCP used in tagged and priority-tagged frames will be the value embedded at the frame, and enabled means that QoS queue selected by each PCP value will be as configured in that port. Possible configuration after clicking Tag Class hyperlink are as follows:
- **Tag Classification:** indicates if Tag Classification for tagged frames should be enabled or not. Possible values are Enabled and Disabled. Selecting Enable allow port to map PCP incoming values to configured QoS queue, and selection Disable allow port to map PCP incoming values to the corresponding QoS queue;
 - **PCP:** show PCP values that can be configured;
 - **DEI:** show DEI values that can be configured;
 - **QoS class:** indicates which QoS queue the frames with PCP and DEI values in the row should be redirected. This allows redirecting incoming frames from one PCP level to another queue;
 - **DP level:** indicates which DP levels the frames with PCP and DEI values in the row should be redirected. This allows configuring incoming frames from a given PCP and DEI values to a determined DPL parameter;
- **DSCP Based:** enable DSCP-based QoS function at the port. If DSCP bits are allowed, this checkbox allows the switch to use this information at the IP packet to perform QoS functions. Checkbox selected means DSCP-based QoS enabled, and checkbox empty means disabled.

12.3 Port Policing

Port Policing menu allows configuring traffic limits for the ports.

- **Port:** shows the ports to be configured at this row;

- **Enabled:** enable Port Policing function at the port. Checkbox selected means function enabled, and checkbox empty means disabled;
- **Rate:** indicates the maximum allowed traffic on that port. Traffic rates at the port higher than this field are not allowed if function is enabled, then traffic close to the limit will start packet losing based on the QoS configured. Allowed values are integer values and limits depend on the Unit used. Range of 100 to 1,000,000 is allowed when kbps or fps units are used. Range of 1 to 32,000 is allowed when Mbps or kfps units are used;
- **Unit:** indicates which unit should be used with Rate value to limit traffic. Allowed values are kbps, Mbps, fps and kfps;

12.4 Queue Policing

Queue Policing menu allows configuring traffic limits at each queue in a port.

- **Port:** shows the ports to be configured at this row;
- **Queue enable:** enable Queue Policing function at the port. Checkbox selected means function enabled, and checkbox empty means disabled. Reason S20 has a table with number of rows equal to the number of ports and number of columns equal to the number of QoS queues. Thus, each queue in each port can be independently configured to do traffic queue policing. If a given port at a given queue is enabled, Queue column displays possible configuration to that queue. Possible configuration is as follows:
 - **Rate:** indicates the maximum allowed traffic on that port. Traffic rates at the port higher than this field are not allowed if function is enabled, then traffic close to the limit will start packet losing based on the QoS configured. Allowed values are integer values and limits depend on the Unit used. Range of 100 to 1,000,000 is allowed when kbps or fps units are used. Range of 1 to 32,000 is allowed when Mbps or kfps units are used;
 - **Unit:** indicates which unit should be used with Rate value to limit traffic. Allowed values are kbps, Mbps, fps and kfps.

12.5 Port Scheduler

Port Scheduler menu allows configuring priority type at each port. By default, Reason S20 operates in strict priority. If necessary, up to 6 queues (except 6 and 7 CoS queues) can be weighted, thus packet drop process should weight the queues instead of waiting higher level queues to be empty. Besides, weighting process will store excess data in an internal buffer to be sent later, thus this function would require memory available to store frames. Possible configurations are as follows.

- **Port:** indicate the ports to be configured at this row. Port field is a hyperlink that allows accessing QoS Egress Port Scheduler and Shapers settings. Port scheduler menu allows configuring port to operate in Strict Priority scheduler mode or 6 Queues Weighted mode. Possible configuration after clicking Port number hyperlink are as follows:
 - **Scheduler Mode:** indicates which mode port scheduler is operating. Each port can be freely configured to operate as strict or weighted mode. Allowed values are Strict Priority and 6 Queues Weighted. Strict priority means that lower priority queue will only start forwarding frames after higher priority queue is empty. 6 queues weighted means that queues CoS 0 to 5 will be weighted and frames will be randomly discarded based on the weight configuration;
 - **Queue Shaper:** indicates queue rate to be used by shaping function. Each queue has its own shaper configuration. If congestion happens at a given queue at the port, queue shapers will perform switching functions to guarantee that average traffic at that queue does not exceed Queue Shaper Rate configured. Possible configuration are as follows:
 - **Enable:** enable Queue Shaper function at the Cos queue. Checkbox selected means function enabled to that queue, and checkbox empty means disabled;
 - **Rate:** indicates maximum average traffic allowed in the queue. Sporadic peak traffic will be stored at internal buffer to be forwarded when peak traffic is lower than Queue Shaper Rate value. Allowed values are integer values and limits depend on the Unit used. Range of 100 to 1,000,000 is allowed when kbps or fps units are used. Range of 1 to 32,000 is allowed when Mbps or kfps units are used;
 - **Unit:** indicates which unit should be used with Rate value to limit traffic. Allowed values are kbps, Mbps, fps and kfps;
 - **Excess:** enable this queue to use (if necessary) excess of bandwidth when compared to the Queue Shaper Rate value. Checkbox selected means function enabled to that queue, and checkbox empty means disabled.
 - **Queue Scheduler:** indicates the weight of the queue on the dynamic weight algorithm. This configuration is only allowed if Scheduler Mode is set to 6 Queues Weighted. Allowed configuration is as follows:
 - **Weight:** indicates the weight that queue will have in the shaping process. This number will be used by

- internal algorithm to define how much average bandwidth that queue can use;
 - **Percent:** shows the percentage value that the queue will fill in allowed bandwidth to the queues in weighted mode.
- **Port Shaper:** indicates port rate to be used by shaping function. Each port has its own shaper configuration, and each queue at a given port have its own configuration too. If congestion happens at a given port, port shapers will perform switching functions to guarantee that average traffic at that port does not exceed Port Shaper Rate configured. Possible configuration are as follows:
 - **Enable:** enable Port Shaper function at the port. Checkbox selected means function enabled to that queue, and checkbox empty means disabled;
 - **Rate:** indicates maximum average traffic allowed in the port. Sporadic peak traffic will be stored at internal buffer to be forwarded when peak traffic is lower than Port Shaper Rate value. Allowed values are integer values and limits depend on the Unit used. Range of 100 to 1,000,000 is allowed when kbps or fps units are used. Range of 1 to 32,000 is allowed when Mbps or kfps units are used;
 - **Unit:** indicates which unit should be used with Rate value to limit traffic. Allowed values are kbps, Mbps, fps and kfps.
- **Mode:** shows priority queue mode of operation configured at the QoS Egress Port Scheduler and Shapers menu;
- **Weight:** shows the value in percentage of the weight of the queues at that port. If operation of the port is Strict Priority, then the “-” character will be displayed as the weight value, which means no weight process being used. If operation of the port is weighted, then displayed values are from allowed queues, from CoS 0 to 5.

12.6 Port Shaping

Port Shaping and Port Scheduler menus work together to allow configuring priority type at each port and each queue. While Port Scheduler shows each port mode and queues weight, Port Shaping shows each port shaper values divided in queues. That is, rate values configured at port scheduler are displayed at this menu. By default, Reason S20 operates in strict priority. If necessary, up to 6 queues (except 6 and 7 CoS queues) can be weighted, thus packet drop process should weight the queues instead of waiting higher level queues to be empty. Besides, weighting process will store excess data in an internal buffer to be sent later, thus this function would require memory available to store frames. Configuration options are similar as Port Scheduler, expect by:

- **Shapers:** shows priority queues and total port shaper values configured at QoS Egress Port Scheduler and Shapers menu. If operation of the port is Strict Priority, then the “disable” word will be displayed as the shaper value, which means no shaper process being used. If operation of the port is weighted, then displayed values are the Rate values configured from each queue and port at the QoS Egress Port Scheduler and Shapers menu.

12.7 Port Tag Remarking

Port Tag Remarking menu allows configuring egress behavior of frames. Thus, this menu allows remapping all frames that have priority information at the ingress process. Ports can be set to not change PCP value at egress of the frame, use only one defined PCP to all frames or map each QoS queue to a specific PCP value. Possible configurations are as follows.

- **Port:** indicate the ports to be configured at this row. Port field is a hyperlink that allows accessing QoS Egress Port Tag Remarking settings. Port remarking menu allows configuring behavior of the port related to frames egressing the port. After clicking Port number hyperlink, the QoS Egress Port Tag Remarking menu will be displayed for the port chosen. Tag Remarking mode indicates port behavior. Allowed values are Classified, Default and Mapped.

Possible configurations are as follows:

- **Classified:** indicates port behavior as classified QoS tag remarking. In this mode, egressing untagged frames are forwarded with port default QoS value (PCP = 0). Tagged and priority-tagged frames are forwarded with PCP bits equal to the PCP bits embedded at the incoming 802.1Q frame;
- **Default:** indicates port behavior as default QoS tag remarking. In this mode, egressing untagged, tagged and priority-tagged frames are forwarded with port default QoS value configured. When this mode is selected, the Default PCP and Default DEI fields are shown, allowing user to configure PCP and DEI values to be used in all forwarded frames. Possible configurations are as follows:
 - **Default PCP:** indicates which PCP value must be attached to all egressing frames. Allowed values are the PCP bits range values, from 0 to 7;
 - **Default DEI:** indicates which DEI value must be attached to all egressing frames. Allowed values are the DEI bits range values, 0 or 1.
- **Mapped:** indicates port behavior as mapped QoS tag remarking. In this mode, egressing untagged, tagged and priority-tagged frames are forwarded with QoS value configured. Each PCP value and DEI value embedded can be mapped to a specific PCP to egress process independently. When this mode is selected, the (QoS Class, DP level) to (PCP, DEI) mapping table is shown, allowing

user to configure PCP and DEI values to be used in all forwarded frames per queue. Possible configurations are as follows:

- **QoS class:** shows the QoS queue to be configured at this row;
- **DP level:** shows the DP level to be configured at this row;
- **PCP:** indicates which PCP value must be attached to frames with QoS class (PCP bits) and DP level shown in the QoS class and DP level columns. That is, a given PCP frame with a given DP level should be remarked at egressing process to the PCP value configured in this field. Allowed values are the PCP bits range values, from 0 to 7;
- **Default DEI:** indicates which DEI value must be attached to frames with QoS class (PCP bits) and DP level shown in the QoS class and DP level columns. That is, a given PCP frame with a given DP level should be remarked at egressing process to the DEI value configured in this field. Allowed values are the DEI bits range values, 0 or 1.

12.8 Port DSCP

Port DSCP menu allows enabling DSCP QoS function and basic configuration. At this menu it is possible to enable if DSCP will be used as quality of service mechanism and define basic behavior of its usage. Possible configurations are as follows.

- **Port:** shows the port to be configured at this row;
- **Translate:** indicates if ingress translation should be used by this port. This checkbox is used together with the Classify field to define the ingress rules of the DSCP function. Checkbox selected means ingress translation enabled, and checkbox empty means disabled;
- **Classify:** indicates how should be executed DSCP ingress classification. Possible configuration is as follows:
 - **Disable:** indicates that no ingress DSCP is used. This means that DSCP analysis for QoS function is disabled at the port;
 - **DSCP=0:** indicates that only frames with DSCP bits equal 0 should be classified. DSCP-to-QoS Class classification will be as configured at the DSCP Classification;
 - **Selected:** indicates that only frames with DSCP bits marked should be classified. If selected, the DSCP Translation menu should be used to select which DSCP levels should be classified;

- **All:** indicates that all frames with DSCP bits will be classified. If selected, all frames will be classified to a DSCP queue.
- **Egress:** indicates how should be executed DSCP egress rewriting process. Possible configuration is as follows:
 - **Disable:** indicates that no egress DSCP rewriting is used. This means that DSCP bits of a given incoming frame will be discarded at the egress process;
 - **Enable:** indicates that egress DSCP rewriting is used, but there is no remap of the DSCP bits. This means that DSCP bits of a given incoming frame will be maintained at the egress process;
 - **Remap:** indicates that egress DSCP rewriting is used and DSCP bits will be remapped to the values configured at the DSCP Translation menu. This means that DSCP bits of a given incoming frame will be changed as configured by user at the egress process.

12.9 DSCP-Based QoS

DSCP-Based QoS menu allows enabling DSCP QoS based on a DSCP-to-QoS Class mapping. At this menu it is possible to map each DSCP value to a given QoS Class queue and DPL levels. Possible configurations are as follows.

- **DSCP:** shows the DSCP level to be configured at this row;
- **Trust:** indicates if DSCP value is trusted, and thus can be remapped to the QoS Class and DPL configured. Only trusted DSCP levels are remapped as configured to the QoS Class and DPL columns. Untrusted DSCP frames are treated as non-IP frame by the switch. Checkbox selected means DSCP level trusted, and checkbox empty means untrusted;
- **QoS Class:** indicates to which QoS Class queue the DSCP level frame should be remapped. Each DSCP value can be configured to the requested QoS Class queue independently. Allowed values are the PCP bits range values, from 0 to 7;
- **DPL:** indicates to which DPL level rule the DSCP level frame should be remapped. Each DSCP value can be configured to the requested DPL level independently. Allowed values are the DPL allowed range values, from 0 to 3.

12.10 DSCP Translation

DSCP Translation menu allows selecting which DSCP levels can be remapped to another level, and to configure translation parameters. If port DSCP translation is enabled (choosing the Selected Ingress Classify at the Port DSCP menu), values to be remapped at the ingress and egress

process will be as configured in this menu. Possible configurations are as follows.

- **DSCP:** shows the DSCP level to be configured at this row;
- **Translate:** indicates to which DSCP value the DSCP at the row should be translated. At a given row there will be the DSCP level to be configured. Incoming frames with this DSCP level will be, at ingress process, remapped to the DSCP level chosen at the Translate field. Allowed values are the DSCP values range, from 0 to 63;
- **Classify:** indicates if selected ingress translation should be used by this port. This checkbox will enable the Selected option at Classify at the Port DSCP menu. Thus, if a port is set to Selected, this field will specify which DSCP levels will be classified at the port. Checkbox selected means that DSCP level will be classified as configured, and checkbox empty means that port will not classify this DSCP level;
- **Remap:** indicates to which DSCP value the DSCP at the row should be translated. At a given row there will be the DSCP level to be configured. Frames internally treated with this DSCP level will be remapped at the egress process to the DSCP level chosen at the Remap field. Allowed values are the DSCP values range, from 0 to 63.

12.11 DSCP Classification

DSCP Classification menu allows selecting which DSCP levels should be applied at a given CoS (PCP) value at the Ethernet frame. While DSCP-Based QoS Ingress Classification allows mapping to which QoS queue the DSCP values should be mapped to, that is, allows a DSCP-to-CoS mapping, DSCP classification allows selecting a CoS-to-DSCP classification. Thus, it is possible to include PCP bits based QoS at the DSCP philosophy QoS. Possible configurations are as follows.

- **QoS Class:** shows the QoS class to be configured at this row;
- **DSCP:** indicates to which DSCP level the QoS class at the row should be mapped to. This field will effectively do the CoS-to-DSCP configuration, as the CoS possibilities are shown in the QoS Class column. Allowed values are the DSCP values range, from 0 to 63.

12.12 QoS Control List

QoS Control List menu allows configuring QCL function. QCL is a way to define quality-of-service for a given traffic based on many settings, such as destination or source MAC address, frame type, and so on. To define traffic to be classified, it must be created a QoS Control Entry (QCE), which will define all parameters and action to be realized.

By default, no QCE is configured. To add a control entry, click at the button. After this button is pressed, the QCE configuration menu is opened. This menu will display all possible configuration to be applied in a QCE to be used at the QCL. Once at the QCE Configuration, after clicking the button shown below, possible configurations are as follows.

- **Port Members**: indicates which port will be a member of this QCE entry. If selected, the port will apply rules configured at the Key Parameters and Action Parameters. Checkbox selected means port is member of the QCE, and checkbox empty means port is not member;
- **Key Parameters**: indicates all parameters to be applied. If frames match with all key parameters configured, then frame will be treated as configured at the Action Parameters. Possible configuration are as follows:
 - **DMAC**: indicates type of destination MAC address. Possible values are Any, which means all MAC addresses types, Unicast, Multicast and Broadcast MAC addresses;
 - **SMAC**: indicates OUI value of source MAC address to be applied as filter. Possible values are Any, which means all MAC addresses, and Specific MAC address. If specific is selected, the OUI field of the MAC address will be used as a parameter. Allowed values are hexadecimal values, and each byte should be separated by a “-” signal;
 - **Tag**: indicates if frame to be applied in this QCE would be tagged or untagged. Possible values are Any, which means no filter based on VLAN identifier number, Tagged and Untagged values;
 - **VID**: indicates VLAN identifier to be used as a filter, if Any of Tagged was selected as options at the Tag field. Possible values are Any, which means all VLAN identifier numbers, Specific and Range. If specific is selected, the Value field must be filled with VID number desired, and allowed values are the VLAN range values (from 1 to 4,095). If range is selected, the From and To fields must be filled with VID range numbers desired, and allowed values are the VLAN range values (from 1 to 4,095);
 - **PCP**: indicates PCP values to be applied as filter at the key parameters. Allowed values are the PCP range values, from 0 to 7;
 - **DEI**: indicates DEI value to be applied as filter at the key parameters. Allowed values are the DEI range values, 0 or 1;
 - **Frame Type**: indicates frame type to be used as filter at the key parameters. Allowed values are Any, EtherType, LLC, SNAP, IPv4 and IPv6. Possible configuration is as follows:
 - **Any**: indicates that all incoming frames will be used at this QCE;
 - **EtherType**: indicates which ethertype will be allowed in this QCE. When selected, the Ethertype

Parameters will be displayed. Possible configuration is as follows:

- **Ethertype**: indicates which filter should be applied based on the ethertype field on the frame. Possible configuration is as follows:
- **Any**: indicates that all incoming frames will be used at this QCE;
- **Specific**: only ethertype configured will be used at this QCE, that is, this entry will map frames based in many parameters including its ethertype value. Values must be inserted in hexadecimal format.
- **LLC**: indicates which LLC values will be allowed in this QCE. When selected, the LLC Parameters will be displayed. Possible configuration is as follows:
 - **DSAP Address**: indicates which filter should be applied based on the Destination Service Access Point (DSAP) field at the frame. Possible configuration is as follows:
 - **Any**: indicates that all incoming frames will be used at this QCE;
 - **Specific**: only DSAP configured will be used at this QCE, that is, this entry will map frames based in many parameters including its DSAP value. Values must be inserted in hexadecimal format.
 - **SSAP Address**: indicates which filter should be applied based on the Source Service Access Point (SSAP) field at the frame. Possible configuration is as follows:
 - **Any**: indicates that all incoming frames will be used at this QCE;
 - **Specific**: only SSAP configured will be used at this QCE, that is, this entry will map frames based in many parameters including its SSAP value. Values must be inserted in hexadecimal format.
 - **Control**: indicates which filter should be applied based on the Control field at the LLC bytes on the frame. Possible configuration is as follows:
 - **Any**: indicates that all incoming frames will be used at this QCE;
 - **Specific**: only Control values configured will be used at this QCE, that is, this entry will map frames based in many parameters

including its Control value. Values must be inserted in hexadecimal format.

