GE VERNOVA

# Reason H49

## Instruction Manual

## PRP/HSR/QuadBox Ethernet Switches

**Publication Reference: H49/EN M/R32**

GE VERNOVA

# Contents

# 1 INTRODUCTION

## 1.1 CHAPTER OVERVIEW

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

This chapter contains the following sections:

## 1.2 FOREWORD

This technical manual provides a functional and technical description of GE Vernova's H49, 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. For further details on general protection engineering theory, we refer you to GE Vernova's publication, Protection and Automation Application Guide, which is available online or from our Contact Centre.

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 centre via:

GA.support@gevernova.com

## 1.3 PRODUCT SCOPE

The DS Agile Ethernet products and software applications are designed to meet the needs of a wide range of electrical substations. Emphasis has been placed on compliance with standards, scalability and modularity.

These features mean that the products can be used in most applications, from the most basic to the most demanding. They also ensure interoperability with other vendors.

GE Vernova provides a range of Ethernet products such as switches, which take into account the compulsory requirements of electrical substations, including power supply and immunity to environmental constraints.

GE Vernova provides solutions to specific requirements such as network redundancy management.

The products can be used independently or be integrated to form a DS Agile system, which is a Digital Control System (DCS).

### 1.3.1 KEY FEATURES

**Ports:**

- Up to 6 1Gbps ports, copper or fiber.

**Redundancy Communication Protocols:**

- Parallel Redundancy Protocol accordingly to IEC 62439-3 (2016) Clause 4 (PRP).
- High Availability Seamless Redundancy Protocol accordingly to IEC 62439-3 (2016) Clause 5 (HSR).
- PRP and HSR RedBox, HSR QuadBox and PRP-HSR coupling.

**Network Protocols:**

- Simple Network Management Protocol an Internet protocol for managing and monitoring devices on IP networks (SNMP).
- Network Time Protocol (NTP) and Precision Time Protocol (PTP) according to IEEE 1588 V2/IEC61588 Ed.2 (2009) provides highly accurate time synchronization.
- Usual secured network protocols are supported: SSH, SFTP, HTTPS. Non-secured protocols are disabled by default.

**Network Standards:**

- IEEE 802.1Q (2014): Networking standard that supports virtual LANs (VLANs) on an Ethernet network.
- IEEE 802.1p defined in IEEE 802.1Q (2014): Class of service (CoS), is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN tagged frames.
- C37.238 (2011): IEEE Standard Profile for use of PTP (Precision Time Protocol) in power system applications.

**Cyber Security:**

- NERC CIP (North American Electric Reliability Corporation - Critical Infrastructure Protection): set of requirements designed to secure the assets required for operating North America's bulk electric system.
- IEEE 1686 (2013): Standard for IED Cyber security capabilities.
- WIB 2.0: Process industry security standard; Working-party on Instrument Behavior. The main parts of theWIB requirements will be merged under the roof of IEC 62443 Industrial Network and System Security.
- CIS: Hardened following Center for Internet Security recommendations.

**Safety and Environment:**

- IEC 61850-3 (2013): General requirements for communication networks and systems for power utility automation.
- IEC 60255-27 (2013): Product safety requirements for measuring relays and protection equipment.
- IEEE 1613 (2009): Environmental and testing requirements for communications networking devices installed in electric power substations.
- IEEE 1613-1 (2013): Environmental and testing requirements for communications networking devices installed in transmission and distribution facilities.

## 1.3.2 ORDERING OPTIONS

| Variants | Order Number | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Model Type** | | 1 - 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| H49 IEC61850 HSR/PRP Switch | Reason | H49 | | | | | | | | | | | | |
| **Port 1** | | | | | | | | | | | | | | |
| None | | | 0 | | | | | | | | | | | |
| One 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km | | | A | | | | | | | | | | | |
| One 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km | | | B | | | | | | | | | | | |
| One 1 Gbps RJ45 copper 100BASE-TX/1000BASE-T Ethernet ports | | | C | | | | | | | | | | | |
| One 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km | | | D | | | | | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 2 km | | | E | | | | | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 15 km | | | F | | | | | | | | | | | |
| **Port 2** | | | | | | | | | | | | | | |
| None | | | | 0 | | | | | | | | | | |
| One 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km | | | | A | | | | | | | | | | |
| One 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km | | | | B | | | | | | | | | | |
| One 1 Gbps RJ45 copper 100BASE-TX/1000BASE-T Ethernet ports | | | | C | | | | | | | | | | |
| One 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km | | | | D | | | | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 2 km | | | | E | | | | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 15 km | | | | F | | | | | | | | | | |
| **Port 3** | | | | | | | | | | | | | | |
| None | | | | | 0 | | | | | | | | | |
| One 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km | | | | | A | | | | | | | | | |
| One 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km | | | | | B | | | | | | | | | |
| One 1 Gbps RJ45 copper 100BASE-TX/1000BASE-T Ethernet ports | | | | | C | | | | | | | | | |
| One 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km | | | | | D | | | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 2 km | | | | | E | | | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 15 km | | | | | F | | | | | | | | | |
| **Port 4** | | | | | | | | | | | | | | |
| None | | | | | | 0 | | | | | | | | |
| One 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km | | | | | | A | | | | | | | | |
| One 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km | | | | | | B | | | | | | | | |
| One 1 Gbps RJ45 copper 100BASE-TX/1000BASE-T Ethernet ports | | | | | | C | | | | | | | | |
| One 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km | | | | | | D | | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 2 km | | | | | | E | | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 15 km | | | | | | F | | | | | | | | |
| **Port 5** | | | | | | | | | | | | | | |
| None | | | | | | | 0 | | | | | | | |
| One 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km | | | | | | | A | | | | | | | |
| One 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km | | | | | | | B | | | | | | | |
| One 1 Gbps RJ45 copper 100BASE-TX/1000BASE-T Ethernet ports | | | | | | | C | | | | | | | |
| One 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km | | | | | | | D | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 2 km | | | | | | | E | | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 15 km | | | | | | | F | | | | | | | |
| **Port 6** | | | | | | | | | | | | | | |
| None | | | | | | | | 0 | | | | | | |
| One 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0.5 km | | | | | | | | A | | | | | | |
| One 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km | | | | | | | | B | | | | | | |
| One 1 Gbps RJ45 copper 100BASE-TX/1000BASE-T Ethernet ports | | | | | | | | C | | | | | | |
| One 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km | | | | | | | | D | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 2 km | | | | | | | | E | | | | | | |
| One 100 Mbps LC-type connector single mode fiber 100BASE-FX Ethernet for up to 15 km | | | | | | | | F | | | | | | |
| **Reserved** | | | | | | | | | 0 | 0 | 0 | 0 | 0 | |
| **Design Suffix** | | | | | | | | | | | | | | |
| Initial Issue | | | | | | | | | | | | | | B |

# 2 SAFETY INFORMATION

## 2.1 CHAPTER OVERVIEW

This chapter provides information about the safe handling of the equipment. The equipment must be properly installed and handled 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.

This chapter contains the following sections:

## 2.2 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 energize and de-energize 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.

## 2.3 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.**

**Warning:**
**Risk of electric shock**

**Warning:**
**Risk of damage to eyesight**

Earth terminal. ***Note:*** *This symbol may also be used for a protective conductor (earth) terminal if that terminal is part of a terminal block or sub-assembly.*

Protective conductor (earth) terminal

Instructions on disposal requirements

*Note:*
*The term 'Earth' used in this manual is the direct equivalent of the North American term "Ground."*

## 2.4 INSTALLATION, COMMISSIONING AND SERVICING

### 2.4.1 LIFTING HAZARD

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.

### 2.4.2 ELECTRICAL HAZARDS

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

**Caution:**
**Consult the equipment documentation before installing, commissioning, or servicing the equipment.**

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

**Warning:**
**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.**

**Warning:**
**Isolate the equipment before working on the terminal strips.**

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

**Caution:**
**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.**

**Warning:**
**NEVER look into optical fibres or optical output connections. Always use optical power meters to determine operation or signal level.**

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

**Caution:**
**Operate the equipment within the specified electrical and environmental limits.**

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

***Note:***
*Contact fingers of test plugs are normally protected by petroleum jelly, which should not be removed.*

## 2.5 DECOMMISSIONING AND DISPOSAL

**Caution:**
**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.**

**Caution:**
**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.**

# 3 COPYRIGHTS & TRADEMARKS

## 3.1 CHAPTER OVERVIEW

This chapter provides copyrights and trademarks about the technical manual.

This chapter contains the following sections:

## 3.2 COPYRIGHTS

## 3.3 TRADEMARKS

GE Vernova, the GE Vernova logos and any alternative version thereof are trademarks and service marks of GE Vernova. The other names mentioned, registered or not, are the property of their respective companies.

# 4 FUNCTIONAL DESCRIPTION

## 4.1 CHAPTER OVERVIEW

This chapter provides information about the product's hardware design and available functions.

This chapter contains the following sections:

## 4.2 HARDWARE

The following sections show different views of the device and its components.



### 4.2.1 FRONT PANEL

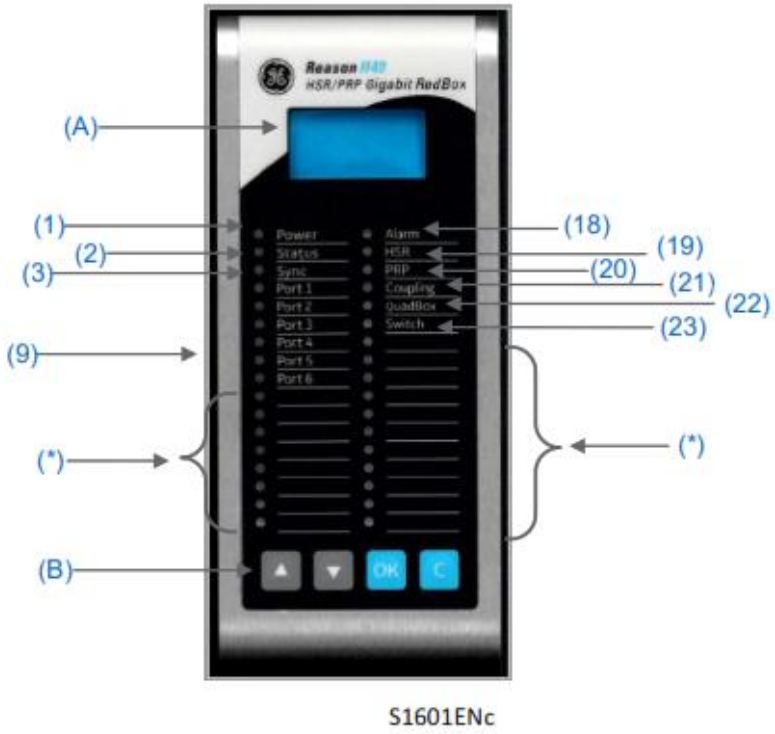



**Figure 1: Reason H49 Front View**

The front panel of the Reason H49 switch contains the following items:

| Item | Description |
|---|---|
| A | Liquid crystal display (LCD) with 4 lines of 16 characters:<br>Line 1: Empty<br>Line 2: H49<br>Line 3: IP address (255.255.255.255)<br>Line 4: Empty |
| B | Navigation buttons to access and browse the test menu. |

Reason H49 is configured through the web application user interface (detailed later in this document) or using configuration file.

### Signification of the LEDs

Light Emitting Diodes (LEDs) and alarm contacts indicate the status of the product and its ports:

| LED rank | Signification | Color | Description | Activity |
|---|---|---|---|---|
| 1 | **Power**<br>1 LED | Green | Powered on | |
| | | Off | Switch is off | |
| 2 | **Operating state**<br>1 LED (boot, ok, alarm) | Amber (default) | As long as the CPU board has not booted. | |
| | | Green | Healthy (board works, no contact alarm) | |
| 3 | **Time Synchronization**<br>1 LED | Green | PTP or NTP synchronization | |
| | | Red | No synchronization or Switch in Grandmaster | |
| 4 to 9 | **Port activity**<br>6 LEDs | Green | 1Gbits/s | |
| | | Amber | 100Mbits/s | |
| | | Red | Not forwarding (access violation, wrong MAC address) | |
| | | | No traffic | On |
| | | | Signs of activity | Blinking |
| | | | Not plugged or disabled by configuration | Off |
| 18 | **Alarm**<br>1 LED | Red (default) | Power redundancy alarm | |
| 19 | **HSR RedBox**<br>1 LED | Green | | |
| 20 | **PRP RedBox**<br>1 LED | Green | | |
| 21 | **PRP-HSR Coupling**<br>1 LED | Green | | |
| 22 | **HSR QuadBox**<br>1 LED | Green | | |
| 23 | **Standard Switch**<br>1 LED | Green | | |

| LED rank | Signification | Color | Description | Activity |
|---|---|---|---|---|
| * | | Alternatively LED chaser, Red, Green and Amber | LED chaser | |

### 4.2.2 BOTTOM VIEW

Reason H49 is a 6-port switch, supporting any combination of 100Mbps and 1Gbps RJ45 copper or LC optical fiber ports. The following figure presents the bottom view of the device together with its components.

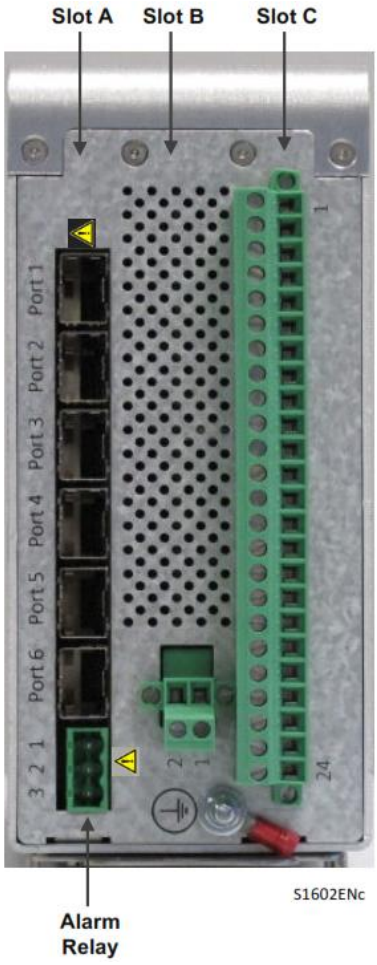



**Figure 2: Reason H49 bottom view**

Multi-mode SFP transceivers are used for connections up to 2km, and single-mode SFP transceivers can be used for distances up to 15km.

### Description of the slots

| Slot | Board | Description |
|---|---|---|
| A | SRPV3 | **Communication port:**<br>Port 1 to port 6: SFP transceiver optical/copper |
| | | **Alarm Relay Connector:**<br>Pin 1: Normally open<br>Pin 2: Common<br>Pin 3: Normally Closed |
| B | BIU261D | **Secondary Power Supply:**<br>Pin 2: In-<br>Pin 1:In+ |
| C | BIU261D | **Primary Power Supply:**<br>Pin1 to Pin21: Not Connected<br>Pin22: Earth<br>Pin23: In+<br>Pin24: In- |

## 4.3 PARALLEL REDUNDANCY PROTOCOL

The Parallel Redundancy Protocol (PRP) is implemented according to the definition in the standard IEC 62439-3 (2016) Clause 4.

PRP allows seamless switchover and recovery in case of network disruption (for instance cable, driver, switch or controller failure).

A PRP compatible device has two ports operating in parallel, each port being connected to a separate local area network (LAN) segment. IEC 62439-3 (2016) Clause 4 assigns the term DANP (Doubly Attached Node running PRP) to such devices. Critical devices should be doubly attached using two ports. The two LANs have no connection between them and are assumed to be fail-independent.

A source DANP sends the same frame over both LANs and a destination DANP receives it from both LANs within a certain time, consumes the first frame and discards the duplicate. In the following figure, DANP1 and DANP2 implement this redundancy.

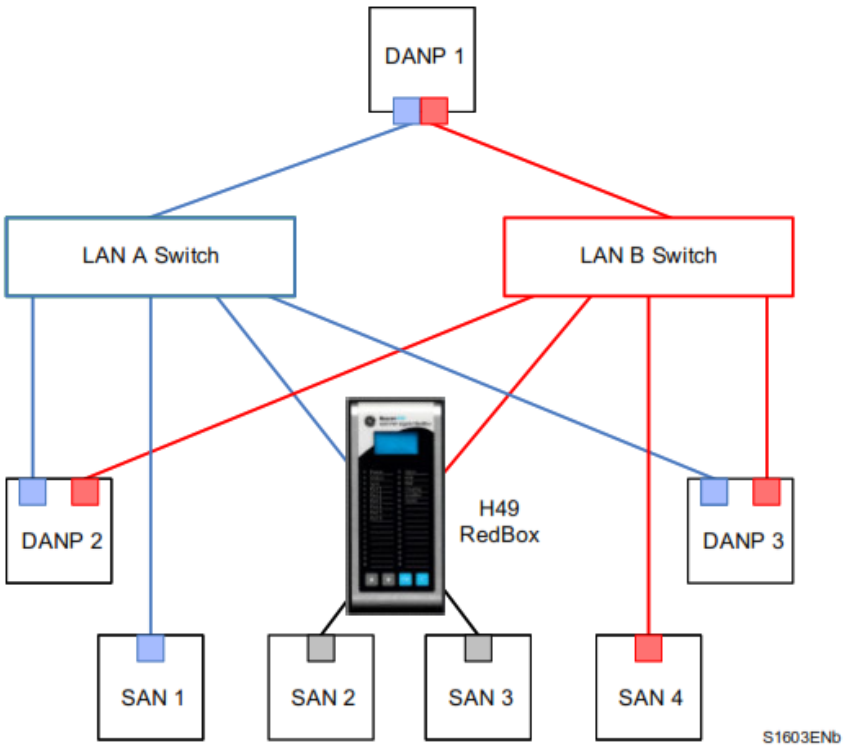



**Figure 3: Example PRP Redundant Network**

Singly Attached Nodes (SAN) are connected to only one LAN (see SAN 1 and SAN 4 in previous figure) and they do not implement any redundancy. They can, however, be connected to both LANs, via the Reason H49 switch that converts a singly attached node into a doubly attached node. It acts as a redundancy box or RedBox.

Devices with single network cards such as personal computers, printers, etc., are singly attached nodes that may be connected into the PRP network via a RedBox as shown in the following figure.

This is the case for SAN2 and SAN3. Because these SANs connect to both LANs, they can be considered as Virtual Doubly Attached Nodes and described as VDANs.

Reason H49 can be configured as PRP RedBox and connect up to four SANs to the PRP network as shown in the following figure:

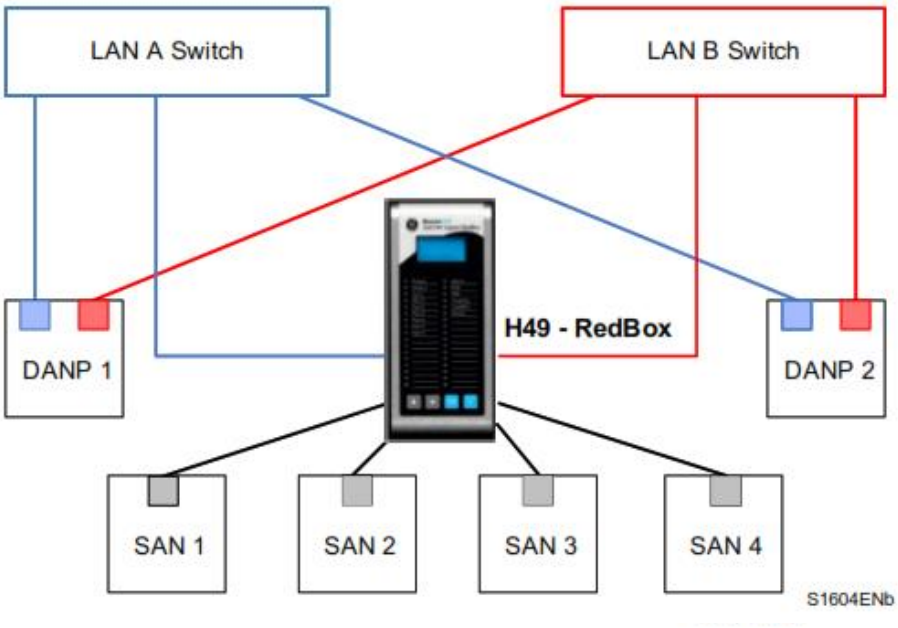



**Figure 4: Reason H49 connecting four SANs to the PRP Network**

## 4.4 HIGH-AVAILABILITY SEAMLESS REDUNDANCY (HSR) PROTOCOL

The HSR protocol is implemented accordingly to IEC 62439-3 (2016) Clause 5.

HSR allows seamless communication in case of a single network disruption (for instance cable, driver, switch or controller failure).