- **SNAP:** indicates which SNAP will be allowed in this QCE. When selected, the SNAP Parameters will be displayed. Possible configuration is as follows:
 - **PID:** indicates which filter should be applied based on the PID (Protocol Identifier field at the SNAP field) field on the frame. Possible configuration is as follows:
 - **Any:** indicates that all incoming frames will be used at this QCE;
 - **Specific:** only protocol identifiers (PID) configured will be used at this QCE, that is, this entry will map frames based in many parameters including its PID value. Values must be inserted in hexadecimal format.
- **IPv4:** indicates which IPv4 values will be allowed in this QCE. When selected, the IPv4 Parameters will be displayed. Possible configuration is as follows:
 - **Protocol:** indicates which filter should be applied based on the IPv4 protocol number field at the frame. Possible configuration is as follows:
 - **Any:** indicates that all incoming frames will be used at this QCE;
 - **UDP:** indicates that only UDP will be used at this QCE, that is, this entry will map frames based in many parameters including if it is a UDP protocol. When selected, the UDP Parameters will be displayed. Possible configuration is as follows:
 - **Sport/Dport:** Sport indicates which source UDP ports will be used at this QCE. In the other hand, Sport indicates which destination UDP ports will be used. Possible configuration is as follows:
 - **Any:** indicates that all incoming frames will be used at this QCE;
 - **Specific:** indicates that only specified UDP port

will be used at this QCE. Values must be inserted in decimal format;

- **Range:** indicates that only a range of specified UDP ports will be used at this QCE. Values must be inserted in decimal format.
- **TCP:** indicates that only TCP will be used at this QCE, that is, this entry will map frames based in many parameters including if it is a TCP protocol. When selected, the TCP Parameters will be displayed similarly to UDP, as described above.
- **Other:** indicates which IP protocol number will be used at this QCE, that is, this entry will map frames based in many parameters including if it is specified IP protocol. Values must be inserted in decimal format.
- **SIP:** indicates which filter should be applied based on the IPv4 source address at the frame. Possible configuration is as follows:
 - **Any:** indicates that all source IP address frames will be used at this QCE;
 - **Specific:** indicates that only specified IP address will be used at this QCE. Values of the IP address and mask allowed are dotted decimal notation;
- **IP Fragment:** indicates if IPv4 fragmented frames will be allowed in this QCE. Allowed values are Yes or No, where yes means accepts fragmented frames for this entry and no means no fragmented frames would be accepted in this frame;
- **DSCP:** indicates which DSCP values will be allowed in this QCE. Possible values are Any, Specific and Range. Possible configuration is as follows:
 - **Any:** indicates that all incoming frames will be used at this QCE;

- **Specific:** indicates that only specified DSCP levels will be used at this QCE. Values allowed are the DSCP range values (from 0 to 63);
 - **Range:** indicates that only a range of specified DSCP levels will be used at this QCE. Values allowed are the DSCP range values (from 0 to 63)
- **Action Parameters :** indicates all action parameters to be applied when frame matches with key parameters. If frames match with all key parameters configured, then frame will be treated as configured at the Action Parameters. Possible configuration are as follows:
 - **CoS:** indicates to which CoS queue incoming frame with key parameters should be redirected to. Allowed values are the CoS range values, from 0 to 7;
 - **DPL:** indicates to which DPL level incoming frame with key parameters should be redirected to. Allowed values are the DPL range values, from 0 to 3;
 - **DSCP:** indicates to which DSCP level incoming frame with key parameters should be redirected to. Allowed values are the DSCP range values, from 0 to 63;

12.13 Storm Policing

Storm Policing menu allows configuring storm prevention function. Storm prevention is a way to implement quality-of-service for a given LAN.

- **Port:** shows the ports to be configured at this row;
- **Unicast Frames:** indicates configuration to be applied when frames are from and to unicast hosts. Possible configuration is as follows:
 - **Enabled:** enable Unicast Frames policing function at the port. Checkbox selected means function enabled, and checkbox empty means disabled;
 - **Rate:** indicates rate to be applied on the storm policing function at that port. Traffic rates at the port higher than this field are not allowed if function is enabled. Allowed values are integer values and limits depend on the Unit used. Range of 100 to 1,000,000 is allowed when kbps or fps units are used. Range of 1 to 32,000 is allowed when Mbps or kfps units are used;
 - **Unit:** indicates which unit should be used with Rate value to limit traffic. Allowed values are kbps, Mbps, fps and kfps;

- **Broadcast Frames** : indicates configuration to be applied when frames are from and to broadcast hosts. Possible configuration is same as Unicast Frames.
- **Unknown Frames**: indicates configuration to be applied when frames are from and to unknown hosts, that is, flooded frames throughout the network. Possible configuration is same as Unicast Frames.

12.14 WRED

WRED (Weighted Random Early Detection Configuration) menu allows configuring storm prevention based on early detection algorithm function. This function applies only when Weighted QoS is performed, and this field allows configuring threshold for queues at weighted priority. Storm prevention is a way to implement quality-of-service for a given LAN. Possible configurations are as follows.

- **Queue**: shows the queues to be configured at this row;
- **Enabled**: enable WRED function at the queue. Checkbox selected means function enabled, and checkbox empty means disabled;
- **Min. Threshold**: indicates minimum average traffic to switch start dropping packets of queues 0 to 5 based on the weight configured in the QoS Egress Port Scheduler and Shapers menu. Values beyond this means no probability to drop packets. Values are in percentage, and allowed values are from 0 to 100. 0 means no traffic and 100 means all capacity traffic at a given port;
- **Max. DP1**: indicates drop probability of DPL 1 frames when traffic at the queue is 100 %. This field allows setting a probability for losing packets marked with Drop Precedence Level (DPL) 1. Values are in percentage, and allowed values are from 0 to 100. 0 means no traffic and 100 means all capacity traffic at a given queue;
- **Max. DP2**: indicates drop probability of DPL 2 frames when traffic at the queue is 100 %. This field allows setting a probability for losing packets marked with Drop Precedence Level (DPL) 2. Values are in percentage, and allowed values are from 0 to 100. 0 means no traffic and 100 means all capacity traffic at a given queue;
- **Max. DP3**: indicates drop probability of DPL 3 frames when traffic at the queue is 100 %. This field allows setting a probability for losing packets marked with Drop Precedence Level (DPL) 3. Values are in percentage, and allowed values are from 0 to 100. 0 means no traffic and 100 means all capacity traffic at a given queue.

Figure below shows Drop Probability versus Average Filling Level of the DPL levels curves.

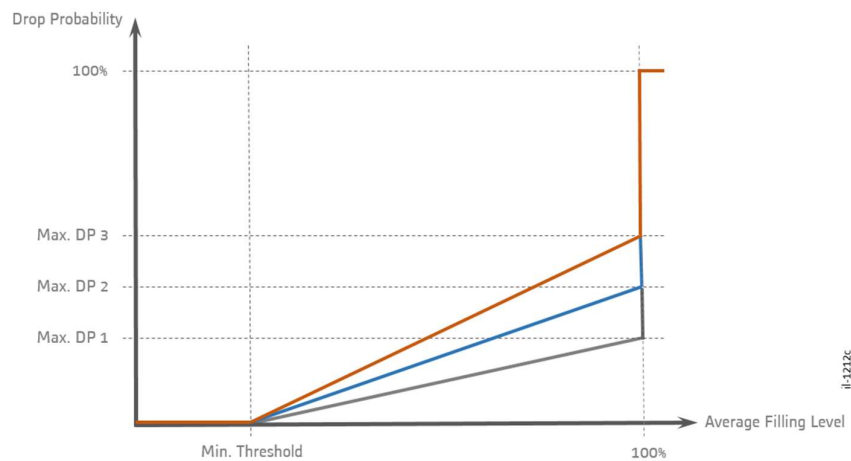


Figure 62: DPL level usage

13 Mirroring

13.1 Mirroring Basics

Port mirroring is a feature used as a monitoring strategy in packet switching networks. When enabled, port mirroring creates a copy of incoming and outgoing data from a specific port. The mirror port could be connected to a network analyzer, which would be useful for analysis and debugging data or network error diagnostics.

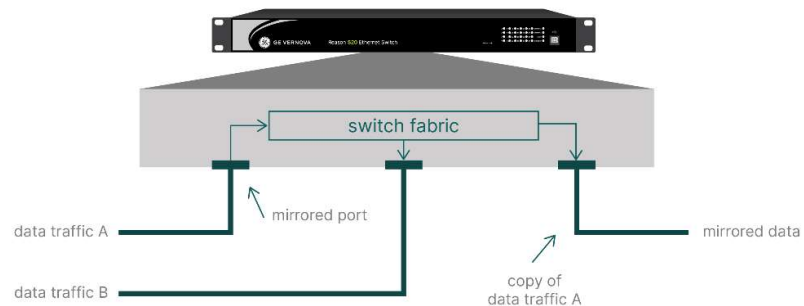


Figure 63: Port Mirroring Being Executed by a Switch

Reason S20 has port-mirroring function capabilities, which can be basically executed in two ways:

- Port mirroring in the same switch;
- Port mirroring in different switches.

Port mirroring in the same switch, as it says itself, is executed in just one switch that shall be configured to Mirror type. Mirrored port and port used to output mirrored data are in the same equipment.

In Mirror type mode of operation, Reason S20 can mirror all port traffic, just incoming data (Rx) or just outgoing data (Tx) from each port. Besides, it is possible to choose more than one port to be mirrored, with only one port outputting the traffic mirrored.



Figure 64: Port Mirroring in One Switch

Port mirroring in different switches is required when a port of one switch must be mirrored to a different switch. Common application of this mode is remote traffic monitoring, e. g., when it is desired to check traffic in a different room from where the Network traffic analyzer is installed. When using mirroring in different switches, all switches at a given LAN must be configured to mirroring. Using Reason S20, it would be necessary to configure switches in Source, Intermediate and Destination types, depending on the position of the switch at the traffic flow. Figure below shows an example of such application, showing the Source, Intermediate and Destination switches.

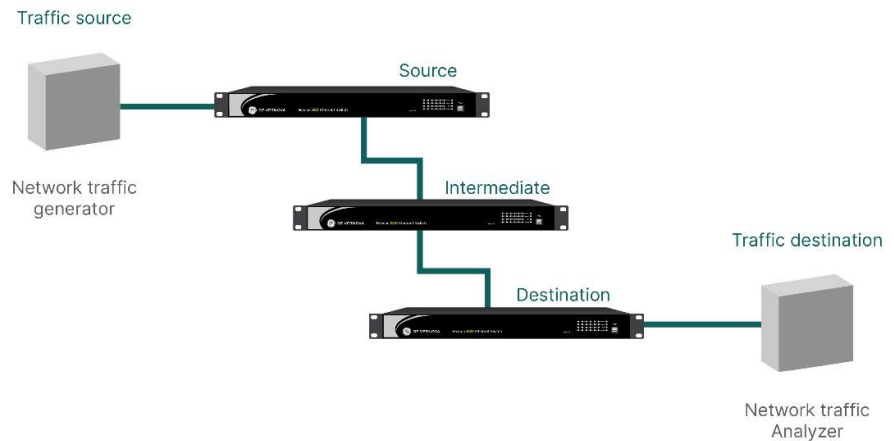


Figure 65: Port Mirroring in Many Switch

In Source type operation, the switch will be configured as the data collector of the data monitor flow. The port that is desired to monitor will be enabled to be mirrored and one fixed copper RJ45 port must be selected as a reflector port. The reflector port is idle and will not communicate, and it must be a fixed copper RJ45 port. Both optical or electrical SFPs will not work as reflector port. Lastly, either intermediate or destination ports can be configured on the Source to communicate with another switch or send the mirrored data to traffic destination, respectively.

In Intermediate type of operation, the switch will operate as a node in the data monitor flow network. It must be selected the ports that are in the monitor flow. In the example above, the intermediate ports should be the ports connected to the Source switch and the Destination switch.

In Destination type of operation, the switch will operate as the end node of the data monitor flow network. It must be selected the ports that are in the monitor flow and the port where the Network Traffic Analyzer is connected. It is possible to choose more than one port as destination, to allow the

connection of more than one Network Traffic Analyzer. Next figure shows how the ports must be configured when port mirroring in different switches.

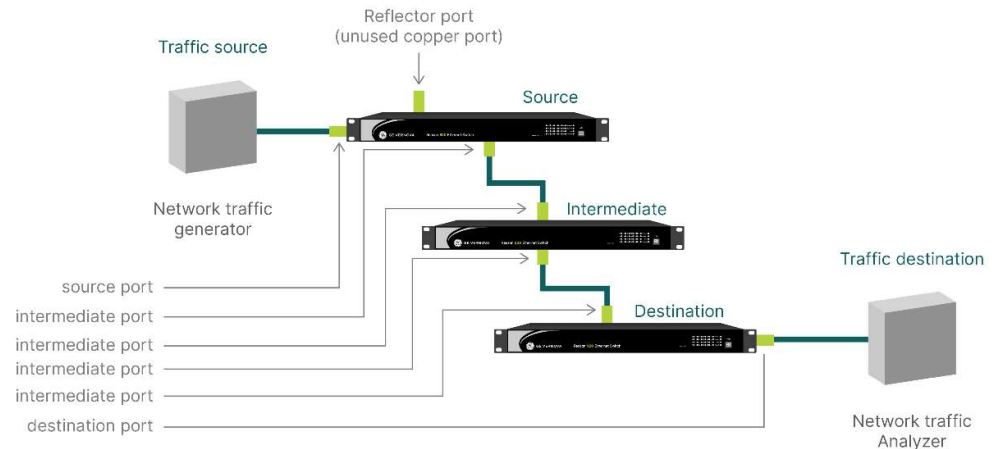


Figure 66: Data Monitor Flow Network

Mirroring menu is located at Settings > Mirroring

13.2 Mirroring Configuration

General Configuration

General settings display main configuration of mirror function. Possible configurations are as follows.

- **Mode:** enable Mirroring function. Enable will allow the function to be operating and Disable will shut down mirroring function;
- **Type:** indicates type operation of the switch. Allowed values are as follows:
 - **Mirror:** indicates that switch will operate in mirror mode, that is, source and destination port are at this switch;
 - **Source (RMirror) :** indicates that the switch will operate as source mode, that is, destination port is at another switch. Source and Intermediate ports are located at this switch;
 - **Intermediate (RMirror) :** indicates that the switch will operate as intermediate mode, that is, source and destination ports are at another switch. Only Intermediate ports are located at this switch;
 - **Destination (RMirror) :** indicates that the switch will operate as destination mode, that is, source ports are at another switch. Intermediate and Destination ports are located at this switch;
- **VLAN ID:** indicates to which VLAN mirroring function should mirror the traffic. This field specifies which VLAN traffic to be mirrored should be redirected, and is used by switches when remote mirroring is performed. This field is not allowed if Type of mirroring is Mirror type, that is, only remote mirroring function will redirect traffic to a specific VLAN. Allowed values are the VLAN range values (from 1 to 4,095);

- **Reflector Port:** indicates the main Source port of a remote mirroring function. Reflector port is the port, at the Source (RMirror) switch, that will receive traffic from all ports mirrored and forward it to Intermediate (RMirror) or Destination (RMirror) remote mirroring switch. Only Electrical ports (RJ45 and UTP cable connection) are allowed to be reflector ports, and only these ports are displayed at the list. Only one port can be a reflector port in a given switch.

Reflector ports must have its MAC Table Learning and Spanning Tree Protocols disabled. Only fixed copper RJ45 Ethernet ports can be configured as Reflector Ports.

Source VLAN(s) Configuration

Source VLAN configuration displays configuration of source VLAN to be used at mirror function. This field allows mapping a VLAN-based mirroring by inserting allowed VLAN identifiers at this field. Possible configurations are as follows.

- **Source VLANs :** indicates which VLAN mirroring function should mirror the traffic. This field allows configuring a VLAN-based mirroring, in addition to port mirror. It is possible to monitor specific VLAN and ports from different VLAN independently. Allowed values are the VLAN range values (from 1 to 4,095);

Port Configuration

Port configuration displays configuration allowed per port to execute mirror function. This field allows defining source, intermediate and destination ports and defining if all traffic, only TX or only RX traffic should be mirrored. Possible configurations are as follows.

- **Port:** shows ports to be configured at this row;
- **Source:** indicates if port is a source port and what kind of traffic is being mirrored. This field is only allowed if switch is operating in Mirror or Source (RMirror) types. Possible values are as follows:
 - **Disabled:** indicates that port is not being mirrored, that is, port is operating normally and no traffic mirroring from this port is being performed;
 - **Both:** indicates that port is being mirrored and all traffic (received and transmitted frames) are being mirrored;
 - **Rx Only:** indicates that port is being mirrored and Rx traffic (received frames) are being mirrored;
 - **Tx Only:** indicates that port is being mirrored and Tx traffic (transmitted frames) are being mirrored;
- **Intermediate:** enable the port to operate as Intermediate port. Intermediate ports are ports that connect switches performing remote mirroring. Checkbox selected means that port will operate as intermediate port, that is, source traffic of this port will be a Reflector port or another Intermediate port. Checkbox empty means port will not operate as intermediate port, that is, port will

operate normally with no mirroring (if also destination is disabled) or port will operate as destination port;

Intermediate ports must have its MAC Table Learning disabled.

- **Destination:** enable the port to operate as Destination port. Destination ports are ports that connect the Destination (RMirror) switch performing remote mirroring to the end station, that is, the traffic analyzer. Checkbox selected means that port will operate as destination port, that is, source traffic of this port will be a Reflector port or another Intermediate port. Checkbox empty means port will not operate as destination port, that is, port will operate normally with no mirroring (if also intermediate is disabled) or port will operate as intermediate port;

Destination ports must have its MAC Table Learning disabled.

14 Precision Time Protocol (PTP) - IEEE 1588v2

The IEEE1588v2 protocol can be enabled by licensing in S20. Precision Time Protocol (PTP) is defined in the IEEE 1588 standard, which describe the precision clock synchronization protocol for networked measurement and control systems. In S20, the IEEE 1588v2 protocol may also be used to synchronize the internal system time.

Note the version IEEE1588v2 is not back compatible with version 1.

14.1 Precision Time Protocol (PTP) Functional

Precision Time Protocol (PTP) uses the Ethernet frames to transport synchronism messages, to do time synchronization of several IED connected to the network. The protocol itself allows to be used layer 2 (Multicast transport mechanism) or layer 3 (UDP transport mechanism) messages, which the chosen one will remain on the application requirements.

Although PTP protocol allows to use both Ethernet (multicast) or IP (UDP transport mechanism), IEC 61850-90-4 Technical Report adverts that only layer 2 communication has accuracy for power system applications, such as synchronization of IED equipment. Based on that, it is recommended Layer 2 communication for power system applications.

The messages are transmitted in a master-slave method. Different from NTP protocol, where the slave sends a request to the master to receive time data, in a PTP network the master multicasts its synchronization messages throughout the network, and slaves receive the messages cyclically, while the master remains sending it to the network.

There are several elements in the PTP network. The main elements in a PTP-aware environment are:

- Grand Master Clock (GMC): This clock is the top-level master at the network, usually a GPS-based clock;
- Master Clock (MC): A master clock at a given subdomains, which can be the GMC clock or the boundary clock;
- Ordinary Clock (OC): A clock in the PTP network, which can be either master or a slave clock.
- Transparent Clock (TC): A clock that forwards Sync messages with value of the forwarding process delay included at the message;
- Boundary Clock (BC): A clock that has a slave port synchronized by a master clock and a master port which synchronizes a time sub-domain;

The PTP operation over the network is as shown below.

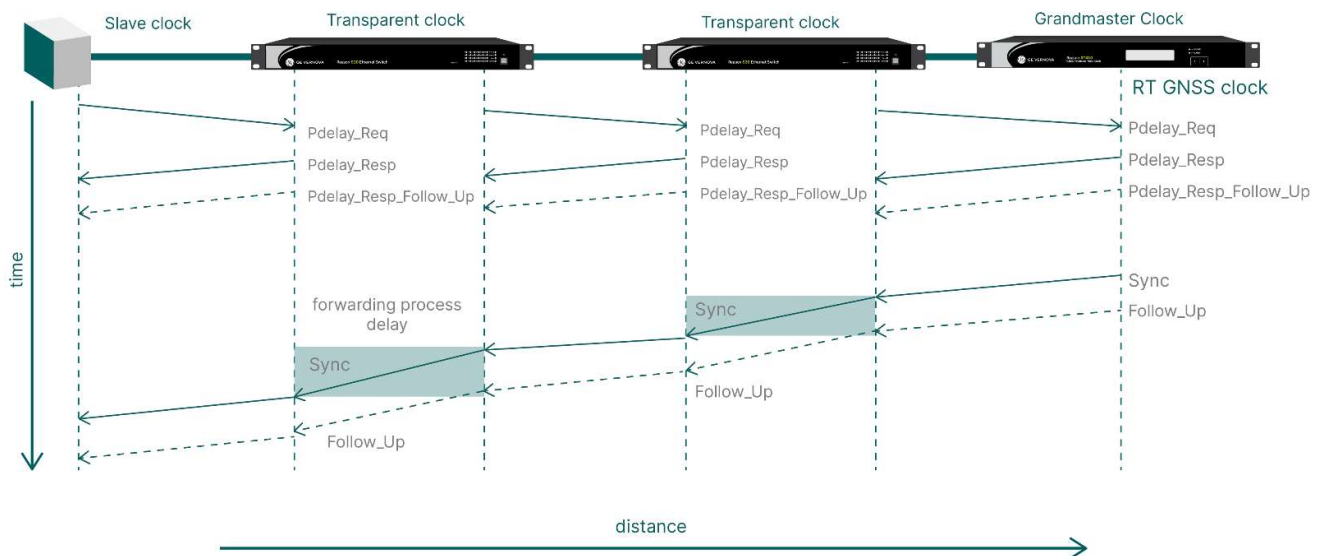


Figure 67: PTP protocol mechanism

At a cyclic period, the GMC sends sync messages throughout the network in a multicast mechanism. Typical cyclic is 1 second, meaning each second the network will receive a sync message from the GMC.

Each path will exchange information to calculate the path delay time. Thus, at each transparent clock there will be a time which will be considered before sending the message to the slave, minimizing the error from the GMC to the slave clock. At the end, all path delay and forwarding process delay at the TC will be corrected, and then the slave clock will receive the timestamp that the GMC clock has sent.

In two-step mode, the TC will store the time stamp of the received Sync frame and will forward it without correction. After the Sync message, the TC will do a sum with the correction of the Sync message ingress, its own forwarding delay and the path delay previously calculated and then send a Follow-up message with the correction that should be made by other clocks in the network.

If there is more than one master in the network, the master-capable equipment will do an election to determine which clock has the best accuracy at the network, based on an Announce message. Thus, PTP network with more than one master will have a failover mechanism directly at the protocol, to allow reliability in the network synchronization. A peer-to-peer (P2P) delay mechanism calculates the path delay and forwarding process delay of each component in the network. PTP also allows to be used in an end-to-end (E2E) delay mechanism, which is like the mechanism used in NTP protocols. In this mechanism, it will be considered all delay between master and slave as one value, the “path delay” value.

Reason S20 can operate either in P2P or E2E modes. For power system applications, the IEC 61850-90-4 Technical Report says E2E mechanism does not have the accuracy desired. Thus, it is recommended to use P2P delay mechanism.

14.2 PTP in GE Reason S20

When enabled, there are four modes of operation when using Reason S20 in PTP networks:

- Transparent Clock (TC);
- Boundary Clock (BC);
- Master only;
- Slave only.

By default, the PTP is disabled in Reason S20.

When operating on a PTP IEEE1588v2 network, it is possible to define one by one which ports will be enabled and what is the asymmetry delay from each of them.

PTP menu is located at Settings > PTP.

General Settings

- **Mode:** to define the Ethernet switch PTP operation mode.
 - **Transparent Clock:** according to IEEE1588v2, a transparent clock has multiple PTP ports and measures the time a PTP event message takes to transit network path and provides this information to the ordinary clocks (slaves) receiving this PTP event message so they can compensate each path delay;
 - **Boundary Clock:** according to IEEE1588v2, a boundary clock has multiple PTP ports (one operating as slave and others as master) in a domain number and maintains the timescale used in the domain. With the PTP slave port synchronized to the PTP grandmaster clock, it serves as a master clock to the slaves IEDs using the remaining ports;
 - **Master only:** According to IEEE1588v2, it is the time source which all other clocks on that path will synchronize. S20 uses its internal time to synchronize ordinary (slave) clocks. Different from Boundary clock, the Master only option does not have a

slave port to synchronize the switch to another grandmaster clock.

- **Slave only:** defined as ordinary clock by IEEE1588v2, this mode is used to only synchronize the S20 internal clock based on a PTP Grandmaster clock. Note this can also be achieved in the other three modes by enabling the adjust system time option.
- **Profile:**
 - **Custom:** all PTP parameters are freely configurable;
 - **Power Utility – IEC/IECC 61850-9-3/2016:** PTP parameters pre-defined in accordance with PTP Power Utility Profile – IEC61850-9-3.
 - **Power Profile – IEEE C37.238/2017:** PTP parameters pre-defined in accordance with PTP Power Profile – IEEE C37.238:2017.
- **Domain Number:** the domain number is the PTP network identifier, so the Reason S20 will only interact with PTP messages from this domain. The range is from 0 to 255.
- **Network Protocol:** Transport protocol used by the PTP protocol engine.
 - **Ethernet:** PTP over Ethernet (Layer 2), multicast;
 - **IPv4 Multicast:** PTP over IPv4/UDP (Layer 3) multicast;
 - **IPv4 Mixed:** PTP using a combination of IPv4/UDP (Layer 3) multicast and unicast;
 - **IPv4 Unicast:** PTP using IPv4/UDP (Layer 3) unicast. IPv4 unicast is only possible when operating as Master only or Slave only mode.

When operating in IPv4 Unicast mode, the Reason S20 can have up to 5 master IP addresses configured. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.
- **VLAN:** Enable/disable VLAN tagging for PTP frames.
 - **VLAN ID:** VLAN Identifier used for tagging the PTP frames.
 - **VLAN Priority:** Priority Code Point (PCP) value used for VLAN PTP frames.
- **Operation Mode:** PTP Operation Mode, only Two-Step mode is supported by Reason S20. In the Two-Step mode, the sync information is sent in one data packet, and timestamp information is sent in another data packet right after.
- **Delay Mechanism:** mechanism used to compensate networking delays.
 - **End-to-End:** measurement of delay across the network between master clock and slave clock;
 - **Peer-to-Peer:** delay measurement is done hop by hop, performed by all PTP-aware devices, including switches when operating as transparent or boundary clock.

- **Priority #1 and #2:** When configured as master, BMC algorithm tie breaking criteria priorities must be attributed. The priority values can vary from 0 to 255, the lower the attributed value is, the higher its priority is. Priority #1 is used to specifically design one priority clock rather than others – this is the first tie breaking condition. Priority #2 is the last PTP tie breaking criteria, coming after clock class, accuracy and variance. After priority #2, the MAC address is used as last tie breaking resource.
- **Sync Interval:** to choose the frequency of sending Sync messages. Range is between 16 messages per second and one message every-32-seconds.
- **Delay Request Interval:** to choose the frequency of sending Delay Request messages. Range is between 16 messages per second and one message every-32-seconds.
- **Announce Interval:** to choose the frequency of sending Announce messages when operating in master mode or boundary clock. Range is between 16 messages per second and one message every-32-seconds.
- **Announce Timeout:** the waiting time of Announce message receipt. In case an Announce message is not received within this time interval, Reason S20 assumes that the current master clock is unavailable and executes the BMC to select another master clock. Range is between 2 and 255 seconds.

System Time Settings

- **Adjust System Time:** Chooses whether PTP will adjust the internal system time or not. This setting will be disabled, even if previously enabled, whenever NTP client mode is enabled.

Port Configuration

To choose which ports will be enabled and operating in the PTP instance as the general settings configured. It is also possible to configure the cable delay asymmetry from each switch port. The configuration is in nanoseconds using the following formula: *delay asymmetry = delay RX - delay TX*.

15 Routing Information Protocol (RIP)

15.1 RIP Basics

RIP is a distance vector routing protocol widely used in IP networks, mostly small to medium size. In other words, a router running RIP send its reachability information to all adjacent routers, which is then saved in the routing table of each router. Periodically, all routers exchange its router table information with one another, so that every router knows the lowest distance (hop count) to reach the destination. The hop count supports up to 15 hops, and as the hop 16 is considered unreachable.

There are two versions of RIP:

- **RIPv1:** Defined by RFC 1058, RIPv1 is a classful routing protocol meaning all devices on the same routing domain must use the same subnet mask. Furthermore, RIPv1 does not support authentication and it uses broadcast to update the routing table.
- **RIPv2:** Defined by RFC 2453, RIPv2 is a classless routing protocol allowing the use of variable length subnet masks, as the subnet masks is included with routing updates. RIPv2 supports authentication (clear text, MD5) and it uses multicast to update the routing table. All the Routers running RIPv2 must have the same Date/Time settings for RIPv2 key chain authentication to work properly, this can be done by using the Network Time Protocol (NTP).

15.2 RIP Configuration

RIP is only available if the Layer 3 licensing is enabled in S20.

Configuration is located at Settings > RIP.

General Configuration

- **Mode:** controls whether RIP functionality is enabled or disabled;
- **Version:** chooses the protocol version, either RIP version 1 or 2;
- **Update timer:** Interval in seconds between routing table advertisements. Default value is 30 seconds, allowed range is from 5 to 65,535 seconds.
- **Timeout timer:** Interval in seconds to invalidate a router that is no longer sending updates. Default value is 180 seconds, allowed range is from 5 to 65535 seconds.
- **Garbage timer:** Interval in seconds to remove a router without updates from the routing table. Default value is 240 seconds, allowed range is from 5 to 65,535 seconds.

VLANs

RIP can be enabled individually on each VLAN. All ports in a given VLAN will transmit RIP protocol and will process the routing information from other routers with RIP enabled. If a RIP packet is sent to a port which VLAN is disabled, the RIP packet is ignored.

Note only VLANs with configured IP address (Settings > System > IP) are shown on this configuration.

- **VLAN:** VLAN number, from 1 to 4,095;
- **Enable:** select to enable RIP on the VLAN correspondent;
- **Authentication mode:** Only available on RIPv2. Selects the authentication method to transmit the RIP protocol in the VLAN. Allowed values are: none, text or MD5.
- **Keychain:** Only available on RIPv2. A keychain can carry one or multiple passwords that validates the RIP protocol. Each VLAN will have a keychain associated.

Neighbors

Neighbors are trusted gateways for receiving RIP protocol. If none neighbor is configured, all received packets will be accepted. If one or multiple neighbors are specified, RIP packets from the configured neighbors will be accepted and packets from other sources will be ignored.

- **Add Neighbor:** Enter the IP address from the neighbor router, and click save. Press delete and save to remove a configured neighbor.

Keychains

As previously mentioned, keychains are used to store one or multiple keys to validate the exchange of RIP information in network. Keychains are associated to VLANs. A single key will be valid at time, which will be included on all RIP responses sent, and checked on all RIP responses received. Passwords are only supported by RIP version 2 and are ignored in version 1.

- **Add Keychain:** Enter the keychain name, from 1 to 32 characters, and press Add Keychain to enter the next parameters.
- **Delete:** Press to delete the created keychain.
- **ID:** The key ID. It must be unique but is ignored for clear text password. Allowed values are in the range 0 through 255.
- **String:** The key string. The string can contain from 1 to 16 uppercase and lowercase alphanumeric character, and the first character cannot be a number.
- **Start/End time:** Optionally, enter the period (start/end time) the key will be valid. If only the start time is set, the key will never expire. The time format is "hh:mm yyyy/mm/dd".

In case of multiple keys, if a period overlap occurs the key with farthest end time or lower ID will prevail on outgoing packets. If all keys have expired, the one that expired most recently or with the lower ID will be used. If no key is valid yet, none is sent. Incoming packets are accepted if they carry the valid key, a key that will be valid within the next 24 hours, or that was valid within the preceding 24 hours.

15.3 Command Line Interface (CLI)

General configuration

Command	Description	Unit	Default	routed parameter
<code>router rip</code>	Enable RIP.			
<code>rip version <1 2></code>	Select protocol version.		2	ripv2
<code>rip timer update <5-65535></code>	Set interval between routing table advertisements.	s	30	

Command	Description	Unit	Default	routed parameter
<code>rip timer timeout <5-65535></code>	Set interval necessary without updates to invalidate a route.	s	180	
<code>rip timer garbage <5-65535></code>	Set interval necessary without updates to remove a route from the routing table.	s	240	
<code>rip neighbor <ip></code>	Add a neighboring router with which to exchange routing information. Maximum of 64 neighbors.			<code>trust_gateway</code>

Keychain configuration

Command	Description	routed parameter
<code>rip keychain <word32> key <uint8> key-string <kword80> [start <hhmm> <date> [{ end <hhmm> <date> }] { duration <uint> }]]</code>	Add key to a keychain.	<code>passwd</code>
<code>keychain <word32></code>	Keychain name. Maximum of 4 keychains.	
<code>key <0-255></code>	Set key id. Maximum of 8 keys for every keychains.	
<code>key-string <kword16></code>	Set key string. The string can contain from 1 to 16 uppercase and lowercase alphanumeric characters, but the first character cannot be a number.	
<code>start <hhmm> <date> [end <hhmm> <date>] { duration <uint> }]</code>	Specify the period from which the key can be used. The earliest acceptable date as January 1, 1993.	

Interface configuration

Command	Description	routed parameter
<code>interface vlan <vlan_list></code>		
<code>rip</code>	Enable RIP on interface.	
<code>no rip</code>	Disable RIP on interface.	<code>no_rip</code>
<code>rip authentication mode {text md5}</code>	Set authentication method for RIPv2	<code>passwd, md5_passwd</code>
<code>rip authentication keychain {key}</code>	Associate a key chain for RIP authentication on the interface	<code>passwd, md5_passwd</code>

Status commands

Command	Description
<code>show router rip keychain</code>	Display key chains.

Command	Description
<code>show router rip neighbor</code>	Display neighbors.

16 Open Shortest Path First (OSPF)

16.1 OSPF Basics

OSPF is a routing protocol for IP networks usually applied from medium to large networks. It uses a link state routing protocol within the Interior Gateway Protocol (IGP) in order to distribute IP routing information throughout a single Autonomous System, (AS) in an IP network. The OSPF version 2 is used for IPv4 as defined by RFC 2328.

Using the Shortest Path First Algorithm, OSPF builds and calculates the shortest path to all known destinations. The link state updates from each OSPF router is sent to the network, and every router keeps a copy from the link state of other routers. Using such information, the shortest path is calculated to all destinations.

For large networks, it is possible to create OSPF areas as boundaries to avoid networking flooding of link state exchanges. When area is used, the switches within an area are called as internal router and they have the same link state database, the switches in the border are called as area border routers (ABRs) and they work as a backbone describing the link state from each area.

Compared to RIP, a few advantages of OSPF are: there are no limits on hop count, the concept of areas to large networks and faster convergence.

16.2 OSPF Configuration

OSPF is only available if the Layer 3 licensing is enabled in S20.

Configuration is located at Settings > OSPF.

General Configuration

- **Mode:** controls whether OSPF functionality is enabled or disabled;
- **Router ID:** defines the router ID from this device in a OSPF network;
- **SPF delay:** interval in seconds between receiving a link state database update and starting the Shortest Path First (SPF) calculation. Default value is 1 second, allowed range is from 1 to 10 seconds;
- **SPF holdtime:** Interval in seconds between consecutive SPF calculations. Default value is 5 seconds, allowed range is from 1 to 5 seconds.

Areas

Areas are logical collections of OSPF networks, routers (or L3 switches), and interfaces with the same area identification. They limit the scope of route information distribution. If multiple areas are being used, you need to

add the backbone area (0.0.0.0) for correct protocol operation. Moreover, areas allow protection against unauthorized access to the identified area using an authentication key. Only areas with configured authentication mode are shown on this configuration.

- **Delete:** Select to delete a previous created area;
- **ID:** Area identification in the format [0-255].[0-255].[0-255].[0-255] ;
- **Authentication Mode:** Select the authentication method for each area. Select text to use a plain text as authentication or md5 to use MD5 hash.

Interfaces

Configure the interfaces (associated to VLANs) available for OSPF routing. Note only VLANs with configured IP address (Settings > System > IP) are shown on this configuration.