An HSR-compatible device has two ports operating simultaneously, both ports being connected to the same LAN. IEC 62439-3 (2016) Clause 5 assigns the term DANH (Doubly Attached Node running HSR) to such devices. Reason H49 is a DANH.

The figure below shows an example of an HSR network. The doubly attached nodes HSR RedBox, DANH 1 and DANH 2 send and receive HSR frames in both directions, while the singly attached nodes SAN 1 and SAN 2 can only send and receive frames without HSR header.

Singly attached nodes can, however, be connected to HSR ring, via a device which converts a singly attached node into a doubly attached node. Devices performing this function are often referred to as redundancy boxes or RedBoxes. Thus, devices with single network cards such as personal computers, printers, etc., are singly attached nodes that may be connected to the HSR network via a RedBox as shown in the figure.

Because these SANs are connected to the HSR network, they can be considered as Virtual Doubly Attached Nodes and described as VDANs.

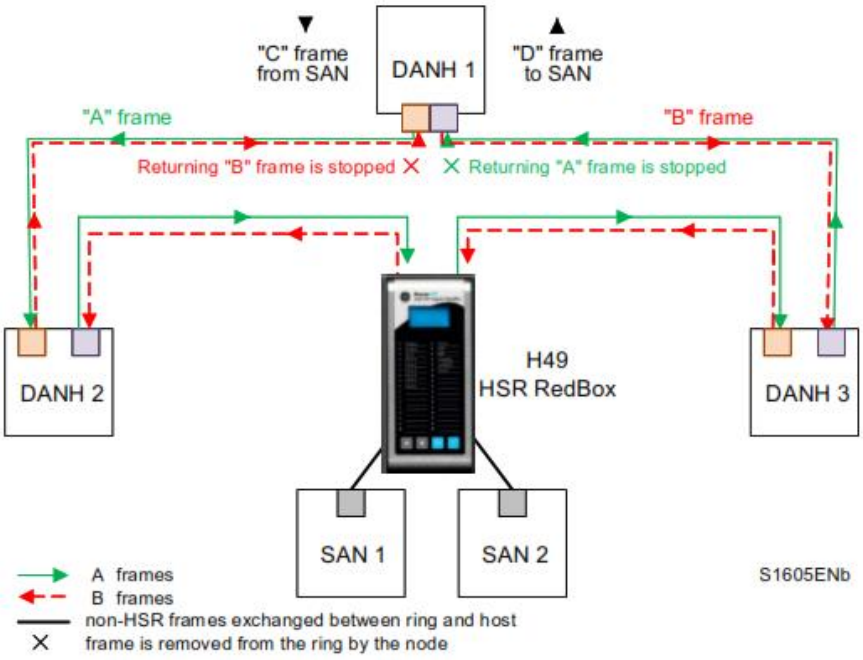



**Figure 5: Example HSR Redundant Network**

HSR is based on a ring-type architecture to achieve its network path redundancy. Duplicate packets, identified as "A" and "B", are sent in opposite directions of the ring to achieve redundancy down to the packet level. When a packet arrives at a DANH node, the node will determine if the packet is addressed to it or to another destination.

- If the packet is addressed to the node, then:
  - It will process it or
  - It will discard it if it is a duplicate packet
- If the packet is for another destination, then
  - If the DANH device receives a frame that it originally sent, it does not forward it
  - Otherwise, it will simply forward the packet on to the next node in the network. Frames sent by a SAN device (see "C" frames in the following figure) are converted into two "A" and "B" frames and sent over the HSR network.

Received frames that are addressed to a SAN managed by a Redbox (such as MMS messages) are not forwarded on to the HSR network.

There are two basic operation principles, depending on whether the broadcasted frames are multicast (e.g., GOOSE) or unicast (e.g., MMS reports).

- **Multicast (e.g., GOOSE)**: A source DANH sends a frame over both ports ("A"-frame and "B"-frame). The destination DANH receives, in a fault-free state, two identical frames from each port within a certain interval, passes the first frame on to its higher layers. A source DANH discards any duplicate multicast frame from the ring.
- **Unicast (e.g., REPORT)**: A destination node of a unicast frame does not forward a frame for which it is the only destination. It removes the unicast frame from the ring.

## 4.5 HSR QUADBOX

It is possible to connect two HSR rings when the traffic flow exceeds the capabilities of a single ring. However, transmission delays from end to end are not improved. This connection is possible thanks to quadruple port devices with forwarding capabilities called QuadBoxes as shown in the following figure.

Although one QuadBox is sufficient to forward traffic, two QuadBoxes are used to prevent a single point of failure. A QuadBox forwards frames over each ring as any HSR node, and passes the frames unchanged to the other ring, except if the frame can be identified as a frame not to be forwarded to the other ring. To this effect, a QuadBox is expected to filter traffic based for instance on multicast filtering or on VLAN filtering. There is no learning of MAC addresses in a QuadBox, though, since the learning of MAC addresses on specific ports of a QuadBox device could lead to a short break in communication if the QuadBox that has learned an address and is forwarding network traffic fails.

With QuadBoxes realized as single physical entities, the two interconnected rings share the same redundancy domain concerning fault tolerance. If one QuadBox breaks down, both interconnected rings are in a degraded state and cannot tolerate a further fault.

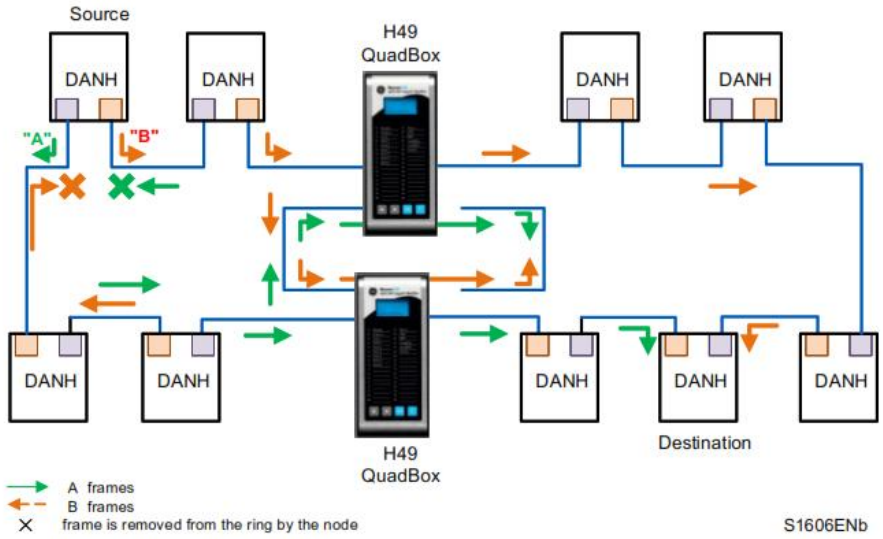



**Figure 6: Two QuadBoxes linking two HSR Rings**

The presence of two QuadBoxes on the same ring causes that two copies of the same frame are transferred from the first ring to the second, each generating other two copies.

This does not cause four frames to circulate on the second ring, since, when a copy from a first QuadBox reaches the second QuadBox on the same second ring, the second QuadBox will not forward it if it already sent a copy that came from its interlink.

Conversely, if the second QuadBox did not yet receive a copy from its interlink, it will forward the frame, but not the copy that comes later from the interlink.

When a QuadBox receives a frame that it itself injected into the ring or a frame that the other QuadBox inserted into the ring, it forwards it to the interlink and to its other port if it did not already send a copy. This duplicate will be discarded at the other end of the interlink. This scheme may cause some additional traffic on the interlink, but it allows to simplify the design of the logic.

> ***Note:***
> *The maximum time skew between two frames of a pair is about the same as if all nodes were on the same ring.*

## 4.6 PRP-HSR COUPLING

An HSR network may be coupled to a PRP network through two RedBoxes, one for each LAN as shown in the figure here below. In this case, the RedBoxes are configured to support PRP traffic on the interlink and HSR traffic on the ring ports.

The sequence number from the PRP RCT is reused for the HSR tag and vice versa, to allow frame identification from one network to the other and to identify pairs and duplicates on the HSR ring, introduced by a twofold injection into the ring through the two HSR RedBoxes.

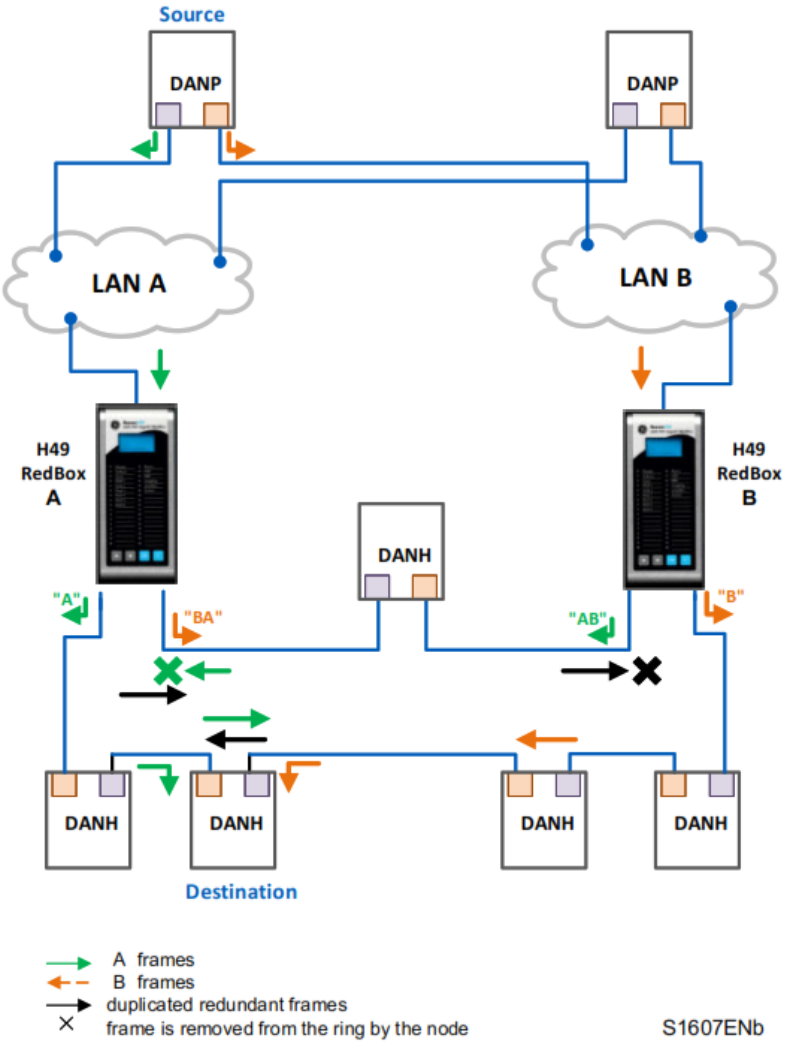



**Figure 7: Coupling two PRP LANs to an SRS Ring**

The HSR RedBoxes for connecting the ring to a PRP network operate identically to those used to attach SANs, except that they are configured as RedBox "A" or RedBox "B" to accept PRP frames on their interlink. In the figure here above, RedBox A and RedBox B would send the same frame (A and AB, respectively B and BA), but if a RedBox receives the frame before it could send it itself, it refrains from sending it.

In the figure here above, RedBox A will not generate an "A" frame on behalf of LAN A if it previously received the same frame as "AB" from the ring, or conversely, RedBox "B" will generate an "AB" frame if it did not previously receive an "A" frame from the ring, which is the case whenever frame "A" is not a multicast frame.

Multicast frames or unicast frames without a receiver in the ring (see figure here above) are removed by the RedBox that inserted them into the ring, if they originated from outside the ring.

The following figure shows the same coupling when the source is within the ring.

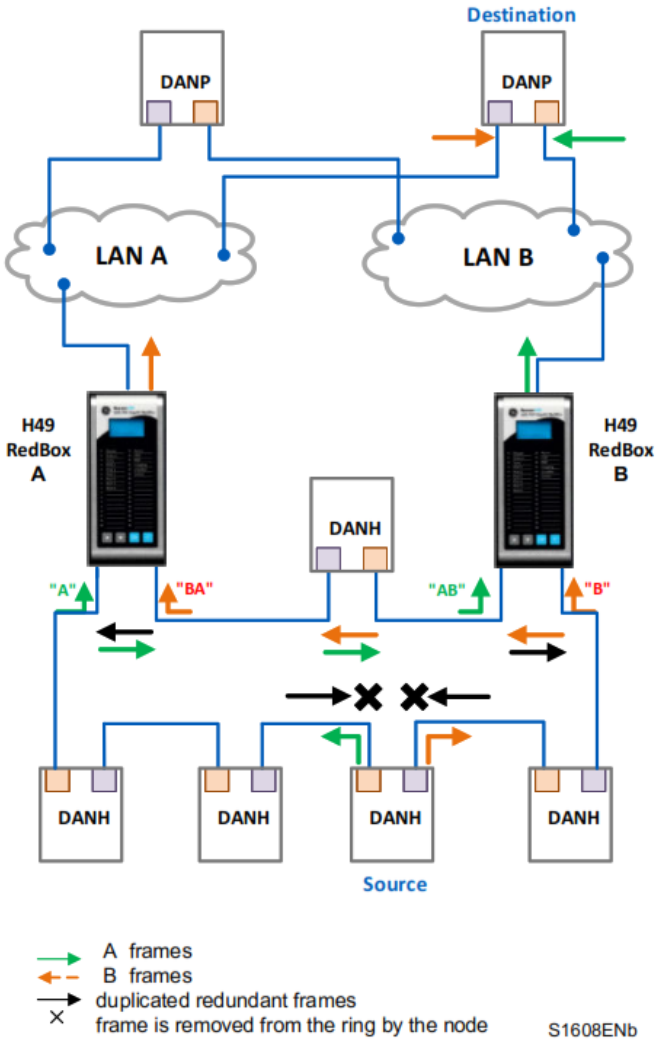



**Figure 8: Coupling an HSR Ring to two PRP LANs**

To avoid reinjecting a frame into the PRP network through the other RedBox, each HSR frame carries the identifier of the PRP network from which the frame came originally. Therefore, RedBoxes are to be configured with the NetId of the PRP network to which they are attached.

Other combinations of PRP and HSR networks are allowed. Some of them are explained in the following sections.

### 4.6.1 CONNECTING SEVERAL PRP NETWORKS TO AN HSR RING

A **maximum of 6 PRP networks** can be connected to an HSR ring, each being identified by a 3-bit netId.

The two RedBoxes that connect a PRP network with an HSR ring are configured with the NetId (1..7) and the LanId (A=0/B=1), see the following figure.

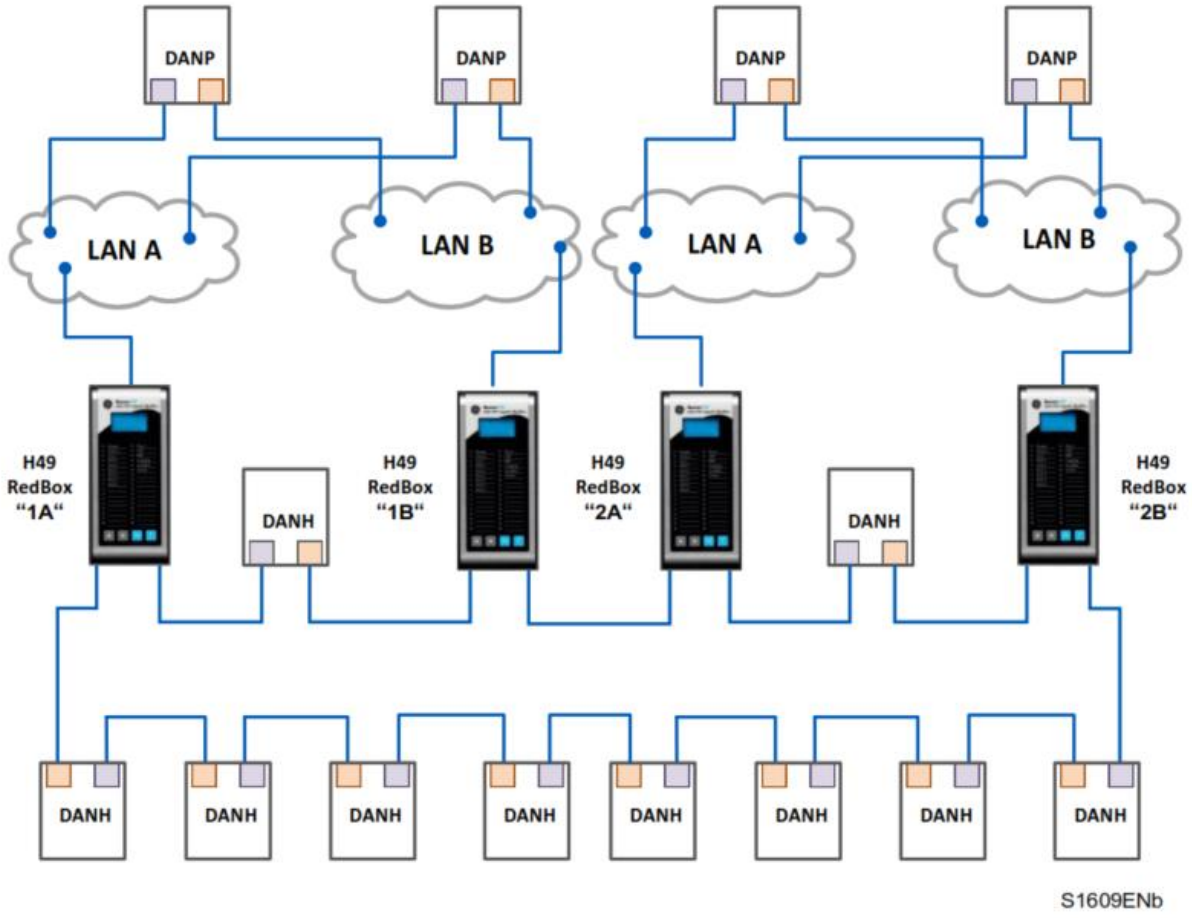



**Figure 9: Coupling one HSR ring to several PRP Networks**

To prevent reinjection of frames coming from one PRP network into another PRP network or from the same, a RedBox only forwards from the HSR ring frames that do not carry its own NetId. When inserting into the ring a PRP frame from LAN A or from LAN B of a PRP network with a given NetId, a RedBox inserts into the PathId of the HSR tag its own NetId and the LanId, i.e. one of "2"/"3", "4"/"5", "6"/"7", "8"/"9", "A"/"B", "C"/"D" or "E"/"F", depending if it is RedBox A or B.

Conversely, when forwarding a frame from the ring to a PRP network, a RedBox insert the LanId "A" or "B" into the RCT, depending if it is RedBox A or RedBox B.

### 4.6.2 CONNECTING ONE PRP NETWORK TO SEVERAL HSR Rings

A PRP network can be connected to any number of HSR rings, but these rings cannot be connected between themselves, neither by QuadBoxes nor by another PRP network since this would create loops.

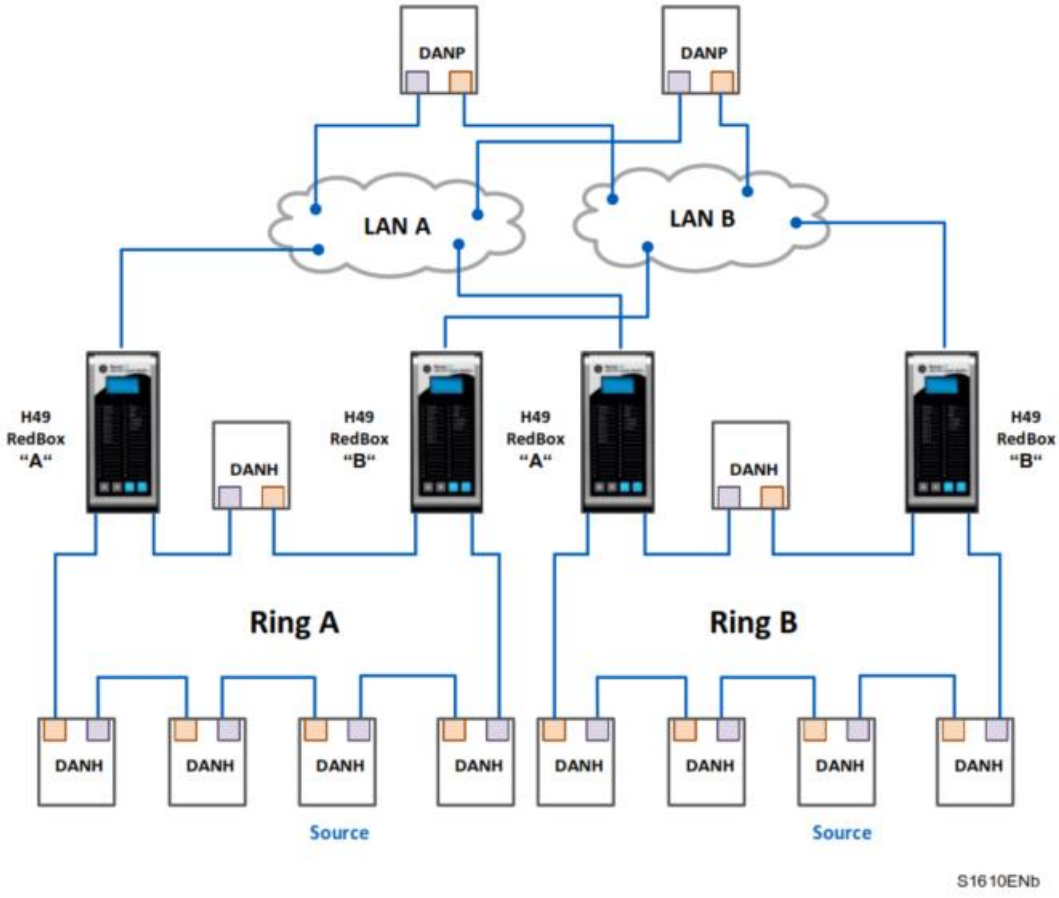



**Figure 10: Coupling Several HSR Rings to a PRP Network**

## 4.7 STANDARD SWITCH

Reason H49 can be configured as a standard Ethernet Switch. In this case, it manages up to six Ethernet ports.