- **VLAN:** display the VLANs ID available to use OSPF;
- **Enable:** check to enable OSPF on the given VLAN;
- **Area ID:** Enter the OSPF area ID in which the interface should be routing;
- **Cost:** Interface cost to route data. Default value is 10, allowed range is from 1 to 65,535. The greater the cost, less likely the interface will be used in the router path;
- **Priority:** Router priority. If set to 0 the router is not eligible as a designated router or backup designated router. The greater the priority, more likely the interface will be designated in the router path.
- **Retransmit Interval(s):** Interval in seconds between link state advertisement transmissions. Default value is 5 seconds, allowed range is from 5 to 3,600 seconds.
- **Transmit delay (s):** Interval in seconds to wait before sending a link state update packet. Default value is 1 second, allowed range is from 1 to 3,600 seconds.
- **Hello interval (s):** Interval in seconds between hello packets sent between interfaces with OSPF enabled. The value must be the same for all nodes on a network. Default value is 10 seconds, allowed range is from 1 to 65,535 seconds.
- **Dead interval (s):** Neighbor inactivity timer. When a neighbor has been inactive for a period equal or greater than the dead interval, the interface state is set to down. Neighbors that have been inactive for more than 24 hours are completely removed. Default value is 40 seconds, allowed range is from 2 to 2,147,483,647 seconds.

Depending on the Authentication Mode chosen in the area, either a plain text authentication key or a MD5 message digest key must be entered.

- **Authentication key:** Set up to 8 characters for plain text authentication.
- **Message digest key:** Message key used for MD5 authentication, with up to 16 characters.
- **Key ID:** Authentication key ID used for MD5 authentication, thus it must be used only when Message digest key is also configured. Default value is 0, allowed range is from 0 to 255.

16.3 Command Line Interface (CLI)

General configuration

Command	Description	Unit	Default	ospfd parameter
<code>router ospf</code>	Enable OSPF			
<code>ospf router-id <ipv4_addr></code>	Set the router ID. If not specified, the numerically lowest IP address of the router will be used			<code>router-id</code>
<code>ospf timer spf-delay <1-10></code>	Set delay between receiving a change to SPF calculation	s	1	<code>spf-delay</code>
<code>ospf timer spf-holdtime <1-5></code>	Set delay between first and second SPF calculation	s	5	<code>spf-holdtime</code>

Interface configuration

Command	Description	Default	ospfd parameter
<code>interface vlan <vlan_list></code>			
<code>ospf</code>	Enable OSPF on interface		
<code>no ospf</code>	Disable OSPF on interface		
<code>ospf area <ipv4_addr></code>	Set the area on which the interface runs		<code>area</code>
<code>ospf cost <1-65535></code>	Set the cost of sending a packet on the interface	10	<code>metric</code>
<code>ospf retransmit-interval <5-3600></code>	Set the number of seconds between link state advertisement transmissions	5	<code>retransmit-interval</code>
<code>ospf transmit-delay <1-3600></code>	Set the number of seconds to wait before sending a link state update packet	1	<code>transmit-delay</code>
<code>ospf priority <0-255></code>	Set the router priority. If set to 0 the router is not eligible as a Designated Router or Backup Designated Router	1	<code>router-priority</code>

<code>ospf hello-interval <1-65535></code>	Set the number of seconds between hello packets sent on an OSPF interface. The value must be the same for all nodes on a network	10	hello-interval
<code>ospf dead-interval <2-2147483647></code>	Set the router dead time (neighbor inactivity timer). When a neighbor has been inactive for router-dead-time its state is set to DOWN. Neighbors that have been inactive for more than 24 hours are completely removed.	40	router-dead-time
<code>ospf authentication-key <string8></code>	Set the authentication key for plain text authentication		auth-key
<code>ospf message-digest-key <0-255> md5 <string16></code>	Set the authentication key and its id for MD5 authentication		auth-md

Area configuration

Command	Description	ospfd parameter
<code>ospf area <ipv4_addr> authentication [message-digest]</code>	Allow protection against unauthorized access to the identified area using authentication key	auth-type

17 Virtual Router Redundancy Protocol (VRRP)

17.1 VRRP Basics

The use of statically configured default router is popular in many networks when IP addresses from terminals are fixed and well known, as it minimizes the routing processing time. However, static routing creates a single point of failure, and if the default router becomes unavailable, the devices that use it as their first-hop router become isolated from the network.

Defined by RFC 2338, VRRP is designed to eliminate the single point of failure inherent in the static default routed environment. The protocol achieves this by creation of multiple virtual routers, in which one is the master and the remaining are backup routers. If the master router fails, one of the backup routers becomes the new master router, providing a virtual default routing platform and enabling traffic on the LAN to be routed without relying on a single default router.

The advantage gained from using VRRP is a higher availability without requiring configuration of dynamic routing or router discovery protocols on every end-host.

17.2 VRRP Configuration

VRRP is only available if the Layer 3 licensing is enabled in S20. Furthermore, only VLANs with configured IP address may take part in a VRRP group, and each VLAN may only have a single and exclusive Virtual IP address. Thus, VRRP load sharing is not available in S20. The priority value will define which router is the master and which are the backups in a VRRP network.

Configuration is located at Settings > VRRP.

General Configuration

- **Mode:** controls whether VRRP functionality is enabled or disabled;

Interfaces

Configure the interfaces (associated to VLANs) available for VRRP routing. Note only VLANs with configured IP address (Settings > System > IP) are shown on this configuration.

- **VLAN:** display the VLANs ID available to use VRRP;
- **Enable:** check to enable VRRP on the given VLAN;
- **Virtual Router ID:** VRRP group identifier, shall be exclusive for each VLAN. Allowed values are in the range from 0 to 255;
- **Virtual IP Address:** virtual IP Address for a specified VRRP group. This address should be in the same subnet as the IPv4 address of the interface;
- **Mask Length:** the netmask in CIDR format. Allowed values are in the range 1 through 32, default being 24;
- **Priority:** priority level of the router within a VRRP group. Each router in the Virtual Router Group has a specific priority, which is a number between 1 and 255. The router with the highest priority (or highest number) is elected the Master, while all other routers are considered Backups. The default value is 100;
- **Preemption Mode:** when preemption mode is enabled, a master router will become backup if another router arrives with a higher priority;
- **Authentication Password:** password for text authentication. Up to 8 characters can be specified;
- **Advertisement Interval (s):** Interval in seconds between sending advertisement packets. The VRRP master sends VRRP advertisements to other VRRP routers in the same group. Allowed values are in the range 1 through 255, default being 1.

17.3 Command Line Interface (CLI)

General configuration

Command	Description
<code>router vrrp</code>	Enable VRRP

Command	Description
no router vrrp	Disable VRRP

Interface configuration

Command	Description	Default	vrrpd parameter
interface vlan <vlan_list>	List all interface VLANs available		
vrrp	Enable VRRP on interface		
no vrrp	Disable VRRP on interface		
vrrp <0-255>	Set the group identifier (Virtual Router Identifier).		server id
vrrp address <ipv4_addr> <1-32>	Set the virtual IP address and mask length for the specified VRRP group. This address should be in the same subnet as the IPv4 address of the interface. The netmask should be in the CIDR format and its default. value is 24.		addr
vrrp priority <1-255>	Sets the priority level of the router within a VRRP group (router-id).	100	priority
vrrp authentication <string8>	Set the password for plain text authentication. The text password is up to eight alphanumeric characters.		password
vrrp preempt	Enable VRRP preemption.	enabled	preempt_mode
vrrp advertisement-interval <1-255>	Sets the interval time in seconds between sending advertisement frames.	1	

18 Failsafe Alarm

Reason S20 has a list of failsafe alarm functionalities which can be recorded as an event of syslog and/or locally operate the front Led “Failsafe” and the rear relay contact. The failsafe alarm functionalities are disabled by default and the setting menu is located at Advanced Settings > Failsafe Alarm.

Failsafe alarms start operating 60 seconds after equipment booting.

Led/Alarm Operation Examples

As an example of how the failsafe alarms operate, consider the power supply failure alarm. The led/alarm will immediately go to active once the failure happens and depending on the configuration, it may remain active or

return to desactive once the power supply returns to normal operation, as examples below.

Example 1: In case the persist option is disabled, and if the failure condition lasts longer than the minimum active time, the led/alarm will remain active as long as the failure lasts.

1. Persist Disabled, Alarm condition > minimum active time
 $t = 3s$

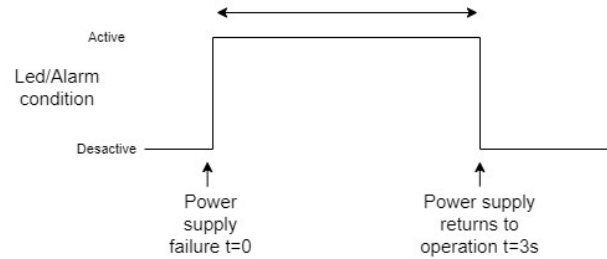


Figure 68: Led/Alarm operation example 1

Example 2: In case the persist option is disabled, and the failure lasts shorter than the minimum active time, the led/alarm will remain active as the duration configured in the minimum active time.

2. Persist Disabled, Alarm condition < minimum active time

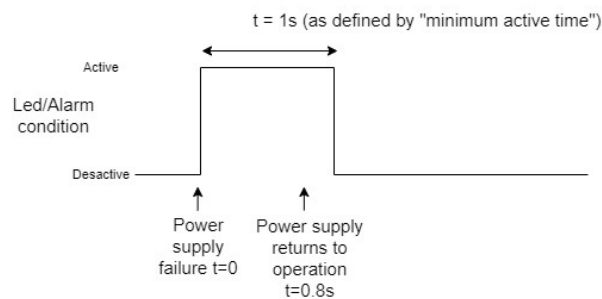


Figure 69: Led/Alarm operation example 2

Example 3: In case the persist option is enabled, the led/alarm will remain active until the user clicks on the “clear trigger” (located at Monitor > Failsafe Alarm) regardless the power supply returning to normal operation or the minimum active time configuration.

3. Persist Enabled

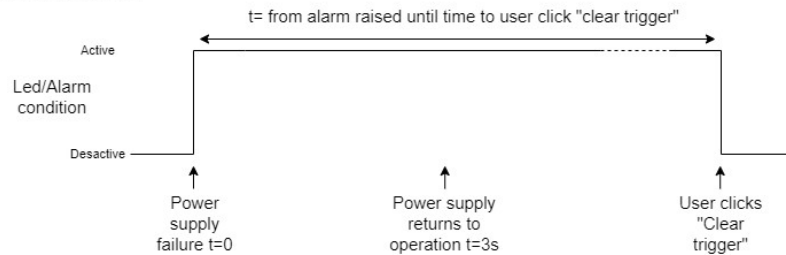


Figure 70: Led/Alarm operation example 3

Configuration options

- *Led & Relay minimum active time (sec)*: Minimal time in seconds that the led and the relay will remain active after an alarm has been activated.
- *Alarm Name: List of events which may be recorded in syslog and/or operate the failsafe Led/Alarm to locally signalize the event:*
 - **Inconsistent Speed or dp_x** : alarm if any operating port is configured with an inconsistent speed or dp_x (half/full duplex);
 - **Invalid configuration** : to alarm when an invalid configuration is uploaded (in Menu Maintenance > Configuration > Upload);
 - **Link change**: up or down: to alarm if any port link is changed from up to down or down to up. This is useful to identify if any port connection is lost or if any non-expected device is connected to the switch;
 - **MAC address authorization failed**: This alarm goes off when the MAC table is full, that is it learned all the possible entries, not only statically but also dynamically;
 - **Port security violated**: If the port has the Limit Control activated and the limit exceeds the configured value, this alarm goes off. To configure Port Security Limit Control, go to Menu Advanced Settings > Security > Network > Limit Control;
 - **Power Supply Failure**: to alarm if either the main or the redundant power supply fails. If the Reason S20 has only one power supply, this option must be disabled otherwise the failsafe will signalize a power supply failure as the redundant power supply is not there;
 - **Received looped-back BPDU**: to alarm if a loop is identified in the network architecture, as described in loop protection section;
 - **CPU temperature out of range**: This alarm goes off whenever the CPU temperature goes out of the set values. The values are set in Celsius degrees.
 - **CPU load out of range**: This alarm goes off whenever the CPU load goes above the set value. The value is set in percentage.
 - **RAM use above the limit**: This alarm goes off whenever the use of RAM goes above the set value. The value is set in percentage.
 - **Module X removal**: to alarm if the specified module X was removed or failed communicating with main board. Module 1 consist of ports from 1 to 4, module 2 of ports from 5 to 8, and so on;
Note: X represents a valid number of modules, up to 5 for model S2020 and up to 6 for model S2024.
 - **Port X removal**: to alarm if the SFP transceiver from a specified port X was removed (this option does not apply to RJ45 fixed Ethernet ports).
 - **Port X link up**: to alarm if the Ethernet communication link state of a specific port changes from down to up.

- *Port X link down: to alarm if the Ethernet communication link state of a specific port changes from up to down.*
Note: X is a number of valid ports on the switch, up to 20 for model S2020 and up to 24 for model S2024.
- *SFP Temperature: to alarm in case any optical SFP reaches the low/high SFP temperature threshold (please refer to Monitor > DDMI to check the SFP threshold levels).*
- *SFP Voltage: to alarm in case any optical SFP reaches the low/high SFP voltage threshold (please refer to Monitor > DDMI to check the SFP threshold levels).*
- *SFP Bias: to alarm in case any optical SFP reaches the low/high SFP Bias threshold (please refer to Monitor > DDMI to check the SFP threshold levels).*
- *SFP Tx Power: to alarm in case any optical SFP reaches the low/high SFP Tx Power threshold (please refer to Monitor > DDMI to check the SFP threshold levels).*
- *SFP Rx Power: to alarm in case any optical SFP reaches the low/high SFP Rx Power threshold (please refer to Monitor > DDMI to check the SFP threshold levels).*
- *Enabled: check to enable the respectively functionality;*
- *Syslog: check to record the event in the syslog;*
- *Level: to choose the syslog level the event should be recorded. It can be either: error (severity 3), warning (severity 4), notice (severity 5) or info (severity 6);*
- *Led/Relay: check to enable the locally alarm using the front "Failsafe" led and the back dry contact relay;*
- *Persist: The alarms marked with Persist will keep the Led/Relay state activated until the user's manual action, when pressing the Clear Triggered button (located at Monitor > Failsafe Alarm). Disabled by default.*
- *Lower Threshold: if applicable, lower threshold defines the lowest amount below which triggers the specific alarm. Acceptable values: depends on alarm.*
- *Upper Threshold: if applicable, upper threshold defines the highest amount above which triggers the specific alarm. Acceptable values: depends on alarm.*

19 DDM Interface (DDMI)

DDMI provides an enhanced digital diagnostic monitoring interface for optical SFP transceivers which allows real time access to device operating parameters. To enable/disable DDMI operation, the setting menu is located at Advanced Settings > DDMI.

Once DDMI operation is enable the user may refer to Monitor > DDMI to monitor the diagnostic of SFP transceivers. By clicking in an optical SFP, SFP information is shown, including the current temperature, voltage, Bias and RX/TX Power as well as the threshold that may raise an alarm. The

monitoring is also available through SNMP Traps (Settings > Security > Switch > SNMP > Trap).

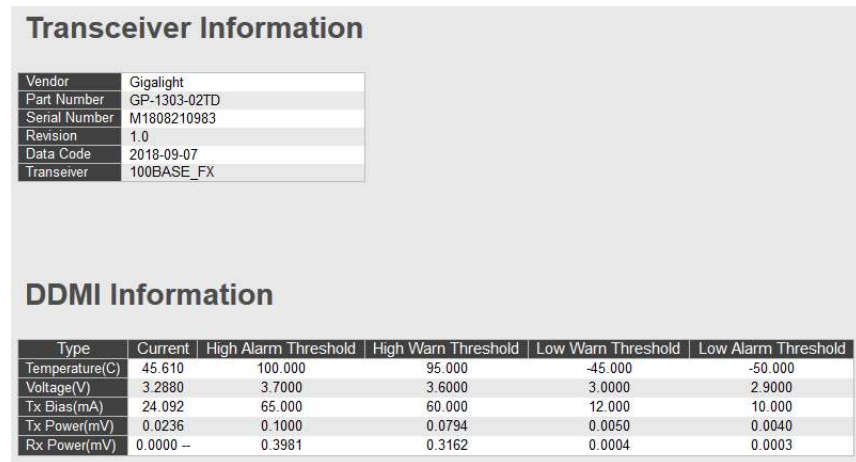


Figure 71: SFP DDM monitoring

Alarms using the dry-contact relay may be configured (Advanced Settings > Failsafe Alarm) to act in case any SFP reach the high or low Alarm threshold. The SFP alarm threshold is set by the SFP manufacturer and cannot be configured.

20 Application Examples

20.1 Configuring VLANs in a Digital Substation Network

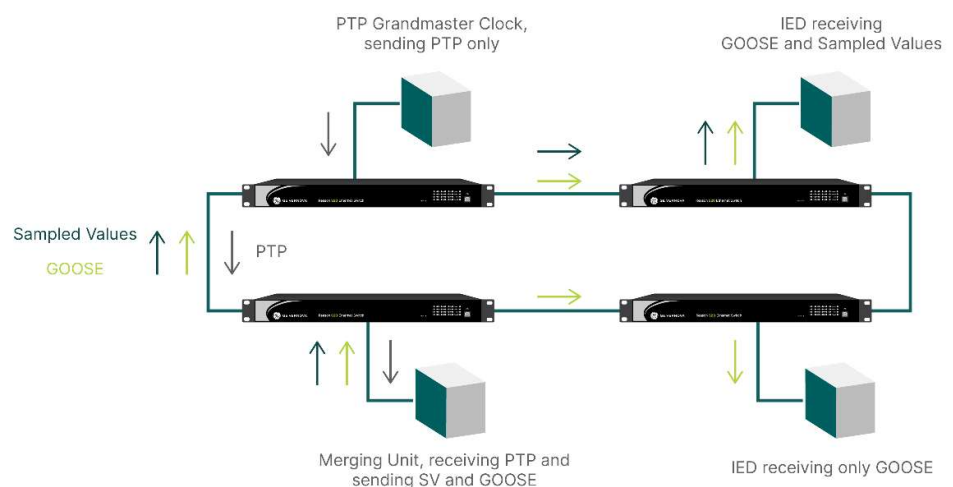


Figure 72: Topology to be configured in a VLAN environment

As a practical example, considering it is necessary to configure VLANs in order to virtually segregate different protocols, as illustrated in the above

figure where Sampled Values, GOOSE messages and PTP are present in the network. Consider the following assumptions:

1. Merging Unit sends GOOSE and Sampled Values with VLAN tag information, and receives PTP messages with VLAN information;
2. PTP Grandmaster Clock sends VLAN information on its PTP packets;
3. IED receiving GOOSE and Sampled Values can receive both messages with VLAN tag;
4. IED receiving only GOOSE messages is VLAN unaware, so GOOSE messages should be delivered to this equipment without VLAN information;
5. All equipment management interfaces used is at the same port used for other messages, and management communication (TCP/IP) is performed with untagged frames;
6. IED Receiving only GOOSE and PTP Grandmaster Clock equipment can have its operation crashed if Sampled Values traffic is injected on its Ethernet port. Other equipment have processing capacity to process Sampled Values traffic, if they are member of the Sampled Values VLAN;
7. GOOSE VID number is 10;
8. Sampled Values VID number is 20;
9. PTP VID number is 30;

Management VLAN to be used internally by the switch will be the VID number.

With information given below, it is possible to go to the Settings > VLANs menu to start configuration process. The configuration of the VLANs should be as follows:

VLAN configuration for Merging Unit

This port will receive untagged and tagged frames and send tagged frames from many VID, as Merging Units will multicast GOOSE and Sampled Values and receive PTP messages. In addition, management software will communicate with the equipment in that port. Thus, Merging Unit configuration ports should have the following characteristics:

- **VLAN Identifier Ingress process** : untagged frames would be forwarded to the Port VID VLAN, and tagged frames are forwarded to the VLAN that is embedded at the frame;
- **Filtering ingress process** : this port should accept both untagged and tagged frames;
- **Egress process** : egress process should be set to Untag only frames with Port VLAN identifier.

In summary, the VLAN configuration for this port may be recommended as follows:

- Port mode chosen as Trunk port;
- Port VLAN chosen 1;
- For trunk ports, Port Type is not allowed to be changed from C-Port;

- For trunk ports, Ingress Filtering is not allowed to be changed from enabled;
- For trunk ports, Ingress Acceptance is not allowed to be changed from Tagged and Untagged;
- Egress tagging chosen as Untag Port VLAN;
- Allowed VLANs chosen: 1, 10, 20, 30;
- No forbidden VLANs configured.

VLAN configuration for other switches

This port will receive untagged and tagged frames and send tagged and untagged frames from many VID, as all traffic from switches should traffic at these ports. Thus, configuration of these ports should have the following characteristics:

- **VLAN Identifier Ingress process:** untagged frames would be forwarded to the Port VID VLAN, and tagged frames are forwarded to the VLAN that is embedded at the frame;
- **Filtering ingress process:** this port should accept both untagged and tagged frames;
- **Egress process:** egress process should be set to Untag only frames with Port VLAN identifier.

In summary, the VLAN configuration for this port may is recommended as follows:

- Port mode chosen as Trunk port;
- Port VLAN chosen as 1;
- For trunk ports, Port Type is not allowed to be changed from C-Port;
- For trunk ports, Ingress Filtering is not allowed to be changed from enabled;
- For trunk ports, Ingress Acceptance is not allowed to be changed from Tagged and Untagged;
- Egress tagging chosen as Untag Port VLAN;
- Allowed VLANs chosen: 1, 10, 20, 30;
- No forbidden VLANs configured.

VLAN configuration for PTP Grandmaster clock

This port will receive untagged frames and send untagged and tagged frames from PTP VID, as Grandmaster Clock will multicast PTP messages. In addition, management software will communicate with the equipment in that port. Thus, PTP Grandmaster clock configuration ports should have the following characteristics:

- **VLAN Identifier Ingress process :** untagged frames would be forwarded to the Port VID VLAN, and tagged frames are forwarded to the VLAN that is embedded at the frame;
- **Filtering ingress process:** this port should accept untagged frames;
- **Egress process :** egress process should be set to Untag only frames with Port VLAN identifier.

In summary, the VLAN configuration for this port may be recommended as follows:

- Port mode chosen as Trunk port;
- Port VLAN chosen as 1;
- For trunk ports, Port Type is not allowed to be changed from C-Port;
- For trunk ports, Ingress Filtering is not allowed to be changed from enabled;
- For trunk ports, Ingress Acceptance is not allowed to be changed from Tagged and Untagged;
- Egress tagging chosen as Untag Port VLAN;
- Allowed VLANs chosen: 1, 30;
- Forbidden VLANs chosen: 10, 20

VLAN configuration for IEDs receiving GOOSE and SVs

This port will receive untagged and tagged frames and send untagged frames, only used by management software communication. Thus, IED Receiving GOOSE and Sampled Values configuration ports should have the following characteristics:

- **VLAN Identifier Ingress process** : untagged frames would be forwarded to the Port VID VLAN, and tagged frames are not expected. Thus, tagged frames can be if to be forwarded to the VLAN that is embedded at the frame;
- **Filtering ingress process** : this port should accept both untagged and tagged frames;
- **Egress process** : egress process should be set to Untag only frames with Port VLAN identifier.

In summary, the VLAN configuration for this port may be recommended as follows:

- Port mode chosen as Trunk port;
- Port VLAN chosen as 1;
- For trunk ports, Port Type is not allowed to be changed from C-Port;
- For trunk ports, Ingress Filtering is not allowed to be changed from enabled;
- For trunk ports, Ingress Acceptance is not allowed to be changed from Tagged and Untagged;
- Egress tagging chosen as Untag Port VLAN;
- Allowed VLANs chosen: 1, 10, 20;
- No forbidden VLANs configured.

VLAN configuration for IEDs receiving GOOSE only

This port will receive untagged and tagged frames and send untagged frames, only used by management software communication. Thus, IED Receiving only GOOSE configuration ports should have the following characteristics:

- **VLAN Identifier Ingress process** : untagged frames would be forwarded to the Port VID VLAN, and tagged frames are not

expected. Thus, tagged frames can be if to be forwarded to the VLAN that is embedded at the frame;

- **Filtering ingress process** : this port should accept both untagged and tagged frames, but there is a critical point on Sampled Values messages on that port. Thus, it is desirable to set Sampled Values VLAN as forbidden;
- **Egress process** : egress process should be set to Untag all frames, as this equipment cannot understand VLAN information.

In summary, the VLAN configuration for this port may be recommended as follows:

- Port mode chosen as Hybrid port;
- Port VLAN chosen as 1;
- Port Type chosen as C-Port;
- Ingress Filtering disabled;
- Ingress Acceptance chosen as Tagged and Untagged;
- Egress tagging chosen as Untag All;
- Allowed VLANs chosen: 1, 10;
- Forbidden VLANs chosen: 20.

These VLAN configuration settings should be enough to guarantee that only equipment expecting to receive a given traffic will receive it. Besides, segregation of traffic would increase the reliability of the network, as congestion on one VLAN would not affect other ones.

20.2 RSTP Configuring in a Ring Network Topology

Considering the same case as previously, this section will demonstrate in a practical way how to configure RSTP in a Ring Network topology.

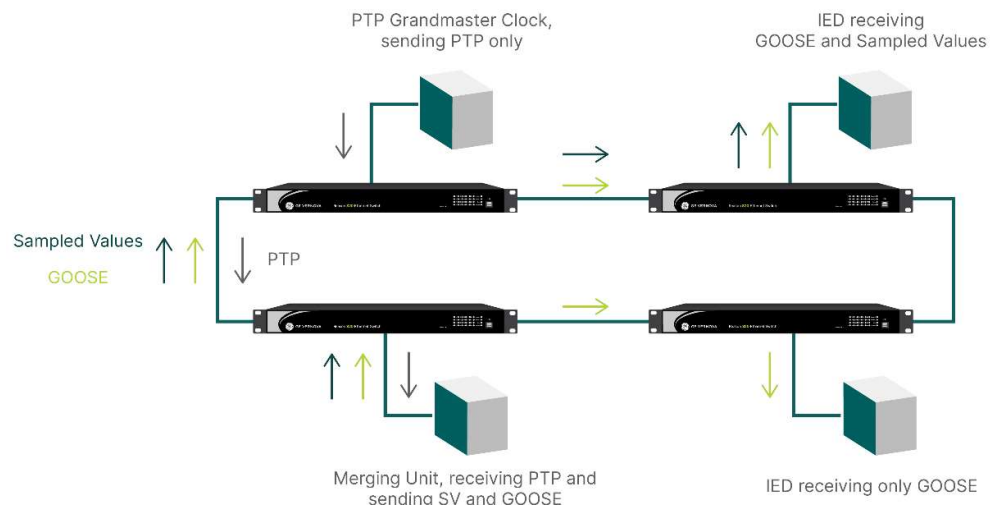


Figure 73: Topology to be configured in a RSTP environment

At this topology, all switches are considered to be RSTP-aware switches, that is, all switches can participate on Root election and use its values to the logical architecture.

Reason S20 supports the following Spanning Tree Protocols: STP, RSTP and MSTP. By default, MSTP protocol is set as the protocol to solve loops at the network. For these applications, there is no major configuration that is necessary to be performed except to change protocol version to RSTP, as default configuration is ready to send and receive BPDU packets and then use it to solve loops in the network. Default settings are as follows:

- Bridge Settings:
 - Protocol used is MSTP;
 - Bridge Priority is 32768;
 - Forward delay is 15;
 - Maximum age is 20;
 - Maximum hop count is 20.
- Ports Settings:
 - STP usage on all ports is enabled;
 - Path cost on all ports is auto;
 - Priority of all ports are 128;
 - All ports are configured as Auto-edge;
 - All ports are configured related to point-to-point connection as Auto;

For the architecture given above, all switches are STP-aware, so no BPDU guard function would be required.

With information given above, it is possible to go to the Settings > Spanning Tree > Bridge Settings menu to start configuration process.

At this situation, the only configuration needed to be done is changing Protocol Version to RSTP. Protocol itself will choose root bridge, designated, root, alternate and backup ports and could deal with the loops at the network in a RSTP environment.

If there is one specific bridge that is desired to be the root, choose the lowest Bridge Priority to that bridge and then configuration is done.

Repeat this steps on all switches at the topology, and after all of them are configured, configuration of basic RSTP usage will be finished.

20.3 PTP Transparent Clock

Considering the same case as previously, this section will demonstrate in a practical way how to configure the Reason S20 as a PTP Transparent clock in a Ring Network topology.

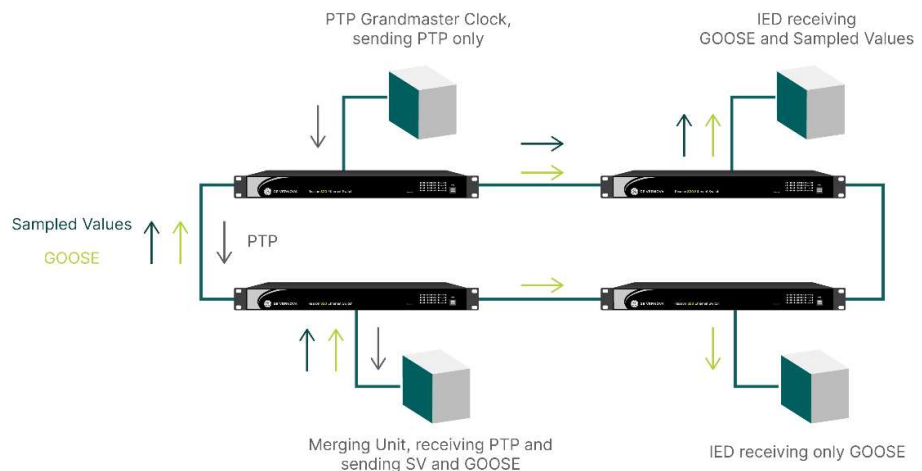


Figure 74: Topology to be configured in a PTP environment

PTP configuration in VLAN network

The first step would be to check the PTP information given by PTP Grandmaster Clock. In this case, let's assume the Grandmaster is configured as follows:

- Domain 0;
- Transmitted over Ethernet with VID 30 and PCP 4;
- Operation mode is two-step;
- Delay mechanism is peer-to-peer.

In this situation, be sure that VLAN 30 is created and ports that should be member of PTP VLAN are correctly configured at the Settings > VLANs menu. If necessary, the first example of this chapter can guide on how to configure a VLAN in Reason S20.

Back to the PTP configuration, it is necessary to create an instance to be used as P2P transparent clock.

- **Mode:** Transparent Clock;
- **Profile:** Custom;
- **Domain Number:** 0;
- **Network Protocol:** Ethernet;
- **VLAN:** Enabled;
- **VLAN ID:** 30;
- **VLAN Priority:** 4;
- **Delay Mechanism:** Peer-to-Peer
- **Delay Request Interval** and **Announce Interval/Timeout** may be configured as PTP network specification. Default values are recommended.

Remaining PTP General Configuration are indifferent for Transparent Clock mode.

After PTP general settings are done, select at the PTP Port Configuration checkboxes which ports will be members of the PTP instance. In the example given, ports that must be in the same parameters instance are:

- Port where PTP Grandmaster Clock is connected;
- Port where there are switch-to-switch connections;

- Port where PTP slave clocks are connected. In this example, port where Merging Unit is connected.

Repeat these steps on all switches that are being as Transparent Clock. In this example, all switches should be configured as shown, and ports connecting switch-to-switch and PTP clocks must be checked as members of the instance.

GE Reason S20

Industrial Managed Ethernet Switch

Chapter 6: Web Interface Monitoring

This chapter gives an overview of how to monitor the functions belonging to the Settings menu, when the equipment is accessed through Web interface.

1 System Management

The system menu provides online information about the system, CPU Load, IP Status, Log and Detailed Log menus.

If desired to update the web screen automatically, check the Auto Refresh checkbox on top to perform it. If selected, monitoring web page will be updated after 3 seconds of the last update automatically.

Information

System information presents basic information about the switch.

- System:
 - System's contact;
 - System's contact name;
 - System's location.
- Key:
 - Key number, which means key activation number;
 - PTP allowed. If "1", PTP function is enabled and if "0", PTP function is disabled.
- Hardware:
 - MAC Address number of the switch;
 - Serial Number of the switch;
- Time:
 - System date in "YYYY-MM-DDTHH:MM:SS-Timezone" format;
 - System Uptime, which means time since last power-up;
- Software
 - Software version, which is the current firmware running at the switch;
 - Software date;
 - Acknowledgements, where the Details link displays all open-source codes used by the switch.

CPU Load

CPU Load option allows user to view graphically CPU usage online of the switch. The graph has 25%, 50% and 75% percentage bars to guide user

about CPU Load, and graph is updated with the web page. Thus, for online monitoring, it should be selected the Auto-refresh checkbox at the top of the web page. Time increases from the left to the right.

Green line refers to a 100 ms average CPU load, blue line refers to a 1 second average CPU load and magenta line refers to a 10 seconds average CPU load.

IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbor cache (ARP cache) status.

- IP Interfaces: shows IP addresses of management interfaces.
 - Interface VLAN. If internal interface, the “OS:lo” text is shown;
 - Interface Type, that is, protocol type and version;
 - Interface Address;
 - Interface Status.
- IP Routes: shows the IP routes
 - Type: Routing protocol type
 - Network: The destination IP network or host address of this route;
 - Gateway: gateway address of route;
 - Status: status flags of the route.
- Neighbor Cache: the ARP cache used.
 - Neighbors IP Address;
 - Link Address of neighbors, that is, neighbor VLAN and MAC address.

Log

Log monitoring option allows user to view equipment log messages through the web interface. These messages are not all messages used internally by the equipment, however these log messages are the ones allowed to be send to a log server.

It is possible to select the log message level to be displayed. Allowed levels are Error, Warning, Notice and Informational messages. If all messages are desired to be displayed, select All option. Log messages are incremented as time passes, thus, lower ID messages are older log messages. Log identifier is a link that, if clicked, displays directly the Detailed Log menu of the ID chosen.

To clear log messages from the memory, the Clear button allows the user to delete log messages stored. The left and right buttons switch the displayed pages. By default, 20 log messages are displayed per page.

The information present are:

- ID of the log message;
- Level of the log message, according to its information;
- Timestamp of the log message, based on switch’s internal clock;
- Description of the message.

Detailed Log

Detailed Log monitoring option allows user to view detailed information for a given ID log message. It is possible to access this menu by clicking in the ID log message number at the Log menu.

On the top of the web page can be typed which ID log message is required. When there is a valid ID, the information per log shown is:

- Level of the log message;
- Timestamp of the log message, based on switch's internal clock;
- Description of the message, that is, the message which this entry contains.

2 Ports

This menu provides online monitoring regarding the State, Traffic Overview, QoS Statistics, QCL Status and Detailed Statistics of each port.

If desired to update the web screen automatically, check the Auto Refresh checkbox on top to perform it. If selected, monitoring web page will be updated after 3 seconds of the last update automatically.

State

State option allows user to view basic information about each port. Each port type possible is represented in a picture, that is, the pictures show if port type is RJ45, SFP LC or SFP RJ45 connector as follows:



RJ45 connector representation at the web interface;






SFP LC connector representation at the web interface;



SFP RJ45 connector representation at the web interface;

In addition, port state is displayed:

-  Port disabled;
-  Port enabled and up; link connected and communicating;
-  Port enabled and down; link not connected or communicating.

Traffic Overview

Traffic Overview option allows user to view basic information about data traffic. It is shown in the screen a table which contains the following information:

- Port number;
 - This number is a link which redirects to the Detailed Statistics menu, explained at the Detailed Statistics menu.
- Packets: Received and transmitted traffic, in number of packets;
- Bytes: Received and transmitted traffic, in bytes;

- Error: Received packets containing errors and transmitted packets incomplete;
- Drops: Received packets that were discarded based on ingress congestion and transmitted packets that were discarded based on egress congestion.
- Filtered: Received frames filtered by forwarding process.

QoS Statistics

QoS Statistics option presents basic information about QoS being executed in each port, as described below:

- Port identifier;
- Queues (Q0 to Q7 queues): Received (RX) and transmitted (TX) frames at the queue;

QCL Status

QCL Status option allows user to view information about the QoS Control List (QCL) configured in the switch. A table containing the following information is shown:

- User;
- QCE identifier;
- Ports member of the QCL;
- Frame type configured at QCL;
- Action executed by this QCL when incoming frames match the QCL filter. At the action columns, information about the CoS, DPL and DSCP values are displayed;
- Conflict information, that is, if there was conflict in the QCE at the QCL shown.

Detailed Statistics

Detailed Statistics option allows user to view detailed traffic information for a given Port. It is possible to access this menu by clicking in the Port Number at the Traffic Overview menu.

On the top of the web page can be selected which port is required.

Information shown is as follows:

- Total received frames at that port, including error frames. This information is divided in all packets, all octets, all unicast, all multicast, all broadcast and all Pause frames received;
- Total transmitted frames at that port, including error frames. This information is divided in all packets, all octets, all unicast, all multicast, all broadcast and all Pause frames transmitted;
- Total received frame size counter, which represents all frames divided by its size. Shown values are 64-bytes frames to 1527-and-above frames;
- Total transmitted frame size counter, which represents all frames divided by its size. Shown values are 64-bytes frames to 1527-and-above frames;
- Total Received Queue counters, in packets.
- Total Transmitted Queue counters, in packets.

- Total received error counters, in packets, which is divided in: Drop, CRC/Alignment, Undersize, Oversize, Fragments, Jabber and Filtered.
- Total transmitted error counters, in packets, which is divided in: Drop, CRC/Alignment, Undersize, Oversize, Fragments, Jabber and Filtered.