**Reason H49 using auto-negotiation:**

- Automatically determines the speed of transmission on the 10/100/1000 Base ports according to the following standards:
  - IEEE 802.3u – 100BaseTX, 100BaseFX.
  - IEEE 802.3ab – 1000BaseTX
  - IEEE 802.3z – 1000BaseLX, 1000BaseSX
- Determines whether communication is half-duplex or full-duplex and adapts accordingly.

**Addressing:**

- Each Ethernet device inserts its unique "MAC address" into each message it sends.
- The receiving port automatically recognizes the MAC address in a received frame and stores it.
- Once an address is recognized and stored, the switch will forward frames to the appropriate port.

- Up to 512 MAC addresses can be stored and monitored at any time.

## 4.8 TIME SYNCHRONIZATION

Reason H49 supports real-time clock synchronization for the timestamp of logs or events through the following network protocols:

- Precision Time Protocol (PTP in accordance with IEEE/IEC 61588 (2009))
- Network Time Protocol (NTP)

The time protocol used is independent of the network architecture (HSR or PRP). Thus, the time server can be placed in either the HSR ring or one of the PRP LANs.

It is important to emphasize that the time server shall be placed in a VDAN device; in other words, it shall be linked to the network through a RedBox.

***Note:***
*The Reason H49 switch does not support Spanning Tree Protocol (STP, RSTP, MSTP).*

### 4.8.1 PRECISION TIME SYNCHRONIZATION (PTP)

Time synchronization from a master clock synchronized to the global positioning satellite (GPS) system is accepted over the network according to IEEE/IEC61588 Ed.2. (2009).

PTP synchronizes all clocks within a network by adjusting distributed clocks to a grandmaster clock. PTP enables distributed clocks to be synchronized and maintained to sub-microsecond accuracy.

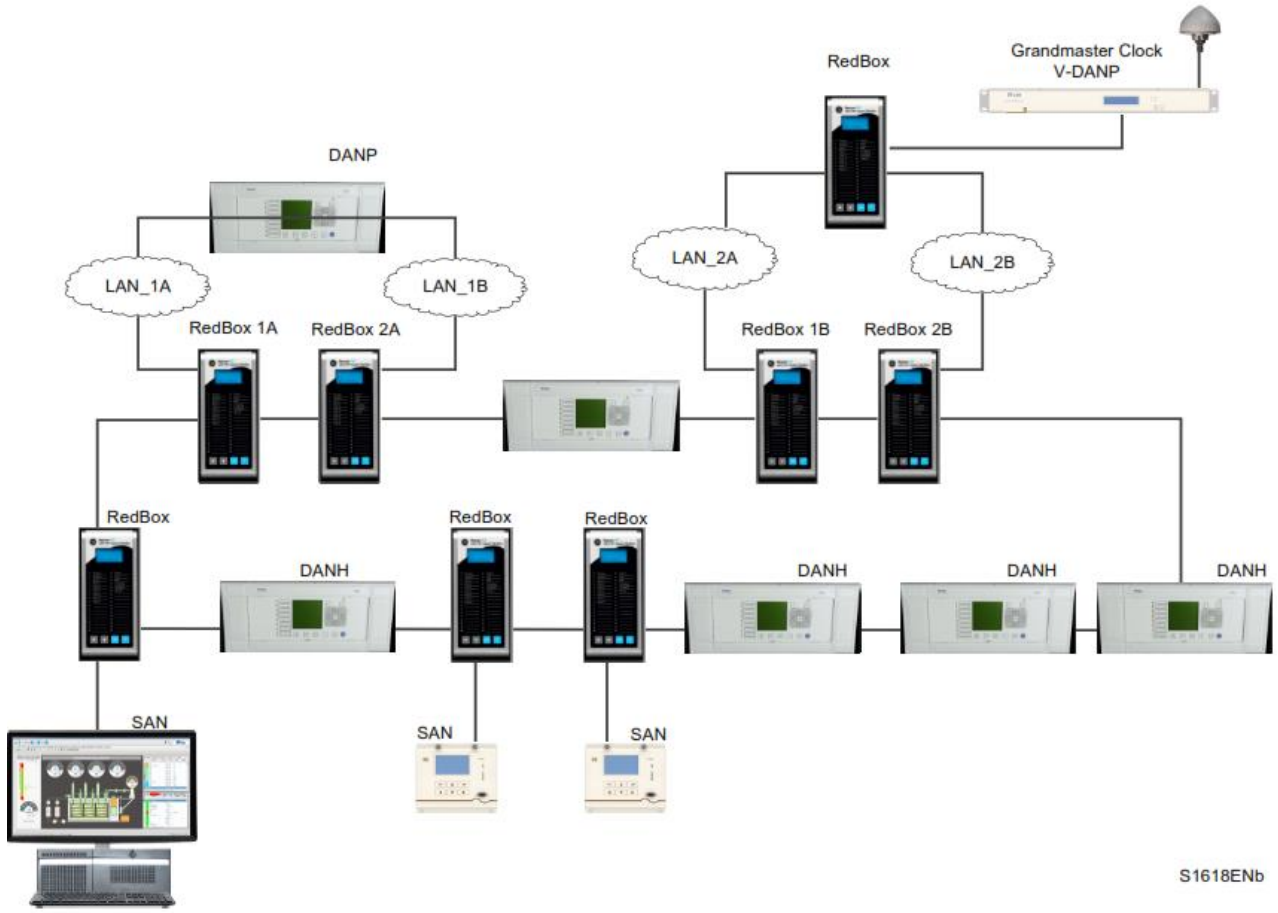



**Figure 10: Example of PRP/HSR Architecture with the Precision Time Protocol (PTP)**

***Note:***
*On PTP protocol, a time discrepancy of 60 milliseconds per 24h is reported on Reason H49 (equipped with a SRPv3 version x) and used as Master Clock (M1) (case VDAN-P Grandmaster Clock not available).*

### 4.8.2 NTP TIME SYNCHRONIZATION

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

Reason H49 supports NTP as shown in the figure below.

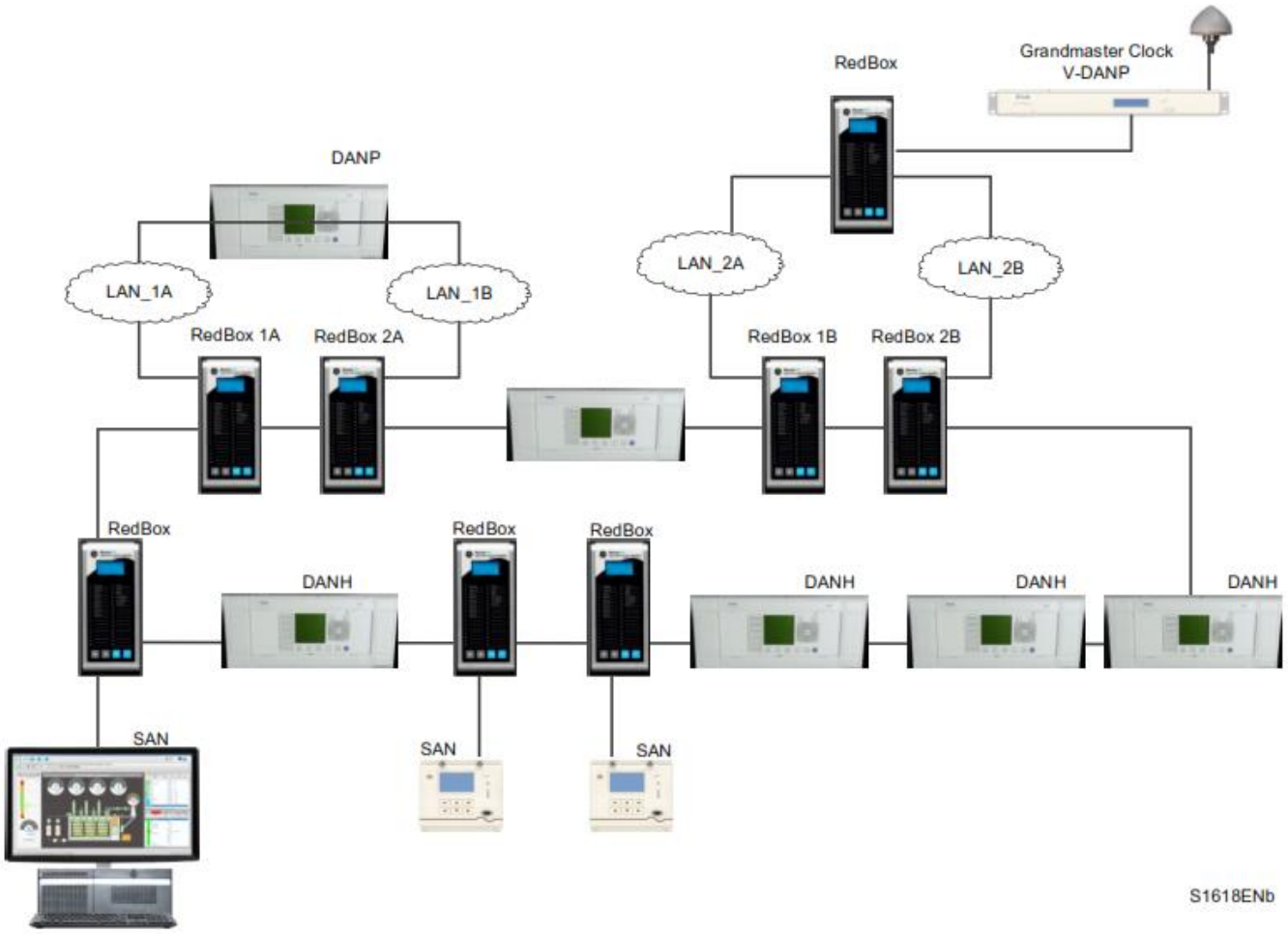



**Figure 11: Example of NTP Synchronization**

#### 4.8.2.1 TIME ZONE

The internal clock of Reason H49 can be synchronized using NTP protocol, which sends the UTC time (Greenwich Mean Time). When using the equipment in other regions, the time zone may be set manually to correct the internal clock.

## 4.9 SNMP

Simple Network Management Protocol (SNMP) is the network protocol developed to manage devices on an IP network.

To exchange information, SNMP relies on a **Management Information Base (MIB)** that contains information about parameters to supervise. A MIB format is a tree structure, with each node identified by a numerical Object Identifier (OID). Each OID identifies a variable that can be read or set via SMP with the appropriate software.

### 4.9.1 SUPPORTED MIB

The SNMP MIB consists of distinct OIDs, each of which refers to a defined collection of specific information used to manage devices over the network.

GE Vernova management information bases (MIB) use the following types of object identifiers (OID):

- BRIDGE-MIB (RFC 1493)
- SNMPv2-MIB (RFC 1907)
- TCP-MIB (RFC 2012)
- UDP-MIB (RFC 2013)
- SNMPv2-SMI (RFC 2578)
- SNMPv2-TC (RFC 2579)
- RMON-MIB (RFC 2819)
- IF-MIB (RFC 2863)
- PRP/HSR MIB (IEC 62439-3)
- Power Profile MIB (IEEE C37.238)

#### 4.9.1.1 GET MIB FILES

The MIB files supported by the H49 are included in release delivery package. To get the MIB files, the following prerequisites must be observed.

- Windows operating system
- 7-zip application
- H49 Release delivery package

1. Unzip the H49 release delivery package.

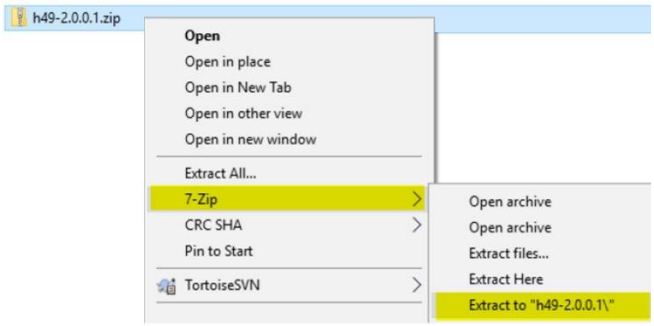



**Figure 12: Release delivery package Zip**

2. Open the H49 unzipped folder:

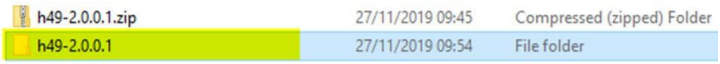



**Figure 13: Unzipped folder**

3. Unzip the *.tar.gz file to folder *.tar:

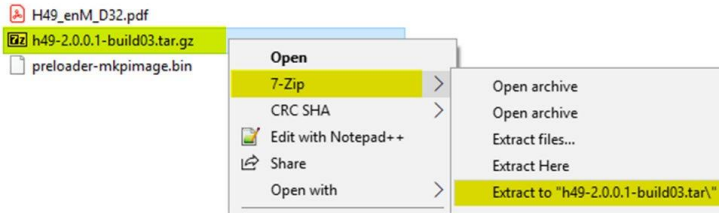



**Figure 14: Unzipped *.tar folder**

4. From the unzipped folder, unzip the *.tar file:

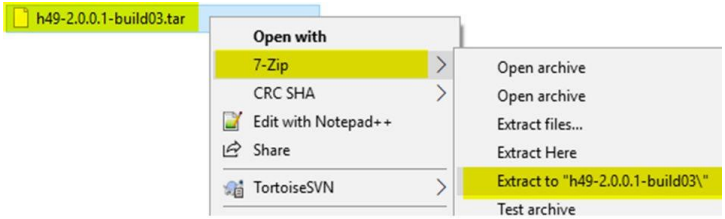



**Figure 15: Unzipped *.tar folder**

5. Open the unzipped folder to find MIB folder:

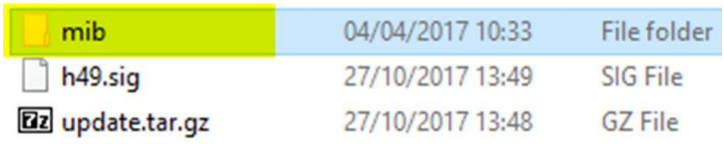



**Figure 16: MIB folder**

6. MIB files available in the MIB folder:


**Figure 17: MIB files**

MIB files can be imported in a MIB browser application in order to get the H49 exposed SNMP information.

Based on these MIB files, the MIB browser application will display the H49 SNMP OID detailed information as well as their functional description.

To get all H49 information, SNMPv3 must be used.

### 4.9.2 SNMP TRAPS

The SNMP agent in the Reason H49 switch can send SNMP traps to the management station. Traps are change-of- state messages alerting the SNMP manager to a condition on the network. A trap message is sent to alert the management station to some event or condition on the switch such as:

- Loss of communication on one port
- Loss of power supply input
- Loss of time synchronization (PTP)
- Resource exhaustion

## 4.10 PORTS/INTERFACES NAMING CONVENTION

Depending on the context of use (WebApp, CLI commands, Device) the H49 interfaces/ports might have different names (e.g.: port1 – X1 – CE01) but they all refers to same entity. The names are described in the matching table below.

Port-Interface name matching table:

| Physical Ports Name | WebApp Port Interface Name | CLI Port Interface name (used in logs)(message) |
|---|---|---|
| Port 1 | X1 | CE01 |
| Port 2 | X2 | CE02 |
| Port 3 | X3 | CE03 |
| Port 4 | X4 | CE04 |
| Port 5 | X5 | CE05 |
| Port 6 | X6 | CE06 |
| N/A | N/A | SE01 |

***Note:***
***SE01*** *refers to the internal switch port/interface.*

# 5 INSTALLATION

## 5.1 CHAPTER OVERVIEW

This chapter provides information about the product's installation.

This chapter contains the following sections:

## 5.2 DIMENSIONS

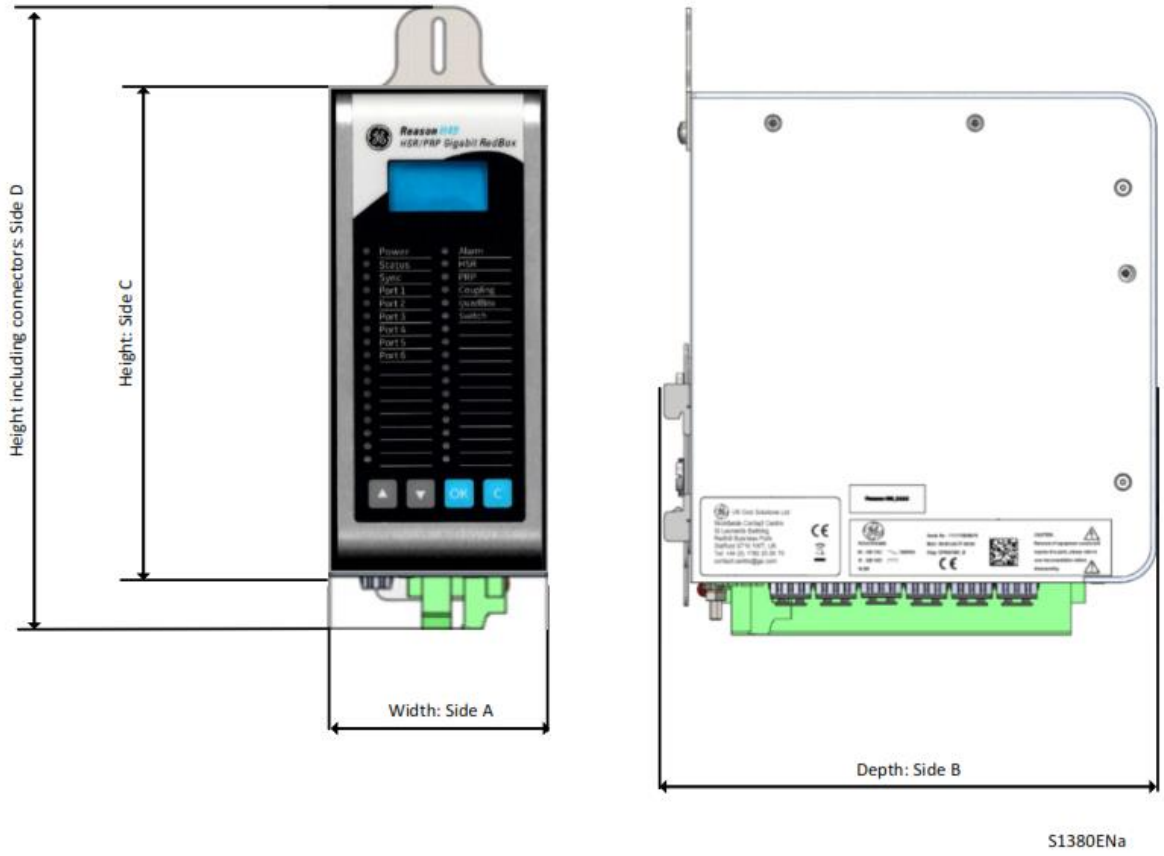



**Figure 18: Front Face and side with dimensions**

### H49 dimensions:

| Item | Unit | Min | Max |
|---|---|---|---|
| Width: Side A | mm | 74.8 | 75.2 |
| Depth: Side B | mm | 175.14 | 177.26 |
| Height: Side C | mm | 175.8 | 176.2 |
| Height: Side D | mm | 224.12 | 226.12 |

## 5.3 DEVICE LABELING

The figure below shows an example of the standard labels stuck to the Reason H49 switch:

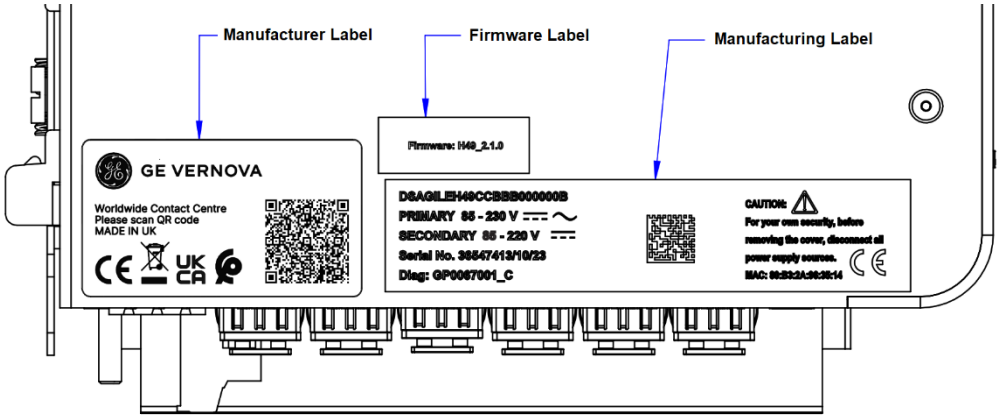



**Figure 19: Example of Device Labeling**

Main information present in these labels includes:

- Company
- Product name
- Cortec code
- Voltage range
- Serial number
- Caution notice
- Firmware version
- MAC address

The following tables give the details of the label components.