3 Security

This section describes the online basic security monitoring possibilities in Reason S20, such as Access Management Statistics, Network, AAA (Authentication, Authorization and Accounting) and RMON.

If desired to update the web screen automatically, check the Auto Refresh checkbox on top to perform it. If selected, monitoring web page will be updated after 3 seconds of the last update automatically.

Access Management Statistics

Access Management Statistics option allows user to view basic information about data traffic (received, allowed and discarded packets) divided in interface protocols (HTTP, HTTPS, TELNET and SSH). Besides, this menu also provides information about SNMP traffic (received, allowed and discarded SNMP packets).

Network

Network option presents information regarding the network where switch is connected.

- Port Security: provides information about the port security status. Port security is a module that does not have a specific direct configuration; as it is a set of configuration done at the switch. Information shown in this menu includes port status (users, state and MAC addresses) and detailed port information (MAC address at a given port, VLAN ID, time since a given MAC entered in the MAC table and so on);
- NAS: if NAS server is available and in use, NAS menu brings information about such as admin and port states and detailed port description.
- ACL Status: When using Access Control List (ACL), this menus present information about the ACL User, Access Control Entry (ACE) identifier, Frame type, Action, Rate Limiter, CPU, Counter and Conflict at a given ACL;
- ARP inspection: provides information about the Dynamic ARP Inspection Table. Shown values are port number, VLAN ID, MAC Address and IP Address of a given port number participating of the ARP inspection function;
- IP Source Guard: provides information about the IP Source Guard Table, such as port number, VLAN ID, IP Address and MAC Address of a given port number participating of the IP Source Guard function.

AAA

AAA (Authentication, Authorization and Accounting) option allows user to view information about the remote RADIUS user server. Information presented is as follows:

- Radius Overview: shows basic information about the RADIUS function at the switch, such the identifier RADIUS server number, server's IP address, UDP authentication port, status of the authentication for a given server (Disabled, Not Ready, Ready or Dead (number of seconds left)), UDP accounting port and status of the accounting function (Disabled, Not Ready, Ready or Dead (number of seconds left));
- Radius Details: shows details of the RADIUS AAA per server. It is shown Authentication and Accounting statistics of received and transmitted data, IP address, State (Disabled, Not Ready, Ready or Dead, including the number of seconds left) and Round-Trip Time of the selected server.

Switch

Switch option allows user to view information about the RMON server, when using RMON. Information shown is as follows:

- Statistics: shows statistic information of RMON monitoring function, such as index of the statistics entry, data source (port identifier to be monitored), drop packets, total data in octets, total data in packets, broadcast address data, multicast address data, CRC error packets, undersize detected packets, oversize detected packets, fragmented detected packets, frames with size larger than 64 bytes received with invalid CRC, best estimate number of collisions detected, total 64-bytes length packets received, total frames received with size between 65 and 127 bytes, total frames received with size between 128 and 255 bytes, total frames received with size between 256 and 511 bytes, total frames received with size between 512 and 1023 bytes and total frames received with size between 1024 and 1588 bytes;
- History: shows an overview of the RMON history entries, such as history entry index, data entry index, data entry start, packets dropped, total data in octets, total data in packets, broadcast address data, multicast address data, CRC error packets, undersize detected packets, oversize detected packets, fragmented detected packets and utilization of the physical layer network utilization estimation;
- Alarm: show an overview of the RMON alarm entries, such as alarm index number, interval for sampling and comparing thresholds, variable to be sampled, sample type, values of the statistics during last sample period, start-up alarm, rising threshold value, rising of the event index, falling threshold and falling of the even index;
- Event: shows an overview of the RMON events table, such as event index number, index of the log entry, timestamp of a given log event and description of the log event.

4 Link Aggregation Control Protocol (LACP)

This section describes the online information about the Aggregation functionality, presenting the System Status, Port Status and Port Statistics, menus, which are located at the LACP menu.

If desired to update the web screen automatically, check the Auto Refresh checkbox on top to perform it. If selected, monitoring web page will be updated after 3 seconds of the last update automatically.

System Status

LACP System Status monitoring option allows user to view basic information about Aggregation current usage.

- Aggr ID, which is the aggregation ID of the instance shown;
- Partner System ID, which is the MAC address (system ID) of the aggregation partner;
- Partner key, which is the key used in that aggregation instance;
- Partner priority;
- Last changed, that last time since each instance has changed;
- Local ports, presents switch ID plus port number, separated each other by the ":" character.

Ports Status

LACP Status option allows user to view information about LACP current usage per port. While the System Status provides information of aggregation instances in given equipment, Port Status allows verifying online status of the aggregation usage. Information shown is as follows:

- Port number;
- LACP information for that port:
 - Yes, which means LACP enabled and link up;
 - No, which means LACP disabled or link down;
 - Backup, which means unused port at the aggregation, but allowed to and can join aggregation group if one of the aggregated ports leaves the group.
- Key assigned in the port;
- Aggregation ID;
- Partner System ID, which is the MAC address (system ID) of aggregation partner;
- Partner port;
- Partner priority.

Ports Statistics

LACP Ports Statistics presents information about LACP messages exchanged between partners. This menu allows verifying if there are LACP messages received, transmitted and discarded by the equipment.

Information presented is as follows:

- Port number;
- Total received LACP messages per port, given in frames;
- Total transmitted LACP messages per port, given in frames;

- Total discarded LACP messages per port, given in frames. Discarded frames are shown divided into unknown and illegal discarded frames.

5 Loop Protection

This section describes the monitoring possibilities for Loop Protection via Web Interface in Reason S20.

If desired to update the web screen automatically, check the Auto Refresh checkbox on top to perform it. If selected, monitoring web page will be updated after 3 seconds of the last update automatically.

Loop Protection

Loop Protection Status monitoring option allows user to view basic information about loop protection running in Reason S20. Information allowed is as follows:

- Port number;
- Action configured to be executed in the interface if a loop is detected, which can be Shutdown, Log and Shutdown+Log;
- Transmit, which represents if the messages sending throughout the network is enabled or not;
- Loops, which represents total loops detected at the port since function was enabled;
- Status, which represents loop detection status at a given port. Allowed values are Up and Down, where Up represents link up and Down represents link down. If a link is disabled because of loop detected, the timestamp of the last loop detected is represented at the following column;
- Time of Last Loop, which represents the timestamp of the last detected loop. Timestamp shown in this column is based on system's internal clock.

6 Spanning Tree

This chapter describes monitoring possibilities for Spanning Tree monitoring, such as Bridge Status, Port Status and Port Statistics. If desired to update the web screen automatically, check the Auto Refresh checkbox on top to perform it. If selected, monitoring web page will be updated after 3 seconds of the last update automatically.

Bridge Status

Bridge Status option allows user to view basic information about the configured Spanning Tree values at the bridge and current topology information.

- MSTI, which represents bridge's instance. If MSTP is not used, only CIST is shown. MSTI name represented is also a link which redirects to the STP Bridge Status menu. If MSTI link is accessed, allowed information is as follows:

- STP Bridge Status: this table contains detailed information about STP current status at the bridge. Allowed information at the table is as follows:
 - Bridge instance;
 - Bridge ID, that is, the bridge identifier number, in the format "Priority.Bridge-MAC-Address";
 - Root ID, that is, the root bridge identifier number, in the format "Priority.Bridge-MAC-Address";
 - Root Cost, which is the current bridge to the Root bridge path cost;
 - Root Port, which is the port current working as Root Port;
 - Regional Root, that is, the MSTP regional root at the instance that is being verified;
 - Internal Root Cost;
 - Topology Flag, that is, current value of the change flag at this instance;
 - Topology Change Count, that is, all topology change messages received on the instance;
 - Topology Change Last, which represents last time since topology has changed at the selected instance;
- CIST Ports & Aggregation State table, where information about STP ports is shown. Allowed values are as follows:
 - Port number shown in the row. Only ports running BPDU exchanging over the network are shown at this table;
 - Port ID, that is, the port identifier number, in the format "Port-Priority.Bridge-Port-Number";
 - Role on the port, that is, Spanning Tree port state. Roles can be RootPort, DesignatedPort, AlternatePort and BackupPort;
 - State of the port, which can be forwarding or discarding;
 - Port's Path Cost, which is the path cost used by that port when transmitting BPDU packets over the network;
 - Edge, that is, if port is an edge port or not. Allowed values are Yes or No. Yes means port is an edge port, and No means port is a trunk port (not edge);
 - Point-to-Point, that is, if port communication is point-to-point or a shared link medium;
 - Uptime, which represents time since port is up.
- Bridge ID, that is, the bridge identifier number, in the format "Priority.Bridge-MAC-Address";
- Root ID, that is, the root bridge identifier number, in the format "Priority.Bridge-MAC-Address";

- Root port, that is, the port at the bridge operating as Root Port;
- Root path cost;
- Topology Flag, that is, current value of the change flag at this instance;
- Topology Change Last, which represents last time since topology has changed at the selected instance.

Port Status

STP Port Status monitoring option allows user to view basic information about all ports at the switch related to Spanning Tree.

- Port number shown in the row;
- CIST Role on the port, that is, Spanning Tree port state. Roles can be RootPort, DesignatedPort, AlternatePort, BackupPort and Disabled;
- CIST State of the port, which can be forwarding or discarding;
- Uptime, which represents time since port is up.

Port Statistics

STP Statistics monitoring option allows user to view packet exchanging information about ports exchanging BPDU packets.

- Port number shown in the row. Only ports enabled to transmit or receive BPDU packets are shown;
- Transmitted BPDU packets, in number of BPDU messages. There are four columns, where BPDU packet exchanging is divided in MSTP, RSTP, STP and total TCN (Topology Change Notification) messages transmitted on a given port;
- Received BPDU packets, in number of BPDU messages. There are four columns, where BPDU packet exchanging is divided in MSTP, RSTP, STP and total TCN (Topology Change Notification) messages received on a given port;
- Discarded BPDU frames received on a given port, divided in Unknown and Illegal BPDU frames received.

7 IPMC

This chapter describes the basic IP multicast (IPMC) monitoring possibilities to be used in Reason S20, providing information about the IGMP and MLD Snooping, such as Status, Groups Information and IP SFM Information.

If desired to update the web screen automatically, check the Auto Refresh checkbox on top to perform it. If selected, monitoring web page will be updated after 3 seconds of the last update automatically.

IGMP Snooping (IPv4 multicast environment)

- Status: shows IGMP table status information.
 - VLAN ID (VID) number of the entry;
 - Querier version (IGMPv1, IGMPv2 or IGMPv3);
 - Host version (IGMPv1, IGMPv2 or IGMPv3);

- Querier status. Allowed values are Active and Idle querier status;
 - Queries transmitted, in number of queries;
 - Queries received, in number of queries;
 - IGMPv1 reports received in number of reports;
 - IGMPv2 reports received in number of reports;
 - IGMPv2 leaves received in number of reports;
 - IGMPv3 reports received in number of reports.
 - Router port: shows IGMP router port information at the switch, that is, ports that are operating as router ports.
 - Port number;
 - Status of the port, that is, if port is Router or not.
- Groups Information: provides information about IGMP table groups allowed in the switch.
 - VLAN ID (VID) number of the group at the row;
 - Group address range of the group at the row;
 - Port members, where is displayed which ports are member of the group.
- IGMP SFM information, that is, IGMP Source-Filtered Multicast information. This information is related only to IGMPv3 and MLDv2 protocols, which has support to channel subscription.
 - VLAN ID (VID) number of the group;
 - Group address range of the group;
 - Port members, where is displayed which ports are members of the group;
 - Mode of SSM filtering, which indicates filtering mode (VID number, port number, address range of the group);
 - Source address, that is, IP address of the multicast source;
 - Type of the filtering of SSM (source-specific mode);
 - Hardware Filter / Switch, which indicates if data plane sent by source of the group can be treated by chip or not.

MLD Snooping (IPv6 multicast environment)

- Status: shows MLD table status information. Allowed information is as follows:
 - VLAN ID (VID) number of the entry;
 - Querier version (MLDv1 or MLDv2);
 - Host version (MLDv1 or MLDv2);
 - Querier status. Allowed values are Active and Idle querier status;
 - Queries transmitted, in number of queries;
 - Queries received, in number of queries;
 - MLDv1 reports received in number of reports;
 - MLDv1 leaves received in number of reports;
 - MLDv2 reports received in number of reports;

- Router port: shows MLD router port information at the switch, that is, ports that are operating as router ports.
 - Port number;
 - Status of the port, that is, if port is Router port or not.
- Groups Information: provides information about MLD table groups allowed in the switch.
 - VLAN ID (VID) number of the group;
 - Group address range of the group;
 - Port members, where is displayed which ports are member of the group.
- MLD SFM information, that is, MLD Source-Filtered Multicast information. This information is related only to IGMPv3 and MLDv2 protocols, which has support to channel subscription.
 - VLAN ID (VID) number of the group;
 - Group address range of the group;
 - Port members, where is displayed which ports are members of the group;
 - Mode of SSM filtering, which indicates filtering mode (VID number, port number, address range of the group);
 - Source address, that is, IP address of the multicast source;
 - Type of the filtering of SSM (source-specific mode);
 - Hardware Filter / Switch, which indicates if data plane sent by source of the group can be treated by chip or not.

8 MAC Table

This section describes MAC Address presented in the web interface for monitoring purposes.

If desired to update the web screen automatically, check the Auto Refresh checkbox on top to perform it. If selected, monitoring web page will be updated after 3 seconds of the last update automatically.

MAC Address Table

MAC Address table presents the current address table being used by the switch. Rows at the table indicate entries of the MAC table, and columns organize information displayed. This table is used for forwarding decision by a bridge.

- Type, which indicates type of the learning process. Ports configured as Auto will be displayed as Dynamic learning type, and Ports configured as Secure will be displayed as Static learning type port;
- VLAN identifier (VID) of the MAC address;
- MAC Address mapped and included at the MAC Table;
- Port members, divided in column per port. If a specific MAC address can be member of a given port, the symbol will be marked at this MAC address row and Port column.

9 VLAN

This section presents the VLAN table and ports for monitoring purposes, providing information about the VLANs Membership and Ports menu. If desired to update the web screen automatically, check the Auto Refresh checkbox on top to perform it. If selected, monitoring web page will be updated after 3 seconds of the last update automatically.

VLAN Membership

VLAN Membership Status for Combined users table allows monitoring current VLANs configured and running at the switch.

- VLAN ID;
- Port members, divided in checkboxes per port.
 - Symbol ☒ shown at a port column means that the port is a member of VLAN ID related to the row;
 - Symbol ☐ shown at a port column means that the port is not a member of VLAN ID related to the row.

VLAN Ports

VLAN Ports Status for Combined users table allows monitoring current port VLAN information configured and running at the switch.

- Port number;
- Port type, that is, if port is Unaware, C-Port, S-Port, S-Custom-Port;
- Ingress filtering at the port. Checkbox enabled means port is performing port filtering, and checkbox disabled means port is not performing port filtering;
- Frame type. If ingress filtering is enabled, frame type column will display which frame types are allowed at that port. Possible values are All, Tagged or Untagged;
- Port VLAN ID;
- Port Tx Tag, that is, configured transmission tag behavior. Possible values are Untag All, Tag All and Untag PVID;
- Untagged VLAN ID, which indicates frame behavior at the egress process;
- VLAN Conflicts status. Conflicts can be functional conflicts or hardware limitation (conflict between user modules).


10 PTP

This section describes the monitoring possibilities of PTP through web interface.

If desired to update Reason S20 web screen automatically, check the Auto Refresh checkbox on top-right corner. If selected, monitoring web page will be updated every 3 seconds.

PTP Clock Configuration

PTP Clock Configuration demonstrates the PTP clock instance configured at the switch. As only one PTP instance is possible, the Inst column will always display “0” and by clicking it further PTP details will be shown. The remaining monitoring interfaces are:

- **Device Type:** Demonstrated the PTP mode Reason S20 is operating;
- **Port List:** If  means the referenced port is member of the PTP instance configured. If blank, the PTP is disabled for that port.

GE Reason S20

Industrial Managed Ethernet Switch

Chapter 7: Maintenance & Troubleshooting

1 Network Diagnostics

1.1 Ping

Ping menu allows using the IPv4 Ping messages to do network diagnostics. Ping messages are ICMP packets that are used to verify if a host is reachable in the IP network environment. In addition, Ping messages can return if host is reachable, presenting the round-trip time.

Reason S20 allows using its management IP interface as the originator of a ping message. Thus, it is possible to verify IP hosts reachability from the switch, doing basic diagnostics functions in the network.

Ping menu is located at Diagnostics > Ping.

IP Address

This field allows configuring IP address of a host connected to the network in order to verify if it is reachable by switch or not. IP address must be typed in decimal dotted format.

Ping Length

Configure ping length, that is, the payload size of the ping packet. Allowed values are integer numbers from 2 to 1452 bytes. By default, ping payload size is 56 bytes.

Ping Count

Define how many times ping messages answers and responses should be performed to the address configured. Allowed values are integer numbers from 1 to 60 times. By default, ping is done 5 times.

Ping Interval

This field allows configuring ping interval from each ping message send. Allowed values are integer numbers from 0 to 30 seconds. By default, ping interval is performed once a second (value = 1).

After one of the configurations described before is changed, there is a button that allows the user to start the function, as follows.

- Start: start the ping messages sending by switch's IP interface.

1.2 Ping6

Ping6 menu allows using IPv6 ping messages to do network diagnostics. Ping messages are ICMP packets that are used to verify if a host is reachable in an IP network environment. In addition, Ping messages can return if host is reachable, presenting the round-trip time.

Reason S20 allows using its management IP interface as the originator of a ping message. Thus, it is possible to verify IP hosts reachability from the switch, doing basic diagnostics functions in the network.

Ping menu is located at Diagnostics > Ping6.

IP Address

This field allows configuring IP address of the host connected to the network in order to verify if it is reachable by switch or not. IP address must be typed in hexadecimal format with a colon (":") separating each field.

Ping Length

Configure the ping length, that is, the payload size of the ping packet. Allowed values are integer numbers from 2 to 1452 bytes. By default, ping payload size is 56 bytes.

Ping Count

This field allows configuring how many times ping messages answers and responses should be performed to the address configured below. Allowed values are integer numbers from 1 to 60 times. By default, ping is done 5 times.

Ping Interval

This field allows configuring ping interval from each ping message send. Allowed values are integer numbers from 0 to 30 seconds. By default, ping interval is performed once a second (value = 1).

Egress Interface

This field allows specifying which VLAN ID should be used in the egress interface to be used to send ICMP Ping packets. VLAN allowed values are 1 to 4,095. By default, this field is empty, which means that Ping6 function will define itself best interface to be used.

After one of the configurations described before is changed, there is a button that allows the user to start the diagnostic, as follows.

- Start: start the ping messages sending by switch's IP interface.

1.3 VeriPHY

VeriPHY is a function performed by Reason S20 itself to verify integrity of electrical cables connected to the switch, for diagnostics purposes.

This function is performed directly at the PHY chips, which do interface between layer 2 and layer 1 communication. PHY chips inspect link quality majority based on the impedance measured on each pair in a CAT-5 cable.

VeriPHY cable inspection can only be used in electrical cables, that is, CAT-5 or higher quality cables connected through a RJ45 connector. This function does not support Optical links.

While running on, VeriPHY function can disturb communication on the port that is being used by this function. Thus, if using VeriPHY function, make sure in the period the function is running, there will be no major problem on data losing.

Port

Select the port that is requested to perform cable inspection by VeriPHY. After one of the configurations described before is changed, there is a button that allows the user to start the function, as follows.

- Start: start the VeriPHY inspection.

The result is displayed in a table, where the rows represent the ports and the columns each pair in a CAT-5 cable. Columns are divided by Pair (pair A, B, C and D) and Length (Length of the pair A, B, C and D).

By default, all cells are shown with the "--" symbol. When the diagnostic is finished, the results are shown to check if any problem was detected. Possible results are as follows:

- Pair column:
 - OK: means that cable is without injuries;
 - Open: means that the pair represented at this cell is open;
 - Short: means that the pair represented at this cell is shorted;
 - Short Pair: can be for pair A, B, C or D. Means that there is a cross-pair short at the pair;
 - Cross Pair: can be for pair A, B, C or D. Means that there is an abnormal cross-pair coupling with the pair.
- Length column:
 - The length (in meters) of the cable pair (5-meters accuracy).

2 Maintenance

2.1 Restart Device

If desired to restart the equipment, the Restart Device menu can be accessed through web interface, located in Maintenance section. The running-config on the equipment will be lost after restarting the device. Once restarted, the booting process will load the startup-config, replacing the previous running-config.

A message on the web interface warns if user wants to restart the device:

- Yes: After clicking this button, system will perform a restart and actual running-config will be lost. In booting process, startup-config will replace the running-config;
- No: leave this menu and do not restart the device.

2.2 Factory Defaults

If desired to restore the factory default configuration, the Factory Defaults menu can be accessed through web interface located in Maintenance section. Alternatively, the user can return the device to factory default configuration by creating a loop between ports 1 and 2 as explained previously in “Factory Reset” section.

When accessing the Factory Defaults menu, the user can choose the following options:

- Yes: reset device. After clicking this button, system will perform a reset and all configurations will be lost. In booting process, startup-config and running-config will be replaced by the factory default config;
- No: leave this menu and do not reset the device.

2.3 Software Upload

Reason S20 performs a secure firmware update, using checksum to check integrity and a digital signature to ensure authentication. The file transfer protocol used to update the firmware is secure (SFTP).

S20 relies on two different software files: application and base.

- The application software is available to users through GE’s website as patch for new features, performance & robustness improvements, etc.

.dat files were used up to FW version 06A02, in which the digital signature was introduced. For this reason, FW 06A02 have both .dat and .sdt files. The first must be used when uploading from a previous FW version to FW 06A02. In case the FW06A02 is corrupted, the .sdt file must be used. From FW 07A00 and on, only the .sdt file is provided. In FW 07A04, the application software remains as .sdt file

- The base software, as the names suggests, is the base software where the application software is installed on. In addition, it also includes the bootloader. This is available through GE’s contact center if needed.

Base software was first introduced in FW 07A04 using .sbs file extension

Both the application and base software upload menu is located at Maintenance > Software Upload.

- Choose File, respectively for application or base software:
 - .dat or .sdt for application software, or;
 - .sbs file for base software
- Upload: after a valid file is selected, this button will execute the software upload function.

While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

After the software image is uploaded, a page announces that the firmware/base software update is initiated. After about a minute, the firmware is updated and the switch restarts.

Software uploading process takes a few minutes (expect FW 06A02 upgrade, which takes up to 15 minutes). While software is being uploaded, the switch will remain unavailable.

2.4 License

S20 has two features that might be enabled by licensing, the IEEE 1588v2 time synchronization protocol and/or the L3 functionalities including RIP v1/2, OSPF and VRRP. Such functionalities may be either enabled when ordering the equipment or upgraded later by ordering a new license file. The S20 will upgrade and activate the functions by simply uploading to the equipment the new license file ordered.

Alternatively, the user can check which features are activated at the device, and download the current license file if desired.

2.5 Configuration

Reason S20 stores internally three configuration files, which can be freely selected by user to become active. One of them is the main active configuration file, the running configuration file used by the switch, which is lost if equipment restarts. Another one is the startup configuration file, that is, the file that will become active at boot process of the switch. The last one is the factory default configuration file. The configuration files and their descriptions are as shown below.

- **Running Config:** This file contains the actual configuration of the switch. When the save button is pressed at any settings menu, changes made at the configuration will be saved at this file. If the

switch is restarted, this configuration is discarded and the switch will replace this running config file, after the reboot, for the Startup Config file;

- **Startup Config:** This file contains the configuration the switch will run after it is powered up or restarted. If a change in the Running Config was performed and it is requested to maintain the Running Config at the Startup Config, the user must save it at the Startup Config at the Save Running Configuration to startup-config option, at the Maintenance menu;
- **Default Config:** This file contains factory default configuration of switch. If necessary, it can be loaded by software to replace actual running configuration or the start-up configuration file.

Save startup-config

Save startup-config menu is located at Maintenance > Configuration > Save startup-config.

It is highly recommended to the user to save in startup-config file the changes made on the device once and a while, as it ensures the configurations already made will not be lost if the device comes to restart or power cycle.

To save running config at the startup config, click at the Save Configuration button. After this is done, running config is stored as startup config.

Download

Download menu is located at Maintenance > Configuration > Download.

In this menu, it is possible to download configuration as a file, to be used as a backup configuration file for restoring system, for instance. It is possible to download running-config, default-config and startup-config configuration files.

To download a configuration, select which configuration is desired to be downloaded and click at the Download Configuration button. In addition, the SFTP copy command is enabled to download the configuration through CLI.

Upload

Upload menu is located at Maintenance > Configuration > Upload.

In this menu, it is possible to upload a configuration file previously downloaded, to be used as a configuration file for restoring system, when required. It is possible to upload a file as the running-config and startup-config configuration files. In addition, it is possible to create a new configuration file (there will be, then, running-config, startup-config and the new file), if required.

If upload file will be used as running configuration, it is possible to choose to replace running configuration or to merge running config with the configuration uploaded. In this last option, running config will be maintained and only mismatches between running config and the uploading file will be uploaded.

To upload a configuration, select which configuration is desired to be uploaded and then click at the Upload Configuration button. After this is done, configuration will be uploaded as selected. In addition, the SFTP copy command is enabled to upload the configuration through CLI.

Activate

Activate menu is located at Maintenance > Configuration > Activate.

In this menu, it is possible to activate a configuration (either default-config or startup-config) to the running configuration.

To do so, select which configuration is desired to be activated and then click at the Activate Configuration button. After this is done, configuration selected will be activated as the running config file.

Delete

Delete menu is located at Maintenance > Configuration > Delete.

This menu gives the capability of deleting the startup-config file.

To delete it, select the startup-config and then click at the Delete Configuration File button. After this is done, configuration file will be deleted of switch's internal memory.

3 Troubleshooting

This chapter describes the most common issues that could occur when using Reason S20. The topics below show the issues that may occur and its description gives the actions that need to be taken to solve the issue.

Power LEDs are off

Power LEDs off means power supply is missing. Check if power cables are correctly connected to the corresponding screws, check if power plug is correctly inserted or check if power supply is enabled at the system, verifying voltage at the power supply connectors.

I do not know switch's management IP address

If IP address of the management interface was lost, there are some actions that could be done to recover it. Major actions are shown below:

- **Maintaining switch's configuration** : connect the terminal to the USB interface of the switch. After communication is established, the command to recover IP address is:

```
show ip interface brief
```
- **Losing switch's configuration** : While the switch is turned off, connect ports 1 and 2 to create a loop between them. After this, power-up the switch. This procedure will restore configuration to the factory default configuration, and then IP address of the equipment will be 192.168.4.88, and mask length will be 255.255.255.0.

Web interface cannot be accessed

If the terminal that is intended to be accessed cannot be reached even when IP is known, there are some steps to be performed to check if terminal can connect to the equipment.

- **Check if cables connecting terminal and switch are properly operating**. In addition, if possible, check if LEDs corresponding to the port used by terminal are blinking, showing that communication is being performed at the port;

- **Be sure that terminal is at the same IP subnetwork of switch's interface.** Check it by inspecting switch's management interface mask length and IP address and terminal mask length and IP address. Bits enabled related to mask length compared to IP address should be equal from both terminal and management interface, which means equipment in the same IP network;
- **Be sure that port where terminal is connected is at the VLAN of the management interface.** If there is no VLAN configured, be sure that VLAN of the management interface configured is the default VLAN (VID = 1);
- **Try a PING command from terminal to the switch's management interface.** If switch responds to PING messages but web interface is not able to open management interface, be sure that web browser's proxy usage is properly configured to permit switch's management interface.

Electrical link is not operating properly

If electrical links are not operating properly, there are two options to be verified:

- **Link is operating, but packets are being lost randomly.** In this case, possible cause of the problem is a pair of the UTP cable broken. It can be verified by VeriPHY function, which will display the pair broken, or exchanging Ethernet cable. It can be also tested by changing the port's speed, as 100 Mbps ports use 2 pairs while 1 Gbps uses 4 pairs of the cable, for instance. Thus, lowering port speed could give a feedback about cable quality. Besides, this problem should be solved after the UTP cable is exchanged by a good quality UTP cable;
- **Link is not operating.** In this case, possible cause of the problem is that cable is broken, RJ45 connector is broken or port is disabled. If port is disabled, enable it at the web interface. To enable ports, go to the Ports menu, choose port to be enabled and then select correct port speed. If cable or connector is broken, this problem should be solved after the UTP cable is exchanged by a good quality UTP cable.

I do not need VLANs. Do I have to change default settings?

By default, all ports are member of the VLAN ID 1 in Reason S20. Management interface is configured to be member of the VLAN ID 1, all ingress frames are classified to the VLAN ID 1 and all egress frames are forwarded without VLAN tag. Thus, all equipment connected will be member of the same VLAN, and will receive and transmit information as they are in the same LAN. Thus, if there is no VLAN usage on the network, default settings would not require to be changed.

I use VLANs, but they do not appear to be working

When using VLANs, there are several topics that must be clarified by user while configuring the switches.. Be sure that the following topics are respected if VLAN is not working properly.

- **Port type must be correct** . Be sure that equipment connected to the port where VLAN is being configured is correct. If not, the ingress filter should drop packets or change incoming VLAN ID frames to the VLAN ID of the ingress port, thus a given VID frame will be redirected to port VID VLAN;
- **Port Filtering is being respected**. If ingress filtering is enabled, untagged or tagged frames could be dropped, depending on the filter configured. Be sure that ingress filtering is correct for that port;
- **Egress tagging parameters work as host requires** . Egress filtering can maintain VLAN tag, cut-off VLAN tag or cut-off only frames with the port VID tag. Thus, be sure that egress tagging is configured as the host needs. If host supports VLANs, be sure that egress filtering is sending VLAN tag the host is expecting to receive. If host does not supports VLANs, be sure that frames are being forwarded without VLAN tag;
- **Be sure that VLAN is allowed in the port, and be sure that VLAN is not forbidden on that port** . Frames with VLAN information can only be forwarded if they ingress at a port that is allowed to receive frame's VLAN. If not, packet will be dropped. In addition, frames with VLAN ID forbidden for a given port will also be dropped.

Date or time are wrong

Reason S20 internal clock is updated based on NTP, PTP 1588 or manually, in this order of priority. If date or time is wrong, follow the steps below:

- Be sure that NTP client is properly configured. It can be verified at the Settings > System > NTP menu;
- Be sure that NTP server of the network is reachable. It can be tested by switch's internal PING command, where it must be commanded a PING to configured NTP server;
- Check if Timezone is configured properly, at Settings > System > Time menu. If Daylight Saving Time is used, check if it is properly configured.
- In case you want to use PTP as time source, make sure to disable the NTP client and check PTP is properly configured including the "PTP Adjust system time" enabled.



Firmware must be updated

When firmware update is required, the first step to be done is requiring GE for the firmware file. After this file is received, copy the file to the PC on which management interface of the switch is performed.

Updating firmware menu is located at the Maintenance menu. To update firmware, go to the Maintenance > Software > Upload menu, select correct firmware file (.dat file) and then click at the Upload button.

How can I guarantee that configuration file will not be lost if I reboot the switch?

When doing configuration changes, the first step is to guarantee that new settings are working properly. After changing and saving configuration, be sure that the configuration saved (the running configuration) is working properly, testing the Ethernet network. After guaranteed that running

configuration is working, save it at the startup config, located in Maintenance  Configuration  Save startup-config. After running configuration is saved at the startup configuration, it is guaranteed that configuration will not be lost in a reboot process.

Be sure that there is no loop between ports 1 and 2 when rebooting the switch if restore the factory configurations is not required.

4 Equipment Return

All parts and components comprising Reason devices shall be repaired exclusively by GE. In case of equipment malfunction the customer shall get in contact with GE's Contact Centre and never attempt to repair the device by own.

To request equipment repair service, call GE to check out shipment options and receive the technical assistance order code.

The equipment shall be packed in its original package or a suitable package to protect against impacts and moisture.

5 Instructions for Equipment Repair Service

The instructions presented in this topic shall only be followed by GE service Personnel.

In case any repair needs to be done in the equipment, follow the procedure below to ensure the safety of the operation.

- 1) Disconnect power supply;
- 2) Disconnect all other connections leaving the grounding strap to be removed at the end;
- 3) Perform a visual inspection to make sure the equipment is isolated;
- 4) Position the device in place where there is free space to work and make sure to install proper working and safety warnings at the location, also keep available all tools and aids that is going to be used;
- 5) Wait a few minutes so the capacitors may discharge;
- 6) Disassemble the device by unscrewing the case screws and pulling up the top side of the case; after that, carry on with the proper repairs. Keep in mind that disassembling the equipment may expose sensitive electronic circuitry. Take suitable precautions against electrostatic voltage discharge (ESD) to avoid damage to the equipment.

After the repairs are done, follow the procedure below in order to verify the safe state of the equipment and to put it back into operation.

- 1) Reconnect all internal cable that have been removed for the repair;
- 2) Perform a visual inspection on the device to make sure there are no remainders of the repair service inside the casing or any other noncompliance;
- 3) Place back the top side of the case and fasten it using the proper screws;

- 4) Connect the grounding strap and then the power supply to the equipment;
- 5) Wait for the equipment to initialize. It could take about a minute;
- 6) Follow the procedures in the Safety Section.

GE Reason S20

Industrial Managed Ethernet Switch

Chapter 8: Technical Specifications

1 General Switching Characteristics

Table 8: General Switching Characteristics

Parameter	Description
Switching Capacity	68 Gbps
Switching Latency	3 μ s
Number of VLANs	up to 4095
MAC Table entries	up to 8192 (64 static)
Class of Service (CoS) levels	up to 8

2 Ethernet Communication

Table 9: Ethernet Communication Characteristics

Parameter	Description
Number	Up to 24 Gigabit ports (up to 6 interface modules with 4 Eth ports each)
Type	Each interface module (4 Eth ports) may be either: <ul style="list-style-type: none"> Fixed RJ45: 10/100 Mbps or 10/100/1000 Mbps SFP slots: blank, with fiber SFP transceivers (100Mbps or 1000 Mbps options) or with electrical RJ45 SFP transceivers (10/100/1000 Mbps)
Mounting	Rear mounting

3 USB Communication

Table 10: USB Communication Characteristics

Parameter	Description
Console port	1x USB Type B 2.0 in front of chassis

Parameter	Description
Speed	11520 bits per second
Data bits	8
Stop bits	1
Parity	None
Flow Control	None

4 Time Synchronization

Table 11: Time Synchronization Characteristics

Parameter	Description
PTP IEEE 1588v2	Available in all ports when enabled. Hardware-based time stamping. Operation as transparent, boundary or slave clock
NTP Client	Possible to configure up to 5 external NTP servers
NTP Server	Can act as NTP server in all ports. Source time is based on either: External NTP Server IEEE 1588v2 (PTP) Manually configured
Real Time Clock (RTC)	When power-off, the real-time clock remains active for 2 days

5 Networking Standards Supported

Table 12: Networking Standards supported

Standard	Description
IEEE 802.3i	10BASE-T
IEEE 802.3u	100BASE-T(X)/100BASE-FX
IEEE 802.3ab	1000BASE-T(X)
IEEE 802.3z	1000BASE-SX/LX/ZX
IEEE 802.3x	Full duplex operation, flow control
IEEE 802.1D	Media Access Control (MAC) bridges
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1s	Multiple Spanning Tree Protocol (MSTP)
IEEE 802.1Q	VLAN (Virtual Local Area Networks)

Standard	Description
IEEE 802.1p	Class of service
IEEE 802.1X	Port-based Network Access Control
IEEE 802.3ad	Link Aggregation Control Protocol (LACP)
IEC 61850	Power Substation applications (tests performed by KEMA)
IEEE 1588 v2 PTP	IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

6 Networking RFC Standards

Table 13: Networking Request for Comments (RFC) Standards

Standard	Description
RFC 4363	VLAN MIB
RFC 2819	RMON
RFC 1213	MIB II
RFC 1215	Traps MIB
RFC 4188	Bridge MIB
RFC 4292	IP Forwarding Table MIB
RFC 4293	MIB for the Internet Protocol (IP)
RFC 5519	Multicast Group Membership Discovery MIB
RFC 4668	RADIUS Authentication Client MIB
RFC 4670	RADIUS Accounting MIB
RFC 3635	Ethernet-like MIB
RFC 2863	Interface Group MIB using SMI v2
RFC 3636	802.3 MAU MIB
RFC 4133	Entity MIB version 3
RFC 3411	SNMP Management Frameworks
RFC 3414	User-based Security Model for SNMPv3
RFC 3415	View-based Access Control Model for SNMP
RFC 5171	Unidirectional Link Detection (UDLD)
RFC 5905	NTP Synchronization
RFC 5424	Syslog Messages

Standard	Description
RFC 5426	Log Messages through UDP protocol
RFC 1157	SNMP Protocol
RFC 3418	SNMP MIB
RFC 3584	SNMP v1, v2c, v3
RFC 4604	IGMPv3 & MLDv2 Snooping
RFC 3260	DSCP
RFC 6040	Explicit Congestion Notification (ECN)
RFC 1058	Routing Information Protocol (RIP) version 1
RFC 2453	Routing Information Protocol (RIP) version 2
RFC 2328	Open Shortest Path First (OSPF) version 2
RFC 2338	Virtual Router Redundancy Protocol (VRRP)

7 RJ45 Ethernet (10/100/1000 Mbps) Ports

Table 14: RJ45 Ethernet Ports specification

Parameter	Description	Notes
Type	Two fixed options (FE or GE) One RJ45 SFP option	SFP Order Code: SFP1GCU02K
Speed	10/100/1000 Mbps (SFP or fixed) 10/100 Mbps (fixed only)	Auto-negotiating
Duplex	FDX/HDX (Full/Half duplex)	Auto-negotiation
Cable-type	Category 5	Shielded/Unshielded
Wiring Standard	TIA/EIA T568A/B	Auto-Crossover, Auto-Polarity
Max Distance	100 m	
Connector	RJ45	
Isolation	1,5 kV	RMS 1-minute



To avoid the risk of electrical shocks when using copper cables the connected cable length shall be less than 3m length and must not extend beyond the cabinet where the product is used. Furthermore, the equipment connected to both ends of the RJ45 cable shall be connected directly to a common earth point within the same cabinet to avoid step voltage (Ground Potential Rise) hazards.