### 5.3.1 MANUFACTURING LABEL

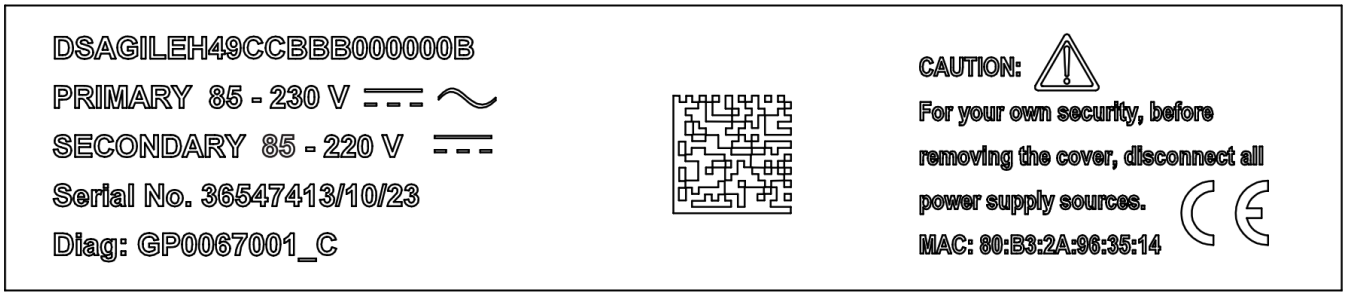



**Figure 20: Manufacturing Label**

| Manufacturing Label |
|---|
| Label 20x94mm |
| Diagram number: |
| GP0067001_B |
| Reference of the product: GP0067001<br>Version of the product: B |
| Serial number: |
| 11111158/06/16 |
| Unique serial number: 8 numerical digits: 11111158<br>Date of manufacturing /MM/YY: /06/16 |
| Barcode content description:<br>DSAGILEH4900000000000B_11111158_80B32AFF0000<br>Cortec number: DSAGILEH4900000000000B<br>Serial number without the manufacturing date: 11111158<br>MAC Address: 80B32AFF0000 |

### 5.3.2 FIRMWARE LABEL


**Figure 21: Firmware Label**

| Firmware Label |
|---|
| Label 10x27mm |
| Firmware version: H49_2.0.0.0<br>Name of the product: H49<br>First digit: Major functional version (2)<br>Second digit: Compatibility indicator version (0)<br>Third digit: Maintenance/Evolution/Bug fix version (0)<br>Fourth digit: Second level maintenance version (0) |

***Note:***
*Firmware label is given as an example. Check last issue of datapack for correct firmware label.*

### 5.3.3 MANUFACTURER LABEL


**Figure 22: Manufacturer Label**

| Manufacturer Label |
| --- |
| Label 28x50mm<br>Font: Alstom regular, black |
| Content: manufacturer contact information |

## 5.4 MOUNTING

Reason H49 is designed to be mounted **vertically** on a standard DIN Rail. For this purpose, two adjustable mounting brackets are located on the back of the H49, one at the top and one at the bottom of the rear face, as shown below:

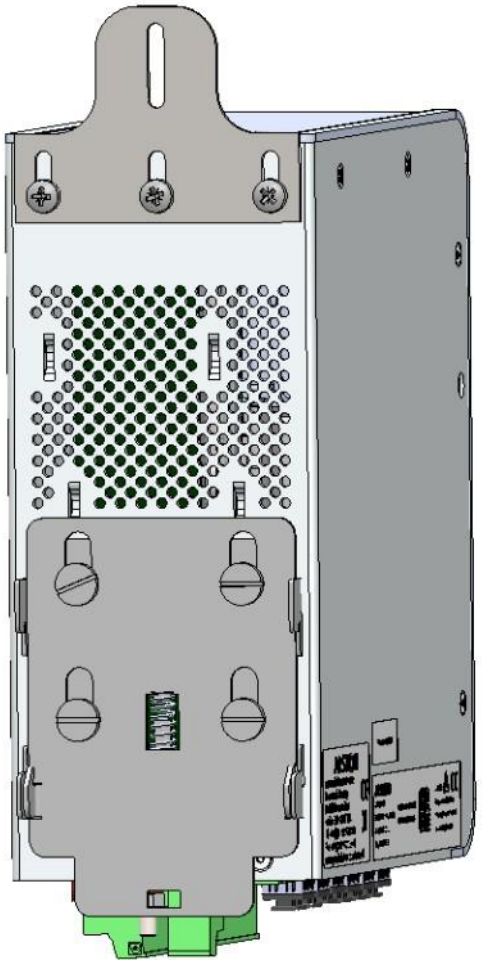


**Figure 23: Reason H49 DIN Rail Mounting Details - Rear View with Mounting Rack**

Optional **Weidmuller FM4 TS35** mounting clip can also be used, as shown in the following figure (to be ordered separately).

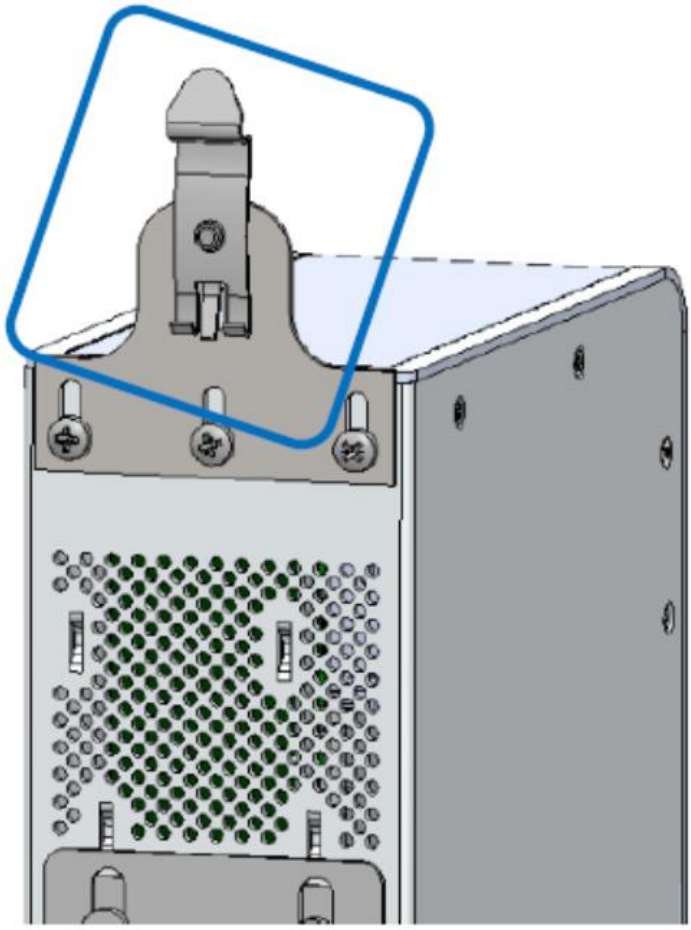


**Figure 24: Reason H49 DIN Rail Mounting Details - Rear View with Weidmuller Clip**

### 5.4.1 RECOMMENDATIONS FOR ELECTROMAGNETIC COMPATIBILITY

Caution:

Reason H49 operates within -25°C/+55°C in normal conditions. As heat within the Reason H49 switch is channeled to the enclosure, it is recommended that 1,5 cm of space be kept between each switch mounted within the DIN Rail to allow for a small amount of airflow. A closer spacing will result in higher device operating temperature.

Caution:

The orientation in which the Reason H49 is fitted on the DIN Rail is a key factor to optimal performance. Reason H49 requires to be installed vertically on the DIN rail. Other position would lead to inadequate ventilation and result in increased heat generation.

Caution:

It is highly recommended to use the following power line filter in order to ensure intended product performance in all environments:

Make: Corcom

Model: 3VB

# 6 CONNECTION

## 6.1 CHAPTER OVERVIEW

As well as connections to the Ethernet network, Reason H49 requires auxiliary power supply connection and safety earth connection. Alarm outputs are provided, and these should be connected for system supervision.

The locations of the various connection points are detailed in this chapter. This chapter contains the following sections:

## 6.2 GENERAL WIRING

Only two wires can be screwed together on any one connector. The AC and DC signal and communication wires should use separate shielded cable.

Caution:

A high rupture capacity (HRC) fuse must be used for auxiliary supplies (for example Red Spot type NIT or TIA) with the following characteristics:

- Current rating: 16 Amps
- Minimum dc rating: 220 Vdc
- gG operating class in accordance with IEC 60269

The fuses must be connected in series with the positive auxiliary supply input connections for both primary (Pin 23) and secondary (Pin 1) BIU261D inputs.

Wires should be connected with the power supply connectors unplugged. Each wired signal has to be tested before plugging and fixing the connectors. The connectors have to be fixed on the Reason H49 case with the screws available at each extremity of the connector.

For connection of the protective (earth) conductor, refer to chapter 6.2 Earth Wiring page **1**.

### 6.2.1 WELL-ORGANIZED WIRING

Caution:

Improperly installed cabling can affect device performance and generate interferences.

To avoid interferences, careful placement of cables is required. The principle consists in physically separating power sources (AC/DC) and communication cables (i.e. high voltage from RJ45/Copper). This is even more important when devices receive time synchronization from PTP master clock.

Whenever possible, use cableways or troughs.

## 6.3 EARTH WIRING

### 6.3.1 PROTECTIVE EARTH WIRING

This equipment requires a protective conductor (earth) to ensure user safety according to the definition in the standard IEC 60255-27: 2005 Insulation Class 1.

Warning:
– To preserve the device's safety features, the protective conductor (earth) MUST not BE disturbed when connecting or disconnecting functional
earth conductors, such as cable screens, to the PCT stud.
– The protective conductor must be connected first, in such a way that it is unlikely to be loosened or removed during installation, commissioning or maintenance. This MAY be achieved by use of an additional locking nut.

Warning:
Always place the protective conductor (earth) as shown on the diagram below.

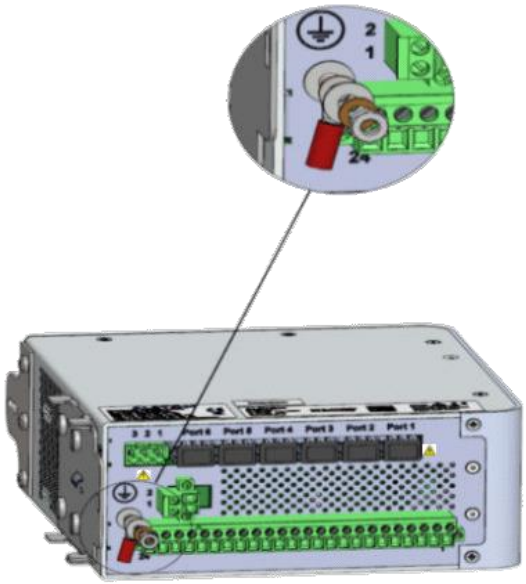



**Figure 25: Protective Earth Screw**

The protective conductor (earth) must be as short as possible, with low impedance. The best electrical conductivity must be maintained at all times, particularly the contact resistance of the plated steel stud surface.

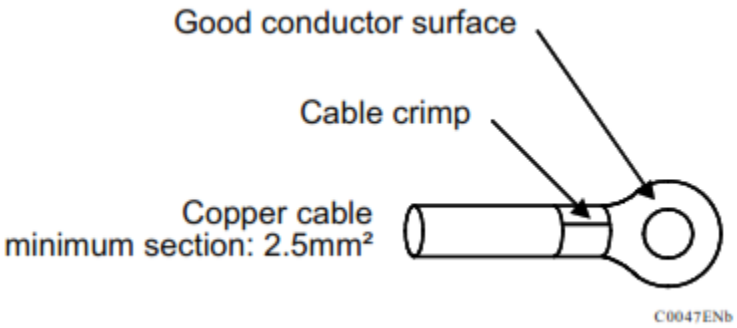



**Figure 26: Example of Earth Cable**

## 6.3.2 CASING/EARTH CONNECTION

To protect against disturbances, each Reason H49 must be carefully and correctly interconnected.

Within Reason H49 equipment, earth and casing must be connected to a grid-like grounding system in the shortest possible way using low impedance (at high frequencies), wide and short electrical connections (wires or braids) as specified in the IEC 61000-5 standard.

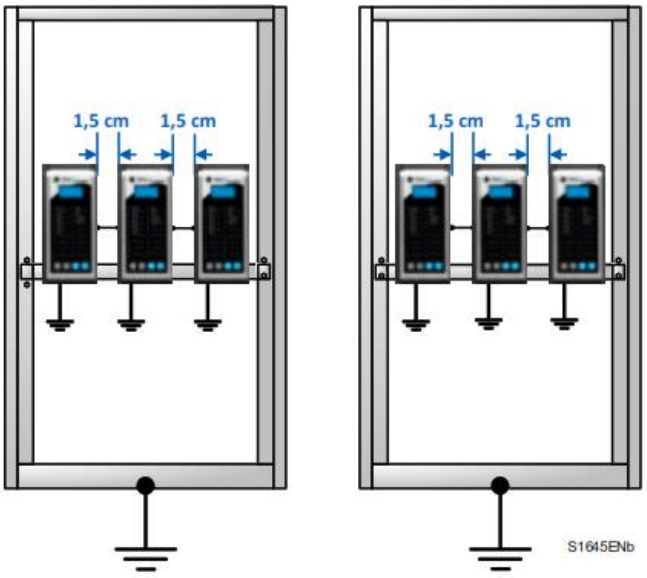



**Figure 27: Recommended mounting and Casing / Earth interconnection**

## 6.4 POWER SUPPLY WIRING

Reason H49 contains a Basic Interface Unit (BIU261D) board, which includes two redundant power supply inputs, as shown in the following figure:

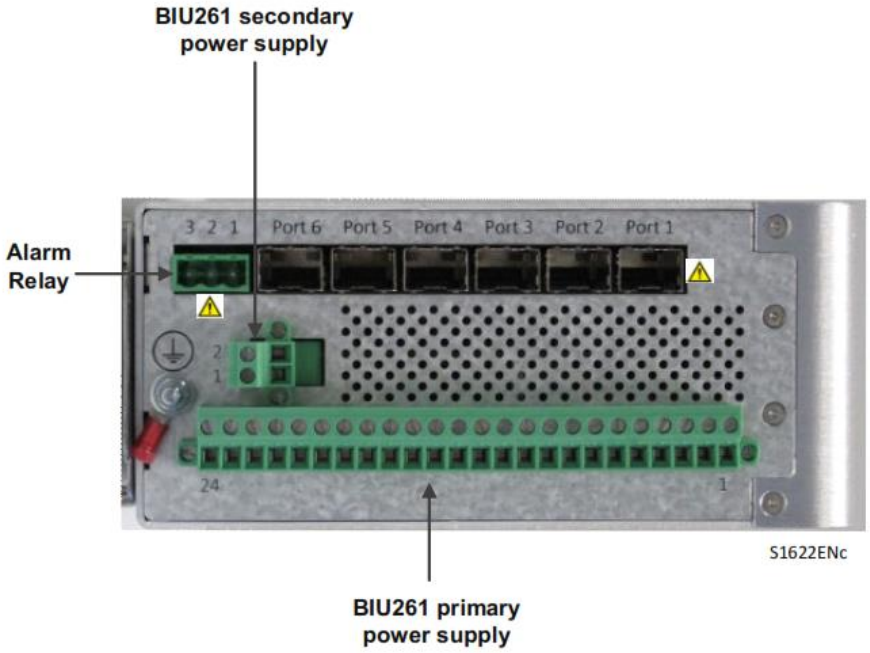



**Figure 28: Reason H49 Power Supply Wiring**

### BIU261D primary power supply

The primary power supply is connected using a 24-way connector block:

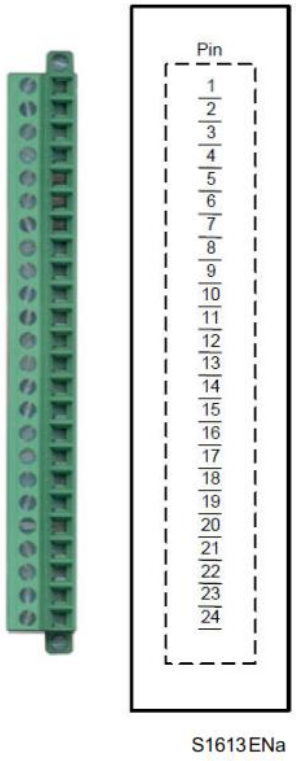



**Figure 29: Typical 24-way Female Connector**

### BIU261D primary power supply

| Pin n° | Description | |
|---|---|---|
| 1 to 21 | Not used | |
| 22 | Voltage input: GND | |
| 23 | Voltage input: AC/DC | ( + ) |
| 24 | Voltage input: AC/DC | ( - ) |

***Note:***
*Inputs must be connected to the specified pins. Other pins must remain unused, and no other connection has to be made.*

The 24-way connector block characteristics are as follows:

- Continuous rating 10A
- Connection method M3 screws
- Cable section 2.5mm2
- Connection pitch 5.08mm
- Insulation between terminals and to the earth 300 V basic insulation
- Standards UL, CSA

***Note:***
*The connector is fixed using 2 M3 screws located at each end of the connector.*

### BIU261D secondary power supply

The secondary power supply is connected using a 2-way connector block:

**Figure 30: Typical 2-way Female Connector**

| Pin n° | Description | |
|---|---|---|
| 1 | Voltage input: DC | ( + ) |
| 2 | Voltage input: DC | ( - ) |

The 2-way connector block characteristics are as follows:

- Continuous rating 10A
- Connection method M2.5 screws
- Cable section 2.5mm2
- Connection pitch 5.08mm
- Insulation between terminals and to the earth 300 V basic insulation
- Standards UL, CSA

If the primary power supply input is lost while being used, the BIU261D switches to the secondary power supply input. It will switch back to the primary power supply when the latter becomes available again and has been stable for a few seconds.

If the secondary power supply is lost while being used, the BIU261 instantly switches to the primary power supply. It will continue to use the primary power supply source as long as it is available, even when the secondary power supply becomes available again.

Reason H49 supports the following power supply use cases:

| Use Case | Primary source | Secondary source |
|---|---|---|
| Use case 1 | DC | DC |
| Use case 2 | DC | OFF |
| Use case 3 | OFF | DC |
| Use case 4 | AC | DC |
| Use case 5 | AC | OFF |
| **Nominal Power supply range** | **85Vac to 230Vac**<br>**85Vdc to 250Vdc** | **85Vdc 250Vdc** |

***Note:***
*If the product is powered at 85Vdc on both Primary and Secondary sources, the power is consumed from the Secondary source and the LED alarm is set ON (red color, refer to section 4.1.1 for LED location).*

### Crimped Ferrule

For safety reasons, wire terminations must be insulated using an insulated crimped ferrule, suitable for 2,5mm$^2$ wire size.

**Figure 31: Pluggable Terminal Block**

Insulated wire ferrules must be slipped over the stripped cable and crimped to prevent stranded wire from fraying.

## 6.5 ALARM RELAY WIRING

The 3-pin connector of the relay alarm on the SRPV3 board allows the following Reason H49 statuses:


**Figure 32: Relay Alarm Wiring**

| Pin | Signal | Description |
|---|---|---|
| 1 | Normally Open | Closed=Normal Operation<br>Open= Power supply defect (both input voltage sources are down) / Operating System defect (Kernel crash, processor overload, memory leak) |
| 2 | Common | |
| 3 | Normally Closed | Closed= Power supply defect (both input voltage sources are down) / Operating System defect (Kernel crash, processor overload, memory leak)<br>Open= Normal Operation |

### 6.5.1 USING TERMINAL BLOCKS

Printed-circuit board connectors can be used:

**Figure 33: Pluggable Terminal Block**

The relay alarm connector shall be plugged with MSTB 2,5 HC/ 3-ST-5,08 - 1911978 manufactured by Phoenix Contact.