8 Optical Transceivers (100/1000 Mbps)

Table 15: Optical Transceivers specification

Model	Rate	Max cable length (fiber type)	Wavelength	Transmitter optical power (min / max)	Receiver max sensitivity / overload
SFP1GFO05K	1.25 Gbps	0.5 km (MMF)	850nm	-9 / -3 dBm	-17 / 0 dBm
SFP1GFO20K	1.25 Gbps	20 km (SMF)	1310nm	-9 / -3 dBm	-23 / -3 dBm
SFP1GFO40K	1.25 Gbps	40 km (SMF)	1310nm	-5 / 0 dBm	-23 / -3 dBm
SFP1GFO80K	1.25 Gbps	80 km (SMF)	1550nm	0 / +5 dBm	-23 / -3 dBm
SFP01GFO2K	155Mbps	2 km (MMF)	1310nm	-20 / -14 dBm	-31 / -3 dBm
SFP01GFO20K	155Mbps	20 km (SMF)	1310nm	-14 / -8 dBm	-32 / -3 dBm



NEVER look into the optical fibers or optical output connections. Always use optical power meters to determine operation or signal level.

9 Power Supply

Table 16: Power Supply specification

Power supply High Voltage AC/DC	Input range
Nominal Range	110-240 V _{AC} , 50/60 Hz 125-250 V _{DC}
Operating Voltage Range	88-264 V _{AC} , 50/60 Hz \pm 3 Hz 88-300 V _{DC}
Maximum Current Consumption	0.5 A
Power Consumption	60 VA max
Power supply Low Voltage DC	Input Range
Nominal DC	48 V _{DC}
Operating Voltage Range	39 – 57 V _{DC}
Maximum Current Consumption	1.1 A
Power Consumption	45 W max

10 Failsafe Relay

Table 17: Failsafe Relay specification

Parameter	Value
Type of output	Dry contact Form C: NC and NO
Maximum AC Capacity	250 Vac / 2 A

Parameter	Value
Maximum DC Capacity	2 A @ 24 Vdc 700mA @ 48 Vdc 200 mA @ 125 Vdc 100 mA @ 250 Vdc (max voltage)

11 Operating/Storage Environment

Table 18: Operating/Storage Environment

Type	Level
Operating temperature (continuously)	-40°C to +52°C
Operating temperature (16h)	-40°C to +85°C (110-240 V _{AC} / 125-250 V _{DC} power supply) -40°C to +70°C (48 V _{DC} power supply)
Cooling system	Fanless
Storage/shipping	-40°C to +85°C
Altitude	≤ 2000m
Humidity	5-95% relative humidity, non-condensing
Ingress Protection	IP20 rear and sides IP30 front
Pollution Degree	II
Conformal Coating	DOWSIL™3-1953

12 Physical Characteristics

Table 19: Physical Characteristics

Parameter	Value
Dimensions	19-inch rack mount (43.6 mm width w/o bracket) 1U in height (43.7 mm) 310 mm in depth
Weight	approx. 3.2 kg (w/o package)
Structure	Steel minimized Z100 0.95mm

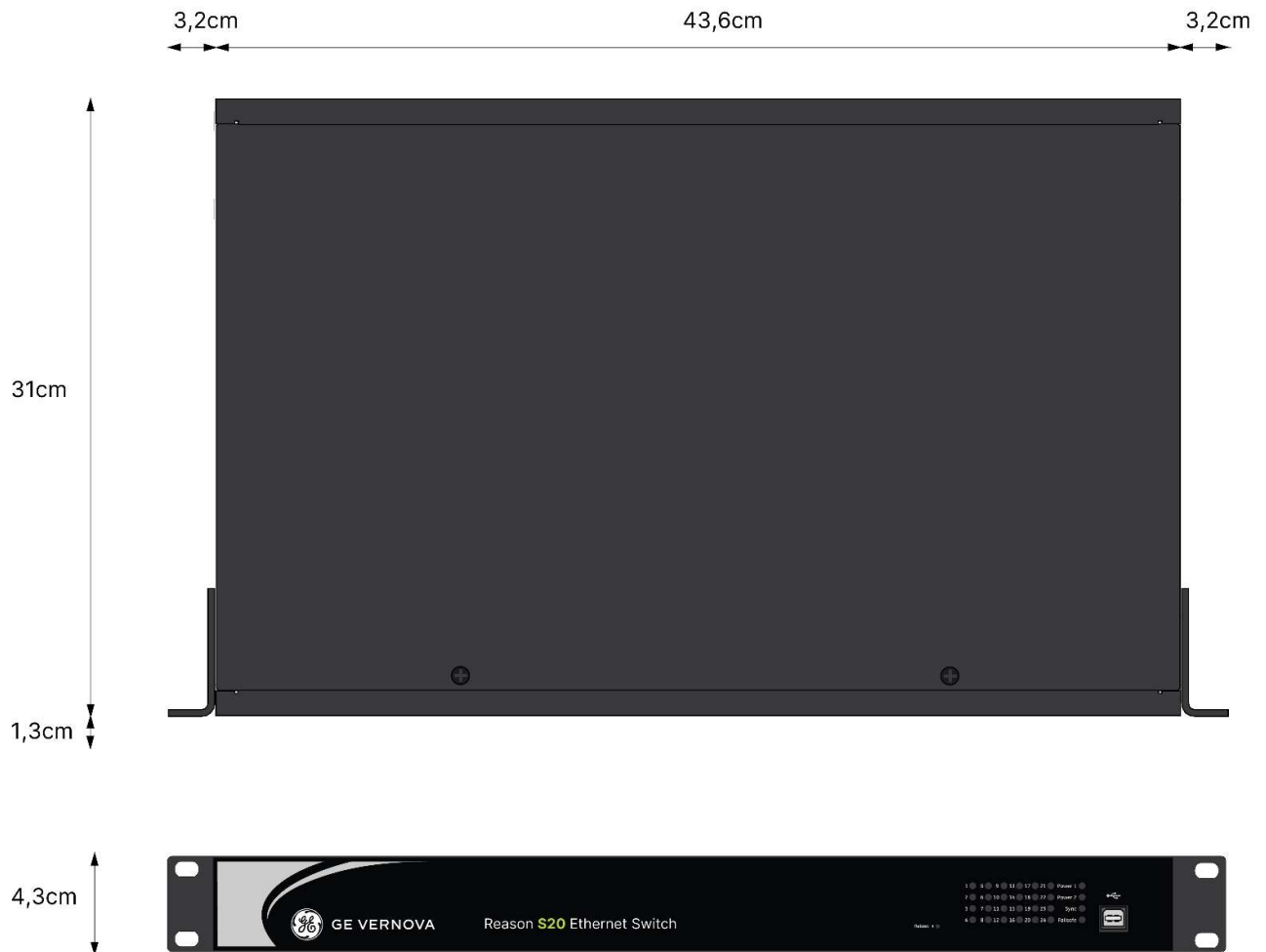


Figure 75: S20 dimensions

13 Safety Compliance

Table 20: Safety Tests

Standard	Test Description	Test Level	
UL 60950-1	General Safety Requirements	Recognized File number E484801	
IEC 60255-27	Impulse voltage	Power supply	5.0 kV
		Relay contact outputs	5.0 kV
IEC 60255-27	Dielectric Voltage (110-240 V _{AC} / 125-250 V _{DC} power supply)	Power supply	3.25 kV _{AC}
		Relay contact outputs	3.25 kV _{AC}
IEC 60255-27	Dielectric Voltage (48 V _{DC} power supply)	Power supply	1.50 kV _{DC}
		Relay contact outputs	1.50 kV _{DC}
IEC 60255-27	Insulation Resistance	> 100MΩ @ 500 VDC	

14 Environmental Tests

Table 21: Climatic Tests

Standard	Test Description	Test Level	
IEC 60068-2-1	Cold operational and storage test	Temperature	-40°C
		Duration of exposure	16 Hours
		Test Type	Ad
IEC 60068-2-2	Dry heat operational and storage test	Temperature	+85°C, 110-240 V _{AC} / 125-250 V _{DC} power supply +70°C, 48V _{DC} power supply
		Duration of exposure	16 Hours
		Test Type	Bd
IEC 60068-2-14	Change of temperature test	Lower temperature	-40°C
		Upper temperature	+55°C
		Duration of exposure	5 thermal cycles
		Dwell/recovery period	9 hours
		Steady-State period	3 hours
		Test type	Nb
IEC 60068-2-30	Cyclic temperature with humidity	Lower temperature	+25°C, ±3°C
		Upper temperature	+55°C, ±2°C
		Relative Humidity at lower temperature	97%, -2%, +3%
		Relative Humidity at upper temperature	93%, ±3%
		Duration of exposure	6 cycles of 24hs (12+12hs)
		Recovery period	1 to 2 hours
IEC 60068-2-78	Damp heat steady state	Temperature	+40°C
		Relative Humidity	93%
		Duration	10 days
		Test type	Cab

Table 22: Mechanic Tests

Standard	Test Description	Test Level	
IEC 60255-21-1	Vibration response	Class 2	
		Frequency range	10 to 150 Hz
		Cross over frequency	59 Hz
		Peak displacement before cross over	0,075 mm
		Peak acceleration after cross over	1,0 gn

		Number of sweep cycles per axis	1
IEC 60255-21-1	Vibration endurance	class 2	
		Frequency range	10 to 150 Hz
		Peak acceleration	2,0 gn
		Number of sweep cycles per axis	20
IEC 60255-21-2	Shock response	class 2	
		Peak acceleration	10 gn
		Pulse duration	11ms
		Number of pulses in each direction	3
IEC 60255-21-2	Shock withstand	class 1	
		Peak acceleration	15 gn
		Pulse duration	11 ms
		Number of pulses in each direction	3
IEC 60255-21-3	Seismic	class 2	
		Frequency range	1 to 35 Hz
		Cross over frequency	8 Hz
		Peak displacement before cross over X and Y	7,5 mm
		Peak displacement before cross over Z	3,5 mm
		Peak acceleration after cross over X and Y	2,0 gn
		Peak acceleration after cross over Z	1,0 gn
		Number of sweep cycles per axis	1

15 EMC Tests

Table 23: EMC – Emission tests

Standard	Test Description	Test Level	
CISPR 11 (below 1Gbps)	Radiated emission	Class A	
		Frequency	30 to 230 MHz
		Level	50 dB (μV/m) quasi peak at 3 m
		Frequency	230 to 1000 MHz
		Level	57 dB (μV/m) quasi peak at 3 m
CISPR 22 (above 1Gbps)	Radiated emission	Class A	
		Frequency	1 to 3 Gbps
		Level	56 dB (μV/m) average; 76 dB (μV/m) peak at 3 m
		Frequency	3 to 6 GHz
		Level	60 dB (μV/m) average; 80 dB (μV/m) peak at 3 m
CISPR 22	Conducted and radiated emission	Class A	
		Frequency	0.15 to 0.50 MHz
		Level	79 dB (μV) quasi peak; 66 dB (μV) average
		Frequency	0.5 to 30 MHz
		Level	73 dB (μV) quasi peak; 60 dB (μV) average

Table 24: EMC – Immunity tests

Standard	Test Description	Test Level	
IEC 61000-4-18	Slow damped oscillatory wave	Test Level 3	
		Frequency	100kHz and 1MHz
		Power supply (CM)	2,5 kV
		Power supply (DM)	1,0 kV
		Relay contact outputs (CM)	2,5 kV
		Relay contact outputs (DM)	1,0 kV
		Communication ports (CM)	2,5 kV
IEEE C37.90.1	1 MHz Damped oscillatory wave	Zone A	
		Power supply (CM)	2,5 kV
		Power supply (DM)	2,5 kV
		Relay contact outputs (CM)	2,5 kV
		Relay contact outputs (DM)	2,5 kV
		Communication ports (CM)	2,5 kV
IEC 61000-4-2		Test Level 4	

	Electrostatic discharge immunity	Contact discharge on conductive surface	8kV
		Contact discharge on coupling planes	8kV
		Air discharges	15kV
IEEE C37.90.3	Electrostatic discharge immunity	Zone A	
		Contact discharge on conductive surface	8kV
		Contact discharge on coupling planes	8kV
		Air discharges	15kV
IEC 61000-4-3	Radiated radio frequency magnetic field	Test Level 3	
		Electromagnetic field strength	10 V/m
		Frequency range	80 to 1000 MHz
		Modulation AM	1 kHz, 80%
		Electromagnetic field strength	10 V/m
		Frequency range	1400 to 2700 MHz
		Modulation AM	1 kHz, 80%
		Electromagnetic field strength	10 V/m
		Spot frequencies	80, 160, 380, 450, 900, 1850, 2150 MHz
IEEE C37.90.2 IEEE 1613.1	RF susceptibility test	Zone A	
		Electromagnetic field strength	20 V/m
		Frequency range	80 to 1000 MHz
		Modulation AM	1 kHz, 80%
		Electromagnetic field strength	10 V/m
		Frequency range	1000 to 3800 MHz
		Modulation AM	1 kHz, 80%
		Electromagnetic field strength	8.5 V/m
		Spot frequencies	1000 to 6000 MHz
IEC 61000-4-4	Fast transient (110-240 V _{AC} / 125-250 V _{DC} power supply)	Test Level 4 / Zone A	
		Power supply (CM)	+/- 4kV @ 5 kHz
		Relay contact outputs (CM)	+/- 4kV @ 5 kHz
		Communication ports (CM)	+/- 4kV @ 5 kHz
		Functional earth port (CM)	+/- 4kV @ 5 kHz
IEC 61000-4-4	Fast transient (48 V _{DC} power supply)	Test Level 3 / Zone B	
		Power supply (CM)	+/- 2kV @ 5 kHz
		Relay contact outputs (CM)	+/- 2kV @ 5 kHz

		Communication ports (CM)	+/- 2kV @ 5 kHz
		Functional earth port (CM)	+/- 2kV @ 5 kHz
IEEE C37.90.1	Fast transient (110-240 V _{AC} / 125-250 V _{DC} power supply)	Zone A	
		Power supply (CM/DM)	+/- 4kV @ 5 kHz
		Relay contact outputs (CM/DM)	+/- 4kV @ 5 kHz
		Communication ports (CM/DM)	+/- 4kV @ 5 kHz
		Functional earth port (CM/DM)	+/- 4kV @ 5 kHz
IEEE C37.90.1	Fast transient (48 V _{DC} power supply)	Zone B	
		Power supply (CM/DM)	+/- 2kV @ 5 kHz
		Relay contact outputs (CM/DM)	+/- 2kV @ 5 kHz
		Communication ports (CM/DM)	+/- 2kV @ 5 kHz
		Functional earth port (CM/DM)	+/- 2kV @ 5 kHz
IEC 61000-4-5	Surge (110-240 V _{AC} / 125-250 V _{DC} power supply)	Power supply, relay contact, communication ports: Test Level 4 / Zone A	
		Power supply (Line-to-Earth)	4,0 kV
		Power supply (Line-to-Line)	2,0 kV
		Relay contact outputs (Line-to-Earth)	4,0 kV
		Relay contact outputs (Line-to-Line)	2,0 kV
		Communication ports (Line-to-Earth)	4,0 kV
IEC 61000-4-5	Surge (48 V _{DC} power supply)	Power supply, relay contact, communication ports: Zone B	
		Power supply (Line-to-Earth)	2,0 kV
		Power supply (Line-to-Line)	1,0 kV
		Relay contact outputs (Line-to-Earth)	2,0 kV
		Relay contact outputs (Line-to-Line)	1,0 kV
		Communication ports (Line-to-Earth)	2,0 kV
IEC 61000-4-6	Conducted disturbance induced by radio	Test Level 3 / Zone A	
		Power supply, relay contact, ground, communication ports	
		Level	10 V
		Frequency range	150 kHz to 80 MHz
		Spot frequencies	27 and 68 MHz
		Modulation AM	1 kHz; 80%
IEC 61000-4-8	Power frequency magnetic field	Test Level 5 / Zone A	
		Frequency	50 Hz / 60 Hz
		Continuous field	180 s
		Level	100 A/m

		Short time field	3 s
		Level	1000 A/m
IEC 61000-4-9	Pulse magnetic field	Test Level 5	
		Number of pulses in each direction	5
		Level	1000 A/m
IEC 61000-4-10	Damped oscillatory magnetic field	Test Level 5 / Zone A	
		Frequency	100 kHz
		Level	100 A/m
		Frequency	1 MHz
		Level	100 A/m
IEC 61000-4-11	AC voltage dips	Residual voltage	0%
		Duration (50/60 Hz)	1/1 cycles
		Residual voltage	40%
		Duration (50/60 Hz)	50/60 cycles
		Residual voltage	70%
		Duration (50/60 Hz)	25 / 30 cycles
		Residual voltage	80%
		Duration (50/60 Hz)	250 / 300 cycles
	AC voltage interruptions	Residual voltage	0%
		Duration (50/60 Hz)	250 / 300 cycles
IEC 61000-4-29	DC voltage dips	Residual voltage	0%
		Duration	50 ms
		Residual voltage	40%
		Duration	100 ms
		Residual voltage	70%
		Duration	100 ms
	DC voltage interruptions	Residual voltage	0%
		Duration	5 s
	DC voltage variations	Residual voltage	80, 85 and 120%
		Duration	10 s
IEC 61000-4-17	Ripple on DC input power port immunity test	Test Level 4	
		Level	15%
		Frequency	100/120 Hz
		Waveform	Sinusoidal
IEC 60255-26	Gradual shut-down/start-up (for d.c. power supply)	Shut-down ramp	60 s
		Power off	5 min
		Start-up ramp	60 s
		Test Level 3	

IEC 61000-4-12	Ring Wave (100kHz)	Power supply (CM)	2 kV
		Power supply (DM)	1 kV
		Relay contact outputs (CM)	2 kV
		Relay contact outputs (DM)	1 kV