#### 6.5.1.1 RECOMMENDED WIRE SIZE

The minimum recommended wire size for terminal blocks is 2.5mm$^2$.

#### 6.5.1.2 CRIMPED FERRULE

For safety reasons, wire terminations must be insulated using an insulated crimped ferrule, suitable for 2,5mm$^2$ wire size.

**Figure 34: Pluggable Terminal Block**

Insulated wire ferrules must be slipped over the stripped cable and crimped to prevent stranded wire from fraying.

**Caution:**

**Refer to section 10.5.3 Auxiliary Fault Relays (Optical Port Alarm) page 1 for electrical characteristics of alarm circuit.**

## 6.6 ETHERNET CONNECTIONS

Reason H49 is easy to install and operate. It is designed to work in an electrical plant environment, and it is fully certified IEEE 1613 series, IEC 61850-3 and IEC 60255-27.

Reason H49 connects to the network through a Small Form-factor Pluggable module (SFP), which can be inserted and removed safely while the switch is powered and operating:

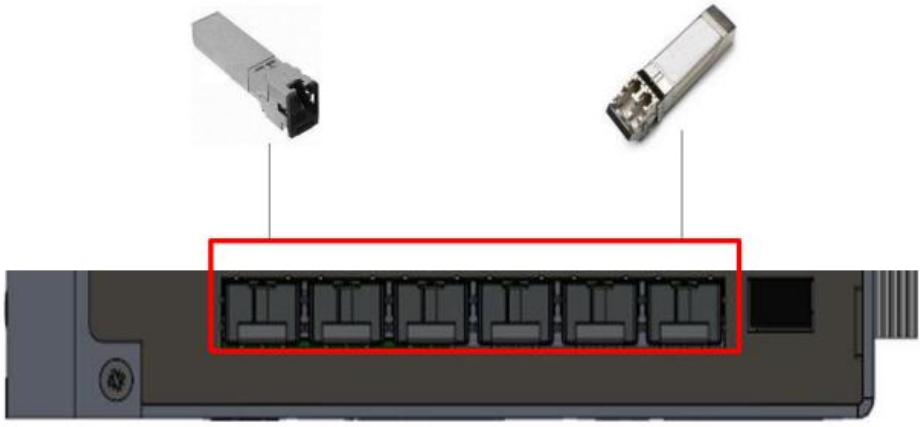


**Figure 35: SFP Module Connection**

The SFP module is a hot-swappable connector that provides high-speed performance. Reason H49 supports two kinds of modules:

- Optical LC-type SFP
- RJ45-type SFP

The table below lists the supported LC-type SFP and references.

| Reference | Manufacturer | Description | Connector Type | Image |
|---|---|---|---|---|
| **AFBR-5715ALZ** | fit-foxconn | 1Gbps Multimode 850nm wavelength | LC Duplex |  |
| **HFBR-57E0APZ** | AVAGO | 100Mbps Multimode 1300 nm wavelength | LC Duplex |  |

| Reference | Manufacturer | Description | Connector Type | Image |
|---|---|---|---|---|
| **AFCT-5765ALZ** | fit-foxconn | 100Mbps Single-mode SR (up to 2 km)<br>1300 nm wavelength | LC Duplex |  |
| **AFCT-5715ALZ** | fit-foxconn | 1Gbps Single-mode (up to 10km)<br>1310 nm wavelength | LC Duplex |  |
| **AFCT-5765ATL Z** | fit-foxconn | 100Mbps Single-mode IR-1 (up to 15 km)<br>1300 nm wavelength | LC Duplex |  |

The table below lists the supported RJ45-type SFP and references:

| Reference | Manufacturer | Description | Connector Type | Image |
|---|---|---|---|---|
| **ABCU-5741ARZ** | fit-foxconn | 10/100/1000Mbps | RJ45 |  |
| **ABCU-5741ARZ- D** | ATGBICS | 10/100/1000Mbps | RJ45 |  |

Caution:

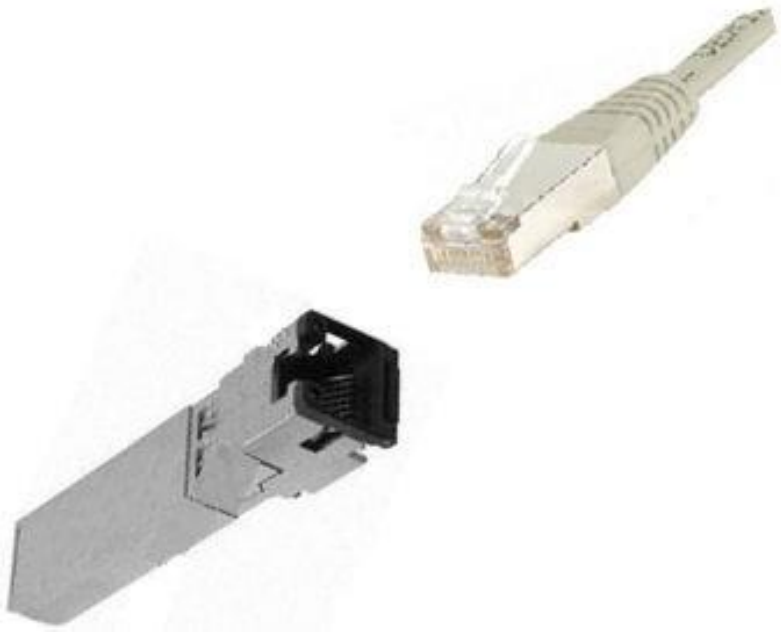
Reason H49 is delivered with SFP cap inserted in each SFP cage. The cap must be inserted in each SFP cage unused. It is a protection against dust.

### 6.6.1 RJ45-TYPE CONNECTION

The following figure shows the RJ45-type module used by the Reason H49 switch and its corresponding RJ45 connector.

Insulated cable category 6 or 5e (FTP: Foil Twisted Pair) or insulated (STP – Shielded Twisted Pair) with RJ45 connectors are mandatory.

***Note:***
*Do not use RJ45 UTP cable. This kind of cable may disrupt time synchronization.*



S1355ENa

**Figure 36: RJ45 SFP Module**


**Caution:**

**When SFP Copper Ethernet modules are used, the connected cables shall be shortened to minimum possible length. We recommend that cables (such as RJ45 category 6 or 5e) do not exceed 3 meters to comply with Electromagnetic compatibility (EMC) requirements. Connected cables shall not extend beyond the cabinet where the product is used. The equipment connected to both ends of the cable shall be connected directly to a common protective earth point within the same cabinet.**

### 6.6.2 OPTICAL LC-TYPE CONNECTION

The following figure shows the optical LC-type module used by the Reason H49 switch and its corresponding LC-type connector.

S1354ENa

**Figure 37: Ethernet Fiber Optic – LC-type Module**

#### Warning about Laser Rays


Caution:

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

Non–observance of this rule could possibly result in personal injury. Signals transmitted via optical fibers are unaffected by interference. The fibers guarantee electrical isolation between the connections.

If electrical to optical converters are used, they must have management of character idle state capability (for when the fiber optic cable interface is "Light off").

LC-type small form-factor pluggable (SFP) modules shall be used. LC/ST or LC/SC optical patch cords may be used to connect the board to devices fitted with ST or SC connectors.

**Figure 38: Example of Optical Patch Cord (Multimode Duplex LC/ST)**

## 6.7 FIBER OPTIC BUDGET CALCULATIONS

Optical power is expressed in Watts. However, the common unit of power measurement is the dBm, defined by the following equation: Power (dBm) = 10 log Power (mW) / 1 mW.

The fiber optic budget is the difference between the power emitted into the fiber and the sensitivity (minimum amount of power required) of the receiver connected through the fiber optic cable.

Link Power Budget = Transmitter Power (dBm) - Receiver Sensitivity (dBm). The distance over which the signals can be transmitted and successfully received is affected by the optical loss, as shown in the figure below.

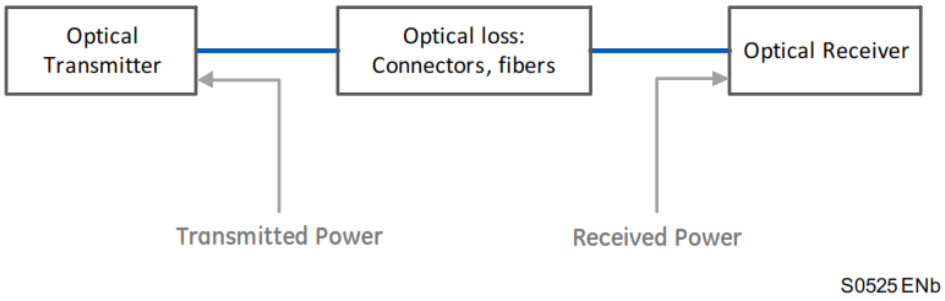



**Figure 39: Fiber Budget**

For this product, the optical budget is given in the table below.

| Fiber type | Multimode 62.5/125 micron | Single mode 9/125 micron |
|---|---|---|
| Power coupled into fiber | -19 dBm | -15 dBm |
| Sensitivity | -31 dBm | -34 dBm |

In calculating the maximum distance, the following figures can be used as a guide, but you should check with your supplier for precise figures.

| Fiber type | Multimode | | | Single mode |
|---|---|---|---|---|
| | 50*µm | 62.5 µm | 125 µm | 62.5/125 µm |
| Link budget | 12 dB | | | 19 dB |
| Typical connector loss<br>(1 per receiver, 1 per transmitter) | 0.8 dB | | | 0.8 dB |
| Safety Margin | 4 dB | | | 4 dB |
| **Allowed link attenuation** | 6.4 dB | | | 13.4 dB |
| Typical cable attenuation | 1 dB/km | | | 0.4 dB/km |
| **Maximum range** | | | | **100Base-FX IR-1: 15 km**<br>**100Base-FX SR: 2 km** |
| 100 Mbits/s – 100Base-FX | N/A | : 2 km | | |
| 100 Mbits/s – 100Base-LX | 550 m | | | |
| 1000 Mbits/s | 1000Base-SX: 500 m | 1000Base-SX: 275 m | N/A | |
| Insertion of a patch panel (per panel) | 2 dB | | | 1 db |

## 6.8 POWER UP

The following indicators are displayed during the power-up process:

- LED 1 is green
- LED 2 is amber
- LED 18 is red, it indicates the state of the redundant power supply

At the end of the power-up process, the following indicators are displayed:

- The LCD screen displays "H49" and the device’s IP address
- LED 1 is green
- LED 2 is green

Refer to section Front panel for LEDs indications.

# 7 SETTINGS

## 7.1 CHAPTER OVERVIEW

To take full advantage of all the features available from the Reason H49 switch, the device must properly be configured for your network.

There are several ways to configure the Reason H49 switch:

- A **web user interface**, accessible via the switch's built-in web server.
- An **SNMP** interface can be used to read/write some settings
- **CLI** (command Line Interface) can be used to read/write most settings (SSH).

***Note:***
*This chapter only explains how to configure the Reason H49 switch through the embedded web server. However, an appendix, at the end of this document, describes the command lines supported by the SSH service.*

This chapter contains the following sections:

## 7.2 CONNECTING TO REASON H49

To access the embedded web server from a PC connected to the same LAN as the Reason H49 switch, the PC and the Reason H49 switch must be on the same subnet.

The default IP address of the Reason H49 switch is **192.168.254.254** and the sub mask is **255.255.0.0**. Your PC IP address must be set in the same LAN for initial configuration.

> ***Note:***
> *The device connects to the network through a Small Form-factor Pluggable (SFP) module. Refer to the Ethernet Connections section to see the references of the supported RJ45-type SFP module.*

## 7.3 ACCESSING THE WEB USER INTERFACE

The Reason H49 web user interface provides an easy way to modify the switch's configuration settings and access the built-in network and security administration functions.

The web user interface can be accessed via a web browser.

Once your PC is connected to the same LAN and subnet as the Reason H49, open the switch's web user interface as follows:

- Open one of the following recommended web browsers:

| Browser name | Manufacturer |
|---|---|
| Chrome | Google |
| Internet Explorer | Microsoft |
| Mozilla Firefox | Mozilla Foundation<br>Mozilla Corporation |
| Safari | Apple Inc. |

- In the web browser's address bar, type the default Reason H49's IP address: **192.168.254.254** and press **Enter** on your keyboard.

> ***Note:***
> *The H49 embedded web server only supports the **secure HTTPS protocol**. When you access the server via HTTPS, you may see a warning dialogue indicating that the certificate was signed by an unknown authority. This is expected as the certificate provided by default is self-signed. To avoid this message in the future, you can choose to install a properly signed certificate. For more information, refer to section **8.1.6 Certificate Management.***

## 7.4 LOGGING IN

The web login window prompts you for a login name and password. Use the following default values:

- Login: user
- Password: user

> ***Note:***
> *See the Cyber Security section for more information on user accounts.*

If an error occurs during the authentication process, an information message appears on screen, as shown in the following figure.

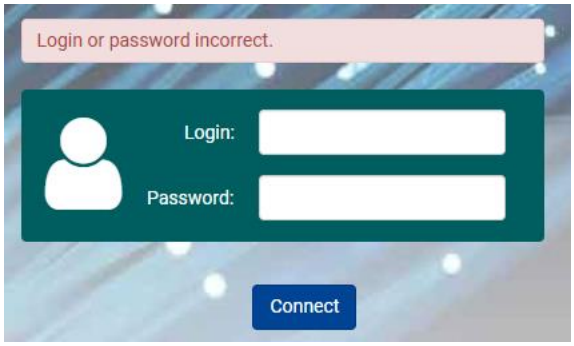



**Figure 40: Reason H49 Web User Interface - Error during Login Process**

When connecting to Reason H49 for the first time, the system prompts the user to change the default password.

- Enter a new password and confirm.

> ***Note:***
> *The new password must match the **Password complexity** parameter, which is enabled by default in Reason H49 web user interface. Refer to section **8.1.5 Password Management**, page **1** for more information.*

Upon successful authentication, the user is granted authorization for access. Read the Software License agreement and click **Yes** to agree to the terms:

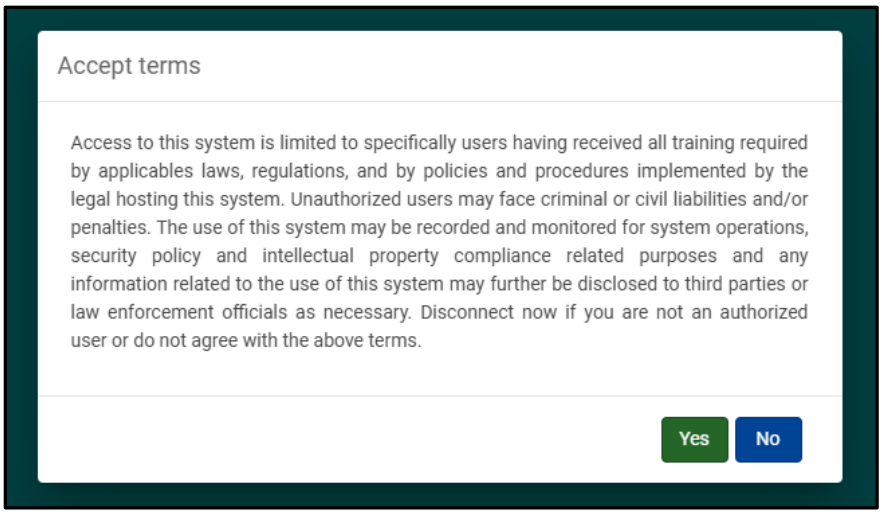



**Figure 41: Reason H49 Web User Interface - Agreement Conditions**

## 7.5 FEATURE OVERVIEW

The embedded web user interface consists of two areas:

- A configuration menu, on the left side of the window, which is organized into three main sections;
  - System
  - Network
  - Security
- A setting panel, on the right.

Navigate through the configuration menu to access each of the switch's functions.

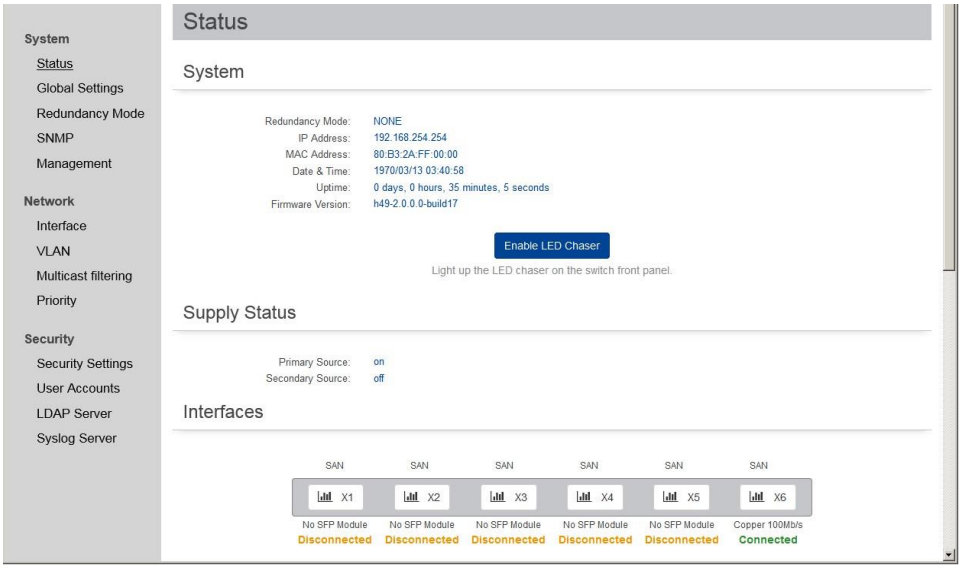



**Figure 42: Reason H49 Web User Interface – Start Page**

### 7.5.1 SYSTEM

The **System** section provides the current configuration of the Reason H49 switch together with its status. It also allows the user to update the main system attributes.

#### 7.5.1.1 STATUS

To get the global status of the Reason H49 switch, click **Status** in the **System** section: The top part of the page shows the following information:

| Attribute | Description |
|---|---|
| **Redundancy mode** | Selected redundancy mode |
| **IP address** | Device's IP address |
| **MAC address** | Device's MAC address |
| **Date & Time** | Device's clock date and time |
| **Uptime** | Elapsed time since last reboot |
| **Firmware Version** | Version of the firmware currently running on the device |

### LED Chaser

The LED chaser of the Reason H49 is a function used to identify correctly a given device amongst others. It consists in sequentially lighting all the LEDs in the front panel one after the other, eight at a time.

- Click **Enable LED Chaser** to activate the LED chaser and make the device's LEDs blink in sequence.
- Click again to stop the **LED chaser** (Disable LED Chaser button), or press the "C" button on the device front panel.

Alternatively, the LED chaser can be stopped by pressing the "C" button in the front panel.

### Supply Status

This area shows information about the input voltage sources (Primary voltage source/Secondary voltage source):


**Figure 43: Reason H49 Web User Interface – Power Supply Status**

### Interfaces

This area displays the interface status:

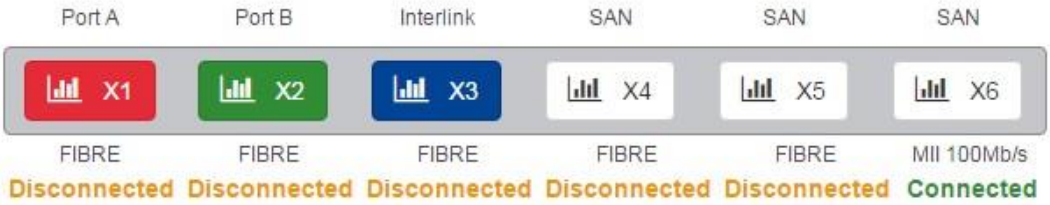



**Figure 44: H49 Web User Interface – Interfaces Status**

> ***Note:***
> *The interface configuration is done in the **System** > **Redundancy Mode** page.*

Each interface has a colored button and some details:

| Attribute | Description |
|---|---|
| **Button color** | Display the port type in accordance of colors.<br>**Red**: Redundant interface Port A<br>**Green**: Redundant interface Port B<br>**Blue**: PRP coupling interface<br>**White**: Standard interface<br>**Grey**: The port is not available in the selected redundancy mode. |
| **Media and speed state of interfaces X1 to X6** | Copper 10/100/1000 Mbps<br>Fiber 100 Mbps<br>Fiber 1000 Mbps |

| Attribute | Description |
|---|---|
| **Connection state of interfaces X1 to X6** | **Green**: Connected<br>**Yellow**: Disconnected<br>**Red**: Disabled<br>These settings can be modified in the **Network > Interface** page. |

Click a connected interface to get the status of the packets sent:

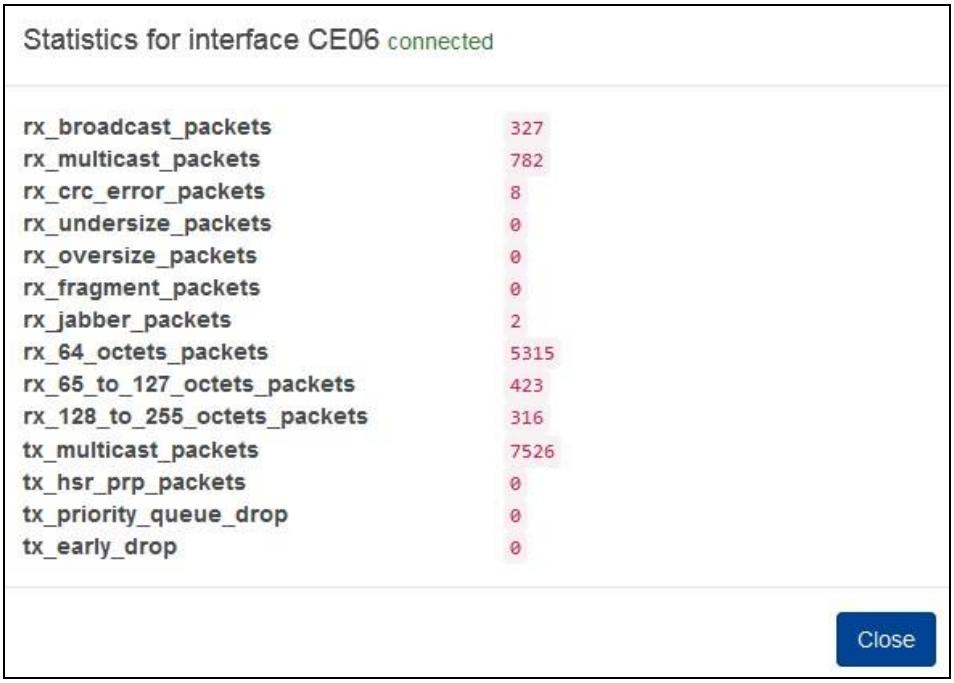



**Figure 45: H49 Web User Interface – Statistics of a Connected Interface**

### Time Synchronization

This area displays read-only information about the device's time synchronization protocol.


**Figure 46: Reason H49 Web User Interface – Time Synchronization Status**

This information comes from the configuration done in the **System** > **Global Settings** page. The following attributes are also displayed according to the selected value.

> ***Note:***
> *When the device uses its Local clock as time source, then no other attribute is displayed in this section.*

### NTP attributes

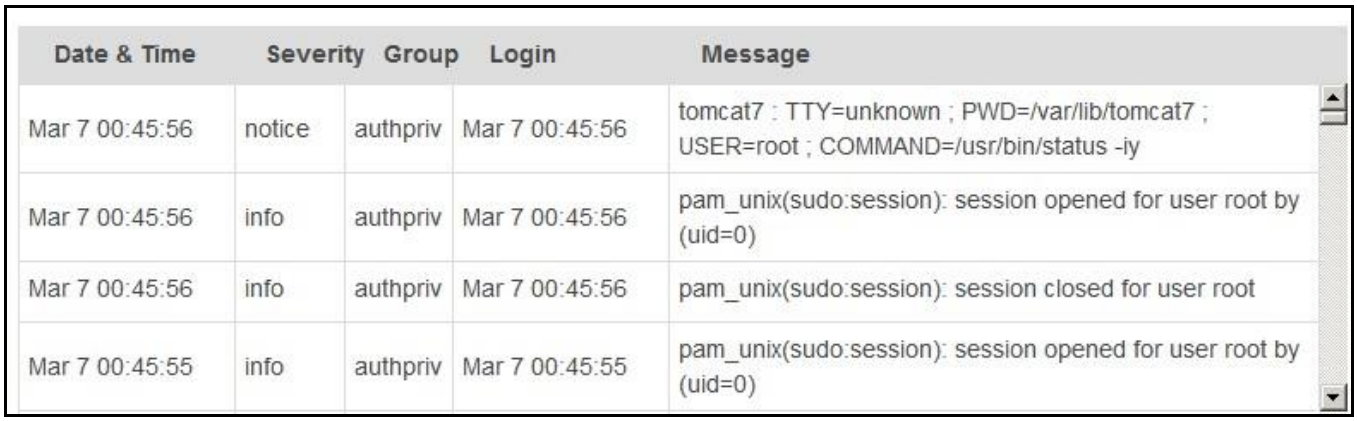
| Attribute | Description |
|---|---|
| **Mode** | System's time synchronization mode:<br>Disable<br>Client<br>Client/Server<br>Server |
| **Status** | Time synchronization status:<br>Synchronized<br>Not synchronized |

### PTP attributes

| Attribute | Description |
|---|---|
| **Mode** | Synchronization mode of the system:<br>Disable<br>Boundary clock<br>Transparent clock - E2E<br>Transparent clock - P2P<br>A label "Slave" or "Master" indicates the current state as time Master or Slave. |
| **Status** | Synchronized to a Master clock<br>Not synchronized to a Master clock |
| **Grandmaster ID** | Grandmaster MAC address |
| **Time Source** | Atomic clock<br>GPS<br>Terrestrial radio<br>Hand set<br>Internal oscillator<br>Other |
| **Clock Accuracy** | Case time error (its magnitude) between time that the device provided a traceable time (Applicable only for PTP clock mode)<br>25ns \| 100ns \| 250ns \| 1us \| 2.5us \| 10us \| 25us \| 100us \| 250us \| 1ms \| 2.5ms \| 10ms \| 25ms \| 100ms \| 250ms \| 1s \| 10s \| >10s |

### Logs

This area displays the log messages in a Syslog format. The syslog level is divided in 4 categories: error, warning, notice and information:



| Date & Time | Severity | Group | Login | Message |
|---|---|---|---|---|
| Mar 7 00:45:56 | notice | authpriv | Mar 7 00:45:56 | tomcat7 : TTY=unknown ; PWD=/var/lib/tomcat7 ; USER=root ; COMMAND=/usr/bin/status -iy |
| Mar 7 00:45:56 | info | authpriv | Mar 7 00:45:56 | pam_unix(sudo:session): session opened for user root by (uid=0) |
| Mar 7 00:45:56 | info | authpriv | Mar 7 00:45:56 | pam_unix(sudo:session): session closed for user root |
| Mar 7 00:45:55 | info | authpriv | Mar 7 00:45:55 | pam_unix(sudo:session): session opened for user root by (uid=0) |

**Figure 47: Reason H49 Web User Interface – Logs Status**

The following table gives a description of each table columns:

| Attribute | Description |
|---|---|
| **Date & Time** | Date and time of log generation |
| **Severity** | Log's severity level:<br>Alert<br>Critical<br>Debugging<br>Emergency<br>Error<br>Informational<br>Notice<br>Warning |
| **Group** | Group name of the Syslog message defined in the Cyber Security system specifications:<br>Authentication<br>Security<br>System<br>Command |
| **Login** | Username at the origin of the Syslog message. |
| **Message** | Message content |

### 7.5.1.2 GLOBAL SETTINGS

To configure the global settings of the Reason H49 switch, click **Global Settings** in the **System** section.

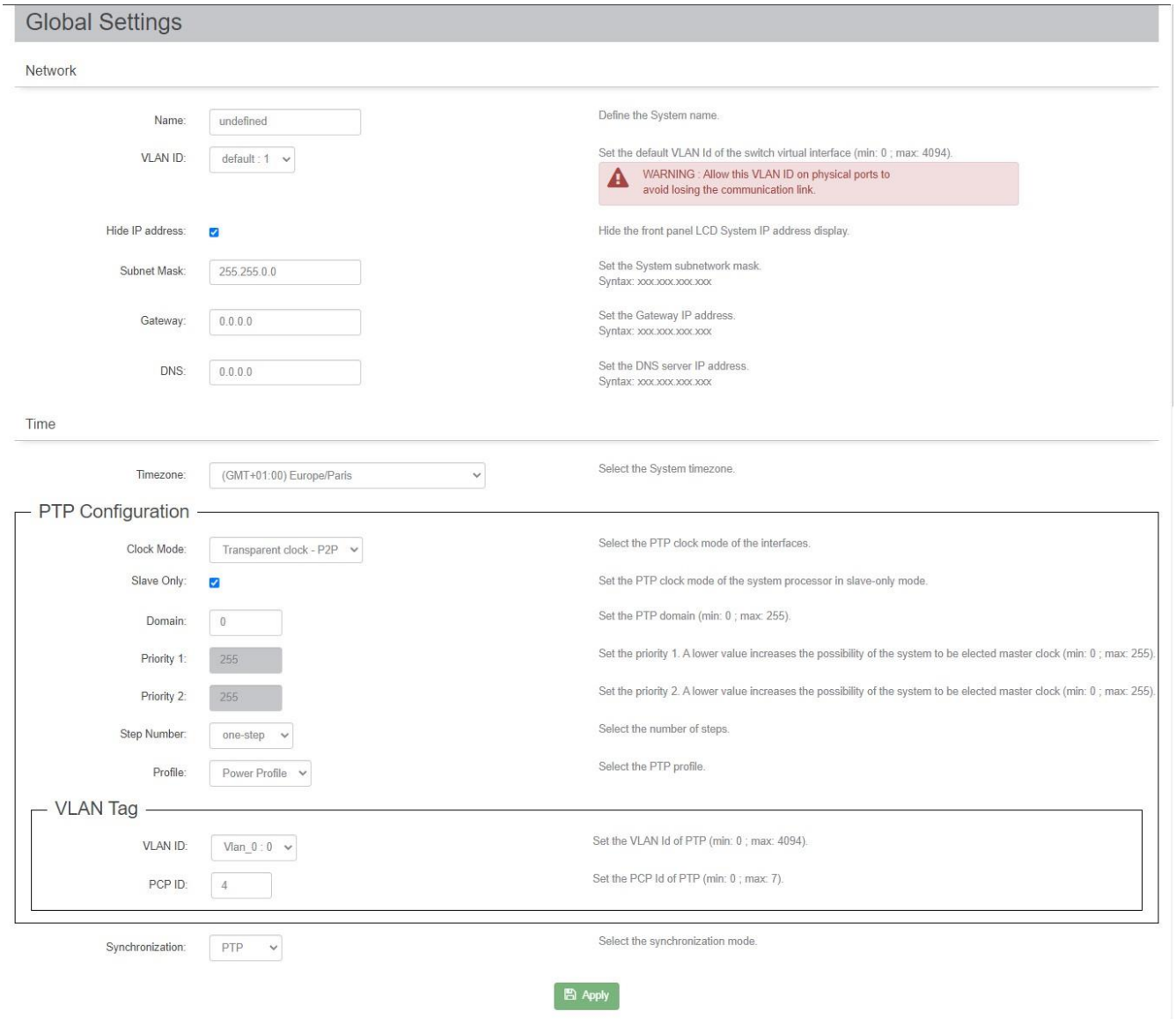



**Figure 48: Reason H49 Web User Interface – Global Settings**

#### Network

The **Network** area allows the user to modify the usual TCP/IP network parameters. An explanation of each configuration item is given in the following table:

| Attribute | Description | Factory Default |
|---|---|---|
| **Name** | Name of the system | **Undefined** |
| **VLAN ID** | Default VLAN ID. It identifies the individual VLANs you create on your network. | |

| Attribute | Description | Factory Default |
|---|---|---|
| **Hide IP address** | Tick box used to hide/show the IP address on the LCD front panel. When booting, the IP address will be displayed on the LCD front panel for 10 seconds before being hidden | **Unticked** |
| **IP Address** | IP address in IPV4 format which identifies the switch on a TCP/IP network. | **192.168.254.254** |
| **Subnet Mask** | Identifies the type of network to which the H49 is connected. | **255.255.0.0**<br>(Class B network) |
| **Gateway** | IP address of the router that connects the LAN to an outside network.<br>Make sure that Reason H49 can access the gateway:<br>If no gateway is connected to the network, enter a "dummy" gateway IP address that **is NOT** in the same range as the Reason H49 switch.<br>If a gateway is connected to the network, the gateway IP address **MUST BE** in the same range as the Reason H49 switch. | **0.0.0.0** |
| **DNS** | IP address of the DNS Server used by your network. | **0.0.0.0** |

### Time

The Time area allows the user to set the time, date and other time source attributes for the system and the PTP settings:

| Attribute | Description |
|---|---|
| **Timezone** | Allows conversion from GMT (Greenwich Mean Time) to local time.<br>Use the drop-down list to select the time zone of the system. |

> ***Note:***
> *Changing the time zone will automatically correct the current time. You should configure the time zone before setting the time.*

### Synchronization

Reason H49 are delivered with a default date set to 1st January 1970.

Before starting to configure the switch, it's important that the time on your device is accurate. Reason H49 synchronization mode can be:

- Manual (the device uses its Local clock as time source)
- NTP
- PTP

**If Reason H49 is synchronized through a NTP or PTP server**

- Make sure that time, date and other time source attributes (NTP or PTP) are configured properly, at **System > Global Settings** menu. If settings are not defined or incorrect, make the relevant changes.

If Reason H49 is NOT synchronized through a NTP or PTP server

You may set the switch internal clock to your date and time manually. The default Reason H49 clock is set to UTC (Coordinated Universal Time, originally known as Greenwich Mean Time, or GMT). The UTC base time equals to **0** (based at Greenwich, England).

To properly set the H49's clock and time zone, you should proceed in the following sequence:

1. Select **Manual** from the **Synchronization** drop-down list.
2. Convert your local time to **UTC 0** and enter the converted time in the **Time** entry field. For example, if your local time is 5:00 PM and the offset to UTC 0 is +3, then, subtract +3 from 5:00 PM. The setting to be entered in the Time entry field will be 2:00 P.M.
3. Set the current date using the **Date** calendar.
4. Set the time zone to your current location using the **Timezone** drop-down list above.
5. Click on **Apply** to save your changes.

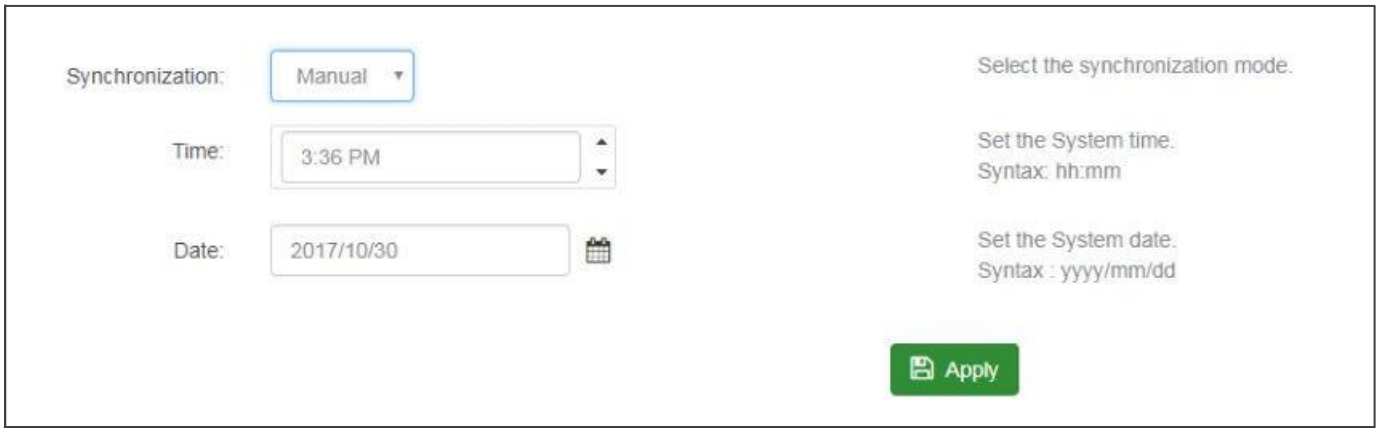



**Figure 49: H49 Time synchronization settings**

***Note:***
*If you cannot access the Reason H49 web user interface, you may also set the system date and time manually through the Secure Shell (SSH) console by running the following command lines, sequentially (i.e on separate lines):*

*system -t local date MMDDhhmmYY.ss (MM for month, DD for day, hh for hour, mm for minutes, YY for Year and ss for seconds). hwclock -w*

### NTP Configuration


**Figure 50: Reason H49 Web User Interface – NTP Settings**

Set the following NTP settings:

| Attribute | Description | Factory Default |
|---|---|---|
| **NTP Mode** | Use the drop-down list to select the NTP operating mode:<br>Disable<br>Client<br>Client/Server<br>Server<br><br>***Note:***<br>*Regarding NTP settings for client behavior:*<br><br>*The NTP client is activated/enabled only if the Client mode is selected, and a Server IP address has been defined (other than 127.0.0.1), and the client/server mode is selected, and a Server IP address has been defined (other than 127.0.0.1).* | Disable |
| **NTP Server** | Set the IP address or THE Fully Qualified Domain Name (FQDN) of NTP server. | 127.0.0.1 |

### PTP Configuration

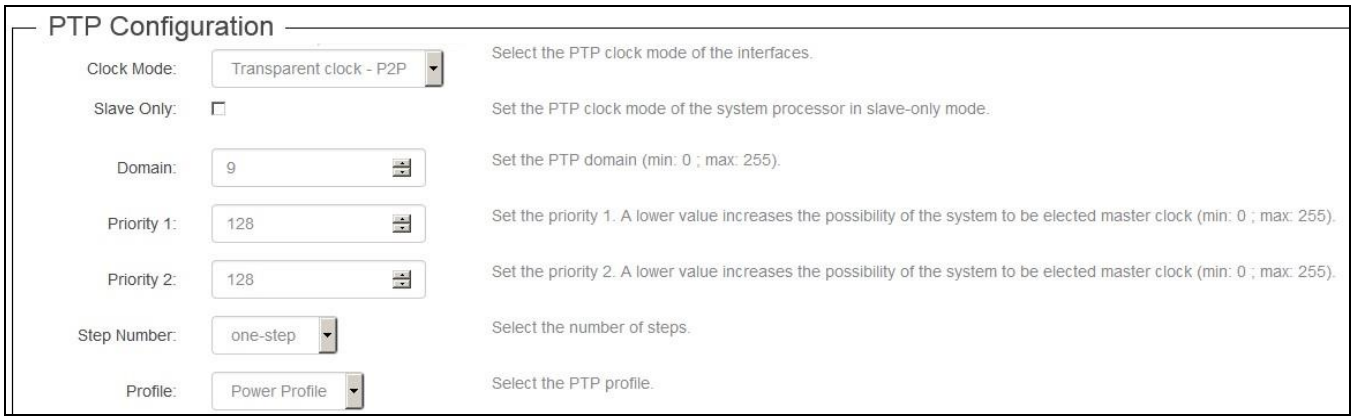



**Figure 51: Reason H49 Web User Interface – PTP Settings**

Set the following PTP settings:

| Attribute | Description | Factory Default |
|---|---|---|
| **Clock Mode** | Use the drop-down list to select the PTP switching mode:<br>Disable<br>Boundary clock<br>Transparent clock - E2E<br>Transparent clock - P2P | Transparent clock - E2E |
| **Slave Only** | Set Reason H49 as a PTP slave-only. It means that the device will not postulate as time master during a selection campaign. | Enabled |
| **Domain** | Enter the PTP domain between 0 and 255 | 0 |
| **Priority 1** | Enter the priority level to turn the H49 as the Master clock. Priority 1 goes from 0 to 255.<br>Lowest values increase the probability for the device to be elected Master clock. | 255 |
| **Priority 2** | Enter the priority level to turn the H49 as the Master clock. Priority 2 goes from 0 to 255.<br>Lowest values increase the probability to be elected Master clock. | 255 |
| **Step Number** | Select the device's step synchronization mode. | One-step |
| **Profile** | Selects the PTP profile<br>Default L2<br>Power profile | Power Profile |

### VLAN Tag

Enable or disable the VLAN tag for PTP messages.

| Attribute | Description | Factory Default |
|---|---|---|
| VLAN ID | Set the VLAN ID of the PTP frames. | 0 |
| PCP ID | Set the priority code point (PCP) of the PTP frames. | 4 |

### 7.5.1.3 REDUNDANCY MODE

Setting up communication redundancy on your network provides a backup data transmission route in the event that the communication is lost.

To set up the H49 redundancy mode, click **System > Redundancy Mode**. Click the desired redundancy mode among the preset switch configurations:

| Selected Redundancy Mode | Description |
|---|---|
| **None** | Uses Reason H49 as a standard switch.<br>All the ports are enabled by default. |
| **PRP RedBox** | Ports 1 and 2 are reserved for redundant connection to LAN A and LAN B respectively.<br>4 Ports are available for SAN connections. |
| **HSR-PRP Coupling RedBox** | Ports 1 and 2 are reserved for redundant connection to HSR ring. Port 3 is reserved for one of the PRP LANs.<br>3 Ports are available for SAN connections. |
| **HSR RedBox** | Ports 1 and 2 are reserved for redundant connection to HSR ring.<br>4 Ports are available for SAN connections. |
| **HSR QuadBox** | In this configuration, 4 ports are reserved for coupling functions. Ports 1 & 2 are reserved for redundant connection to HSR ring A. Ports 3 & 4 are reserved for redundant connection to HSR ring B. The two remaining ports are inoperative.<br>**Note:**<br>Pay attention when using this configuration since no more standard Ethernet ports will be available and you will need to connect to the device by using an HSR compliant device (another H49 for example). |

In order to facilitate identification, each port is colored in relation to its configured function:

| Color | Description |
|---|---|
| Red | Redundant port |
| Green | Redundant port |
| Blue | HSR/PRP coupling port |
| White | Standard port |
| Grey | OFF port |

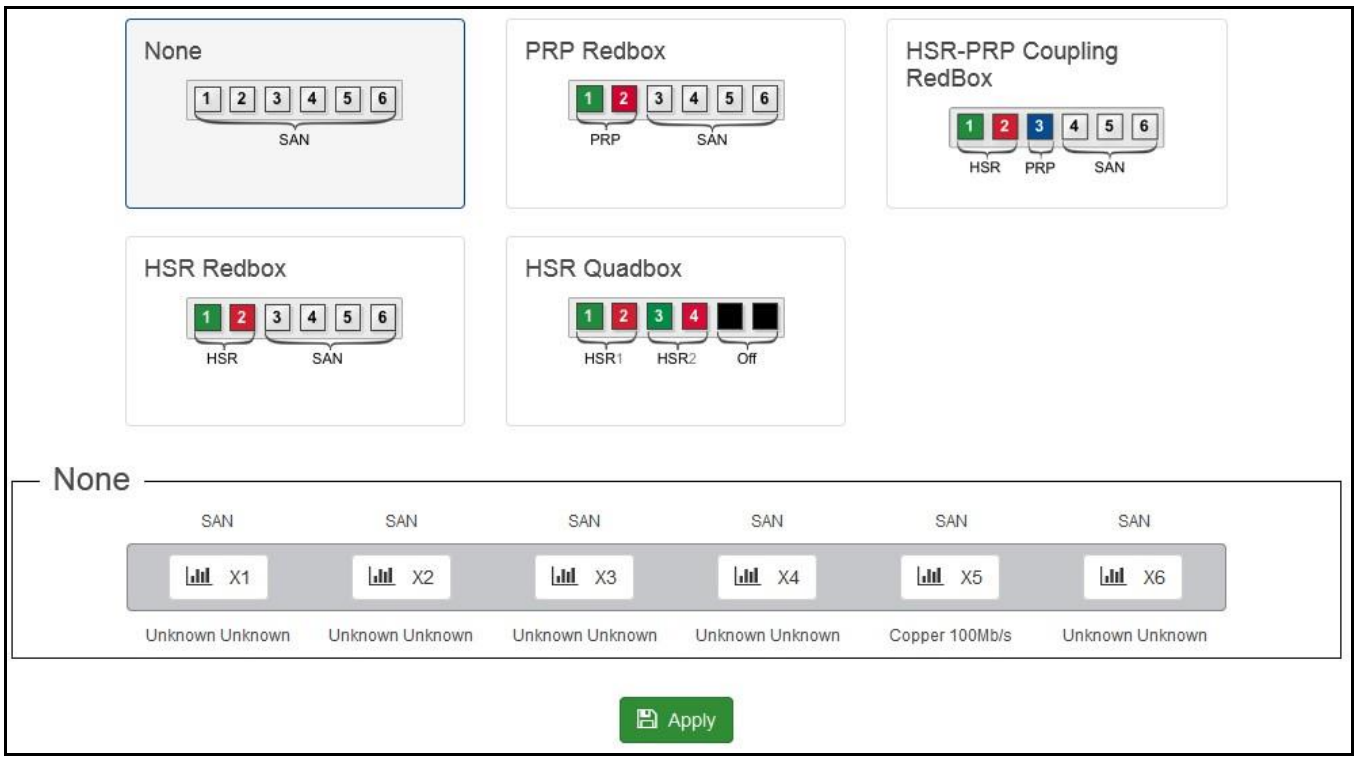



**Figure 52: Reason H49 Web User Interface – No Redundancy Mode Selected**

### Redundancy Mode Details

The lower part of the page changes according to the selected redundancy mode (highlighted in blue):

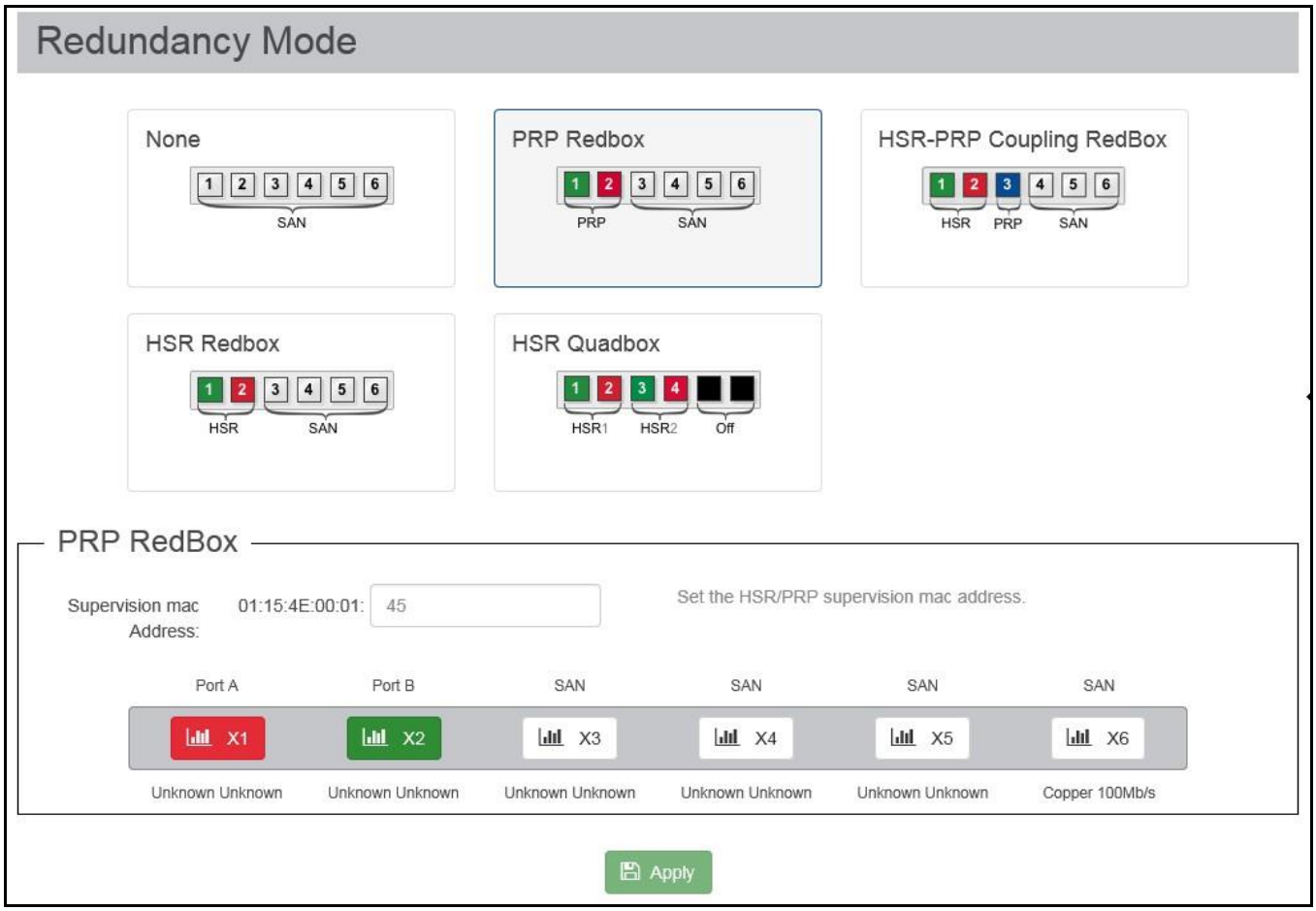



**Figure 53: Reason H49 Web User Interface – PRP RedBox Mode Selected**

Set the settings for the selected redundancy mode:

| Attribute | Description |
|---|---|
| Supervision Mac Address | Set the PRP or HSR supervision Mac Address |
| Network ID | Only displayed for "HSR/PRP coupling" redundancy mode.<br>It is an integer between 1 and 6 allowing the device to identify the network and to avoid duplicated packages.<br>**Note:** When coupling rings with two RedBoxes, both RedBoxes must be configured with the same Network ID. |
| LAN ID | Only displayed for "HSR/PRP coupling" redundancy mode.<br>It identifies the PRP LAN to be connected to the device.<br>**Note:** When coupling a ring with two RedBoxes, one shall be set on LAN A and the other one shall be set on LAN B. Pay attention not to configure both RedBoxes on the same LAN. |

***Note:***
*When switching from one redundancy mode to another, reboot Reason H49 to apply changes in the Start-up configuration. The system and network configuration will be erased except the **Name**; **IP address**; **Subnet mask** and **Gateway** attributes set in the **Global Settings** > **System** page. The security settings will be kept.*

#### 7.5.1.4 SNMP

Reason H49 implements **Simple Network Management Protocol** (SNMP) and is capable of exchanging information with other SNMP devices on the network. This information is saved in the Management Information Base (MIB) of the switch.

GE Vernova recommends considering the following items when using the SNMP service:

- Change the SNMP Priv and default passwords and ensure they are strong.
- Use only SNMP v3 to enhance cybersecurity and minimize risks.
- Change the community string or modify the default password.
- By default, SNMP is disabled and there is no SNMP WRITE permission on User Admin.

To configure the SNMP settings of the switch, click **System** > **SNMP**.

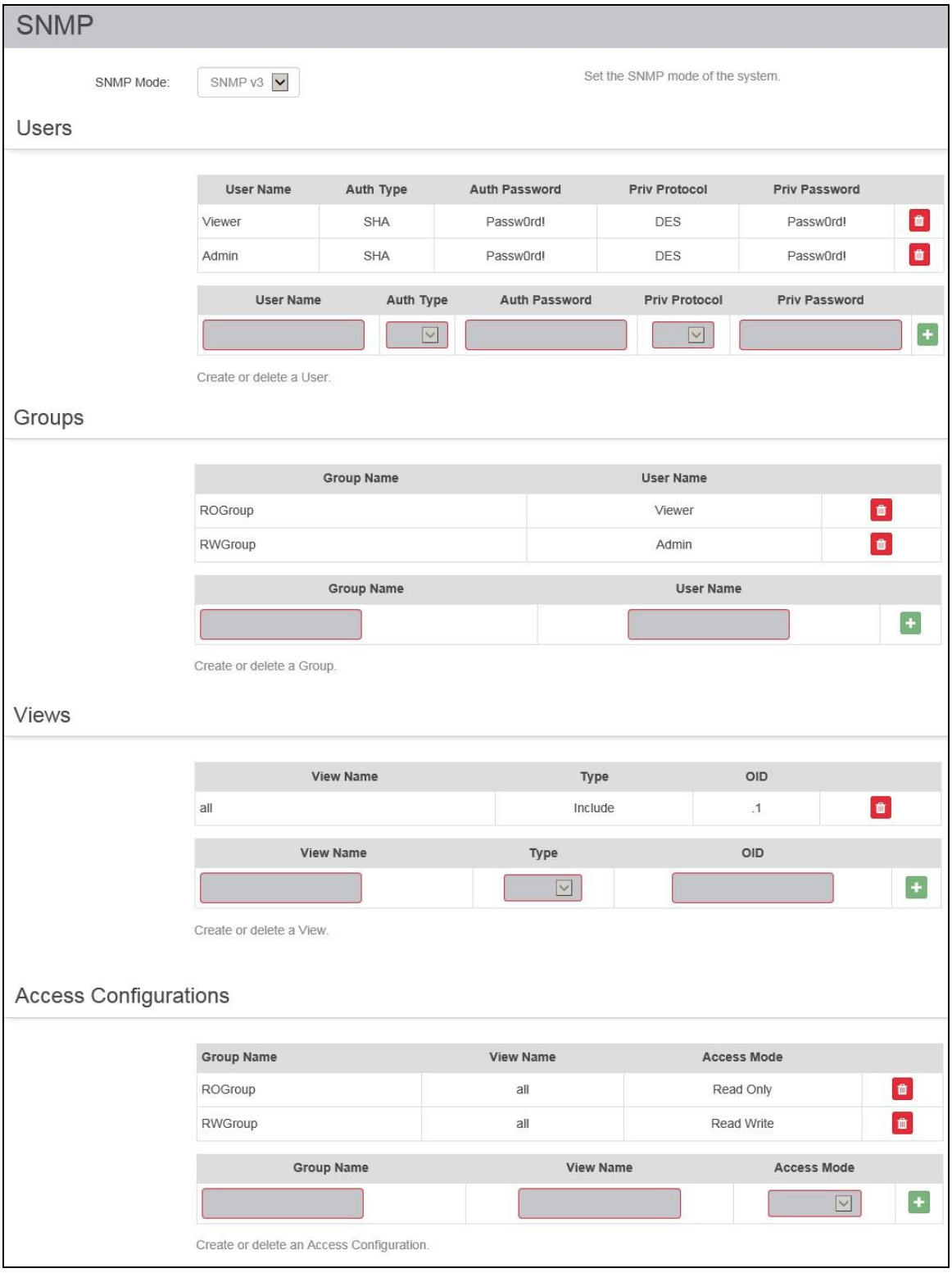



**Figure 54: Reason H49 Web User Interface – SNMP Page**

The content of this page depends on the selected SNMP version.

Reason H49 supports three versions of SNMP:

- **SNMPv1**: SNMPv1 uses a community string for authentication. The SNMP agent accesses all objects with read-only permissions using the community string public and/or all objects with read/write permissions using the community string private.
- **SNMPv2c**: SNMPv2c is a later version of the SNMP protocol. It supports the same community-based security standard.
- **SNMPv3**: SNMPv3 is the most secure protocol. It supports the View-Based Access Control Model and User- Based Security Model along with encryption and Authentication features.

The following table summarizes the sections corresponding to each SNMP version.

| | V1 | V2C | V3 |
|---|---|---|---|
| **Communities** | Yes | Yes | No |
| **Groups** | Yes | Yes | Yes |
| **Users** | No | No | Yes |
| **Views** | Yes | Yes | Yes |
| **Access configurations** | Yes | Yes | Yes |

Throughout the page:

- Click the **+** button to add a new element and set the related attributes as detailed below,
- Click the remove button in front of the desired row, to delete an element from a section.

### SNMP Version selection

From the SNMP mode drop-down list, select the desired SNMP protocol version to be used to manage the switch:

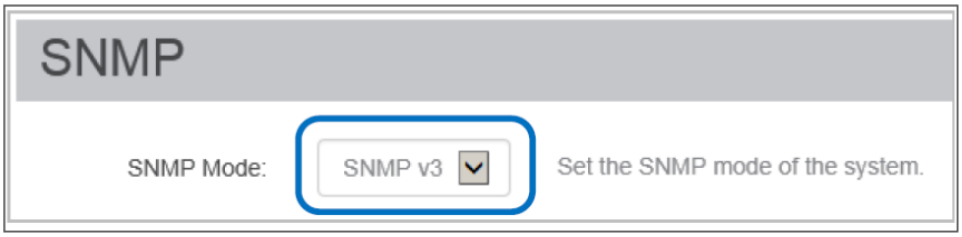



**Figure 55: Reason H49 Web User Interface – SNMP Version Section**

| Attribute | Description |
|---|---|
| **SNMP mode** | SNMP v1<br>SNMP v2c<br>SNMP v3<br>Disable<br>If the "Disable" option is selected then the SNMP protocol will be disabled in the device. |

### SNMP v1 and v2c

#### Communities

This section allows the user to create a new community by defining the community name and the community string (access mode):

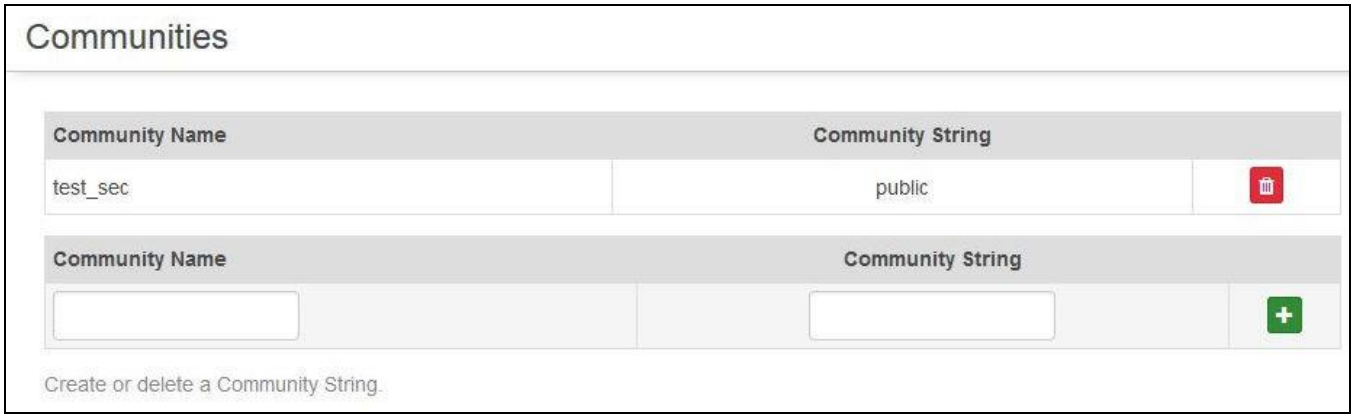



**Figure 56: Reason H49 Web User Interface – SNMP Community Section**

| Attribute | Description |
|---|---|
| **Community Name** | Name of the community |
| **Community String** | Authentication key to access the device (acts as a password) |

#### Groups

Manage user groups by defining the group name and the related community name:

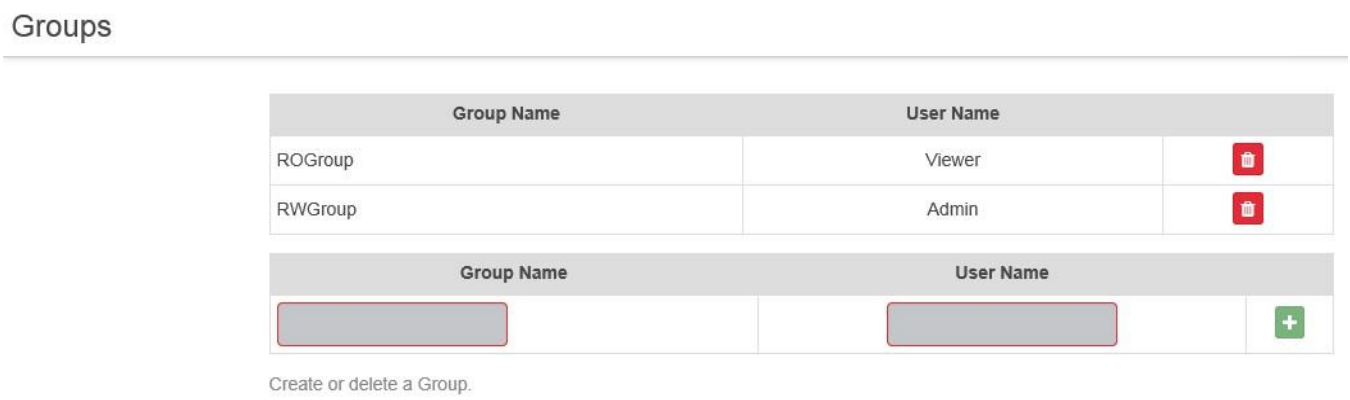



**Figure 57: Reason H49 Web User Interface – SNMP Group Section for SNMP v1/v2c**

| Attribute | Description |
|---|---|
| **Group name** | A unique group name |
| **Community Name** | List of existing communities |

### SNMP v3

### Users

This section allows the user to manage SNMP users:

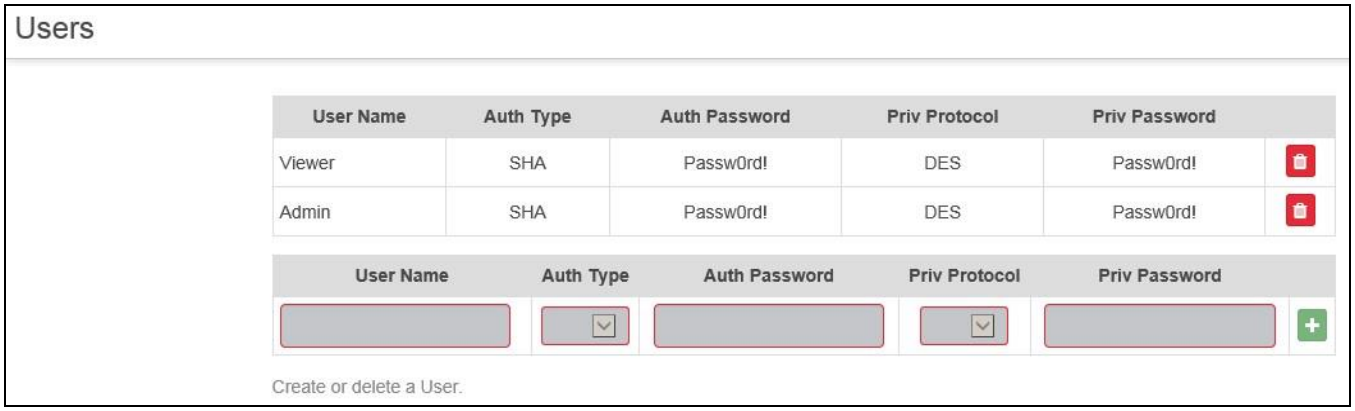



**Figure 58: Reason H49 Web User Interface – SNMP User Section for SNMP v3**

Set the SNMP users together with their authentication and their privacy attributes as detailed below:

| Attribute | Description |
|---|---|
| **User name** | User name |
| **Auth Type** | Authentication protocol.<br>Select the encryption algorithm for the authentication key:<br>MD5 (Message-digest algorithm)<br>SHA (Secure hash algorithm) |
| **Auth Password** | User's authentication Password |
| **Priv Protocol** | Select the privacy protocol to be used to encrypt the data of the SNMP Message:<br>AES (Advanced Encryption Standard)<br>DES (Data Encryption Standard) |
| **Priv Password** | User's privacy password |

### Groups

Manage user groups by defining the group name and the user that belongs to this group:

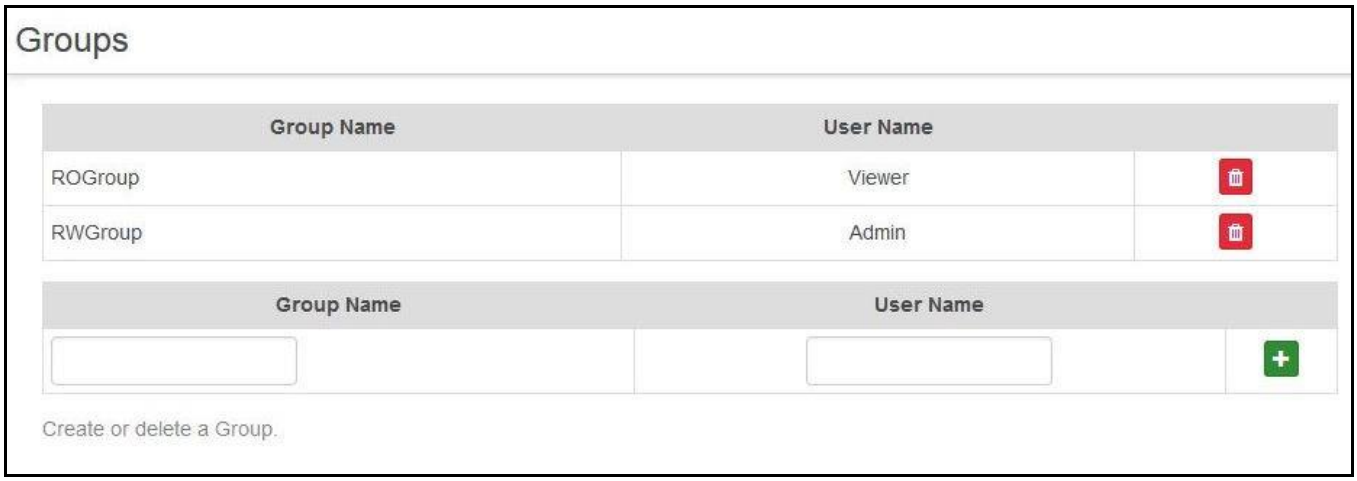



**Figure 59: Reason H49 Web User Interface – SNMP Group Section for SNMP v3**

| Attribute | Description |
|---|---|
| **Group name** | A unique group name |
| **User Name** | User attached to this group |

### All SNMP versions

### Views

This section allows the user to manage Views by defining their name and their related OID A given View is linked to a single OID (and its sub-OIDs)

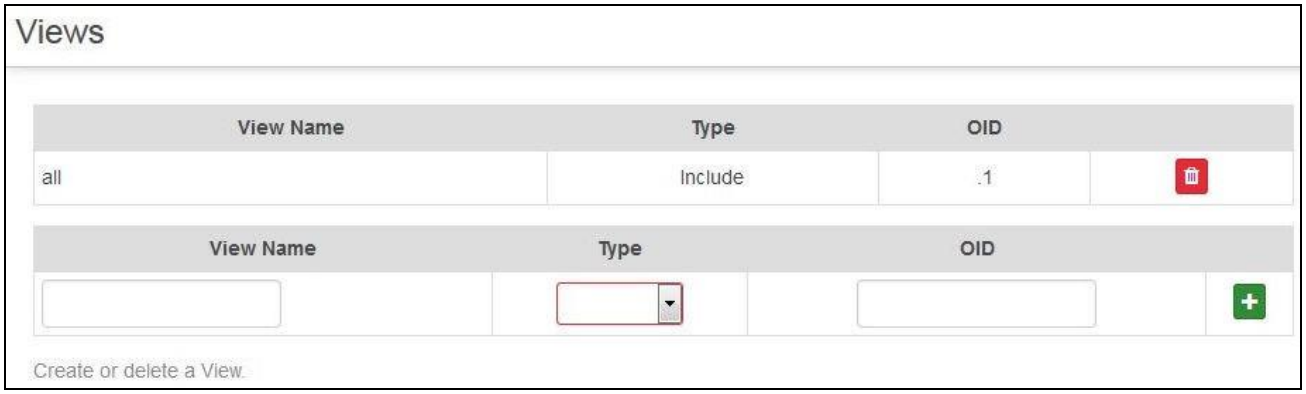



**Figure 60: Reason H49 Web User Interface – SNMP View Section**

| Attribute | Description |
|---|---|
| **View name** | A unique View name |
| **Type** | Include or Exclude mode:<br>**Include**: The given OID and all its tree will be visible for the group gathering this view<br>**Exclude**: The given OID and all its tree will be hidden for the group gathering this view |
| **OID** | OID associated with the view |

### Access Configurations

This section allows the user to link a Group and a View. A Group can gather more than one view.

You shall be careful not gathering two contradictory view in the same group; for example: gathering a View including a given OID and another view excluding the same OID.

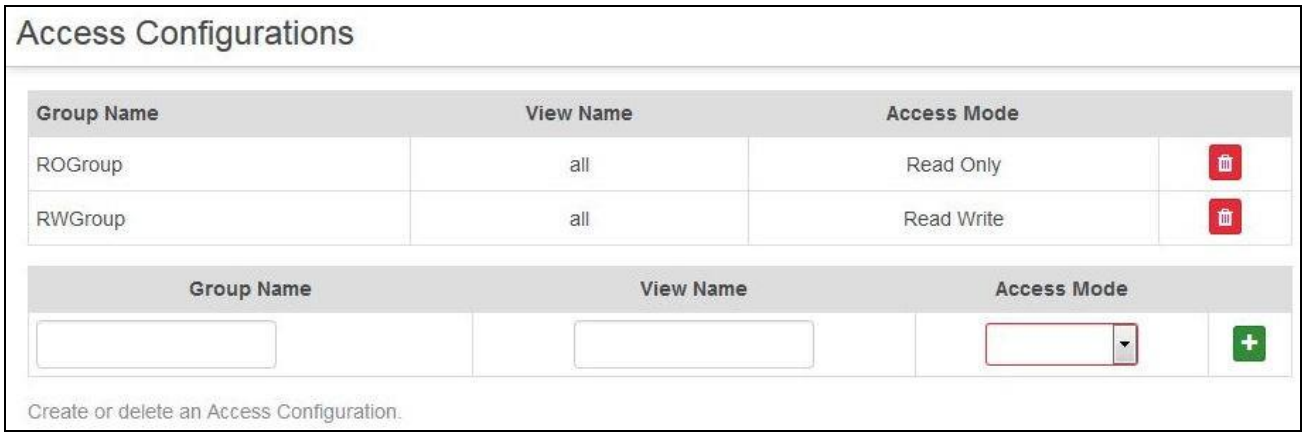



**Figure 61: Reason H49 Web User Interface – SNMP Access Configuration Section**

| Attribute | Description |
|---|---|
| **Group name** | List of existing groups |
| **View name** | List of existing Views |
| **Access Mode** | Access mode to the view (Read, Write) |

### 7.5.1.5 MANAGEMENT

This page allows the user to manage the firmware and configuration settings of Reason H49.

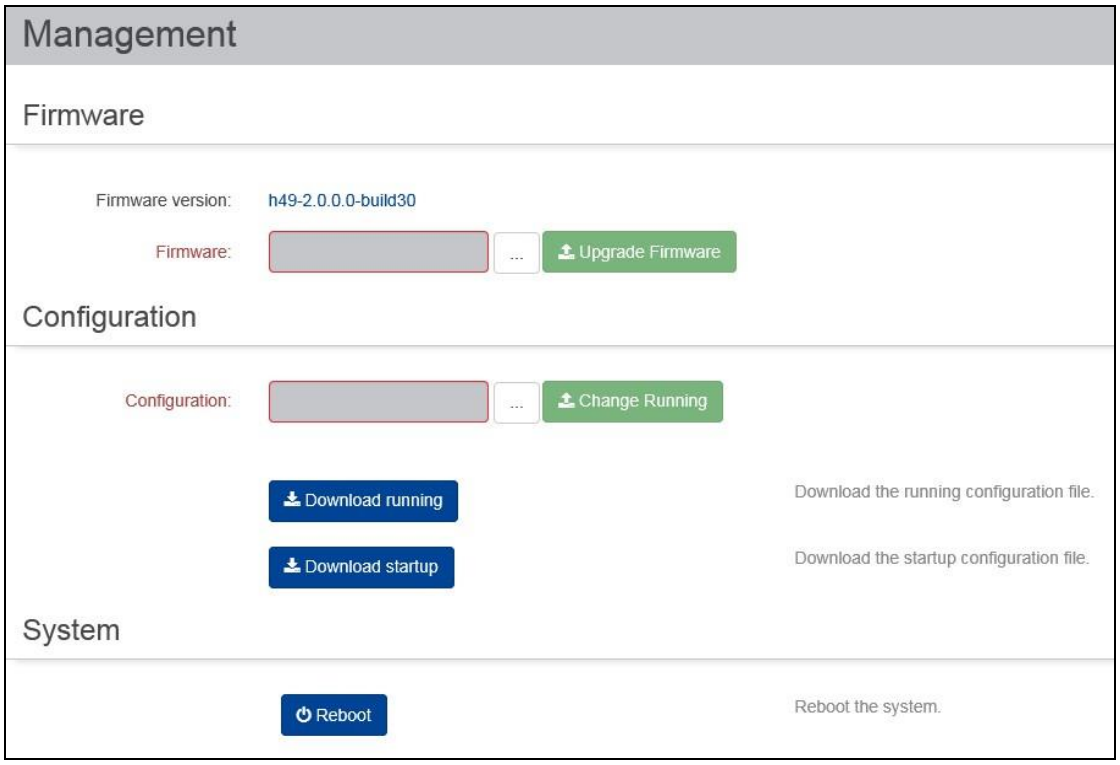



**Figure 62: Reason H49 Web User Interface – Device Management**

### Firmware Update

The Firmware section allows an authorized user to keep Reason H49 up to date with the latest firmware from General Electric or revert the switch to factory settings and firmware.

When firmware update is required, the first step to be done is requiring GE Vernova for the firmware file (***.tar.gz**). After this file is received, copy the file to the PC on which management interface of the switch is performed.

To update firmware, go to the **System > Management** menu.

- Click the "**...**" button and then, select the correct tar.gz file:

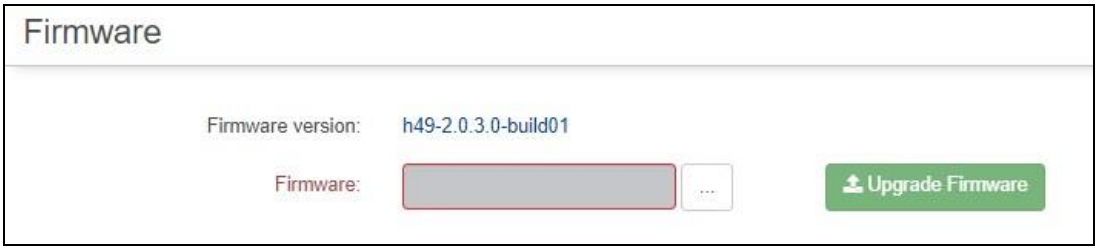



**Figure 63: Reason H49 Web User Interface – Select a Firmware File**

- Click the "**Upgrade Firmware**" button to activate the upgrade process:


**Figure 64: Reason H49 Web User Interface – Start the Upgrade Process**

The package signature is verified before allowing the firmware to be installed.

A popup prompts the user to decide whether he/she wants to keep the existing switch configuration settings (user accounts, logs, date/time…).

- Check the box to save the existing switch configuration and click **Confirm**:


**Figure 65: Reason H49 Web User Interface – Firmware Upload Confirmation**

Do not select “Check this box if you want to save the configuration before upgrading the firmware” if you are upgrading to firmware H49-2.1.0.

At the end of the upgrade process, the system will ask for a reboot.

### Configuration

Reason H49 runs internally two configuration files:

- **Running Configuration**: This file is the current configuration of the switch. When the **Apply** 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 Configuration** file.
- **Startup Configuration**: This file represents the configuration that the switch will run after it is powered up or restarted. If a change in the **Running Configuration** was performed and it is requested to maintain the **Running Configuration** at the **Startup Configuration**, the user must save it using the **Save Running as Startup** option, in the **Management** page.

### Import a New Configuration File

**Warning:**

**Before proceeding to the import, check that current redundancy mode (Quadbox, HSR, PRP…) is the same as the one specified in the configuration file.**

To import a new configuration file to the device, perform the following steps:

- Click the "**…**" button to navigate to the folder that contains the configuration file and then, select the relevant .yaml, yml file:

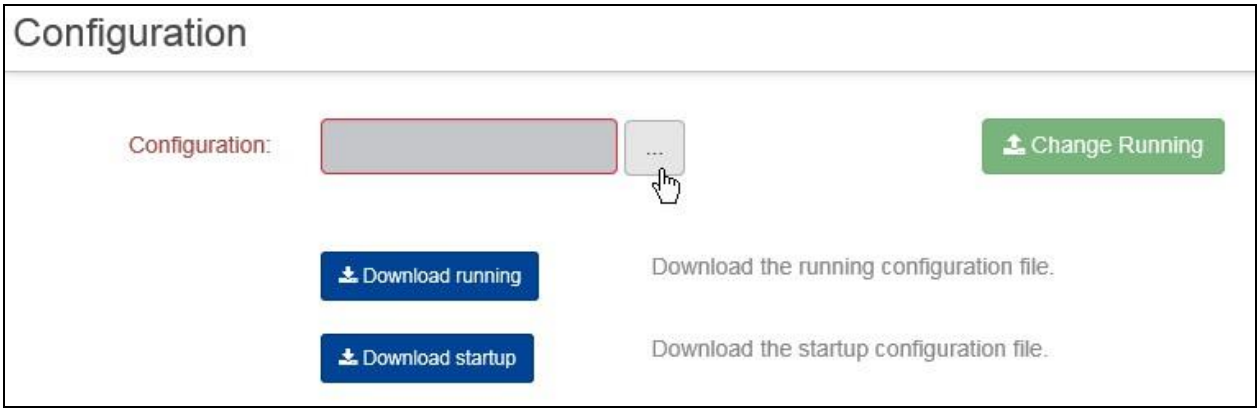



**Figure 66: Reason H49 Web User Interface – Select the Configuration File to be imported**

- Click "**Change Running**" to import the file.


**Figure 67: Reason H49 Web User Interface – Start the Upgrade Process**

At the end of the upgrade process, the new configuration is running on the device.

Only **System** and **Network** parameters are preserved in **Running** and **Startup** configuration.

A new button invites the user to save the Running configuration as Startup-configuration so it will be preserved after reboot.

### Running and Startup configurations are different

When the **Running** and the **Startup** configurations are different, a warning icon is displayed in the navigation menu as shown in the following figure.


**Figure 68: Reason H49 Web User Interface – New Configuration Notification**

A message warms the user in the **Management** page, as shown in the following figure:

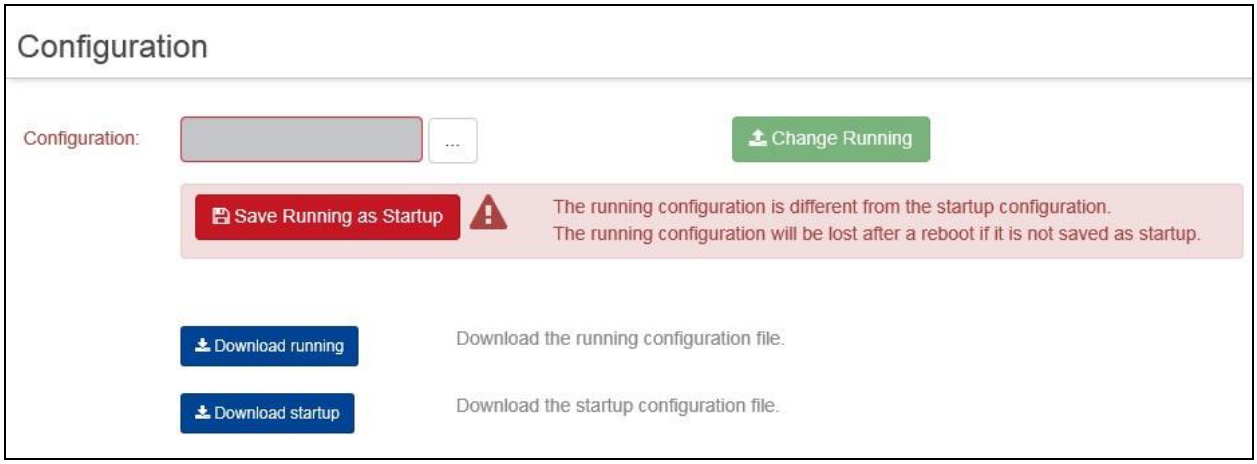



**Figure 69: Reason H49 Web User Interface – New Configuration Notification**

### Export Reason H49 Configuration File

It is possible to export the **Running** and/or the **Startup** configurations of the switch (.yaml file).

> ***Note:***
> *SNMP configuration is not included in configuration file exported.*

- Click the corresponding button as shown in the following figure.


**Figure 70: Reason H49 Web User Interface – Downloading Running or Startup Configuration**

From the popup that appears on screen, select **Save File** and click **OK** to save it to the local host:


**Figure 71: Reason H49 Web User Interface – Configuration Export**

By default, the file is saved to the **Downloads** folder onto your local host.

### System Reboot

The user can reboot the device by clicking the **Reboot** button:


**Figure 72: Reason H49 Web User Interface – Reboot Button**

The system will ask for confirmation before proceeding.

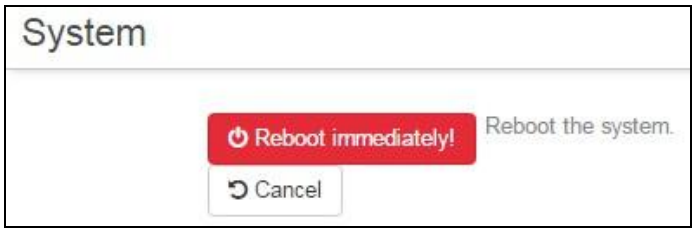



**Figure 73: Reason H49 Web User Interface – Confirmation Button**

To upgrade the H49 product from a release prior to h49-2.1.0, follow the process below:

1. Download the H49 configuration files.
2. Upgrade first to previous firmware release version h49-2.0.3.1, if it is not yet your current version.
3. Upgrade to h49-2.1.0.

4. DO NOT CHECK the option “Check this box if you want to save the configuration before upgrading the firmware.”
5. After the firmware upgrade, power off then power on the H49 product.
6. Restore your H49 configuration file.

## 7.5.2 NETWORK

This section provides the current network configuration of the Reason H49 switch.

### 7.5.2.1 INTERFACE

This page allows the user to configure the device’s interfaces available in the selected redundancy mode. Each interface is represented by a row in the table.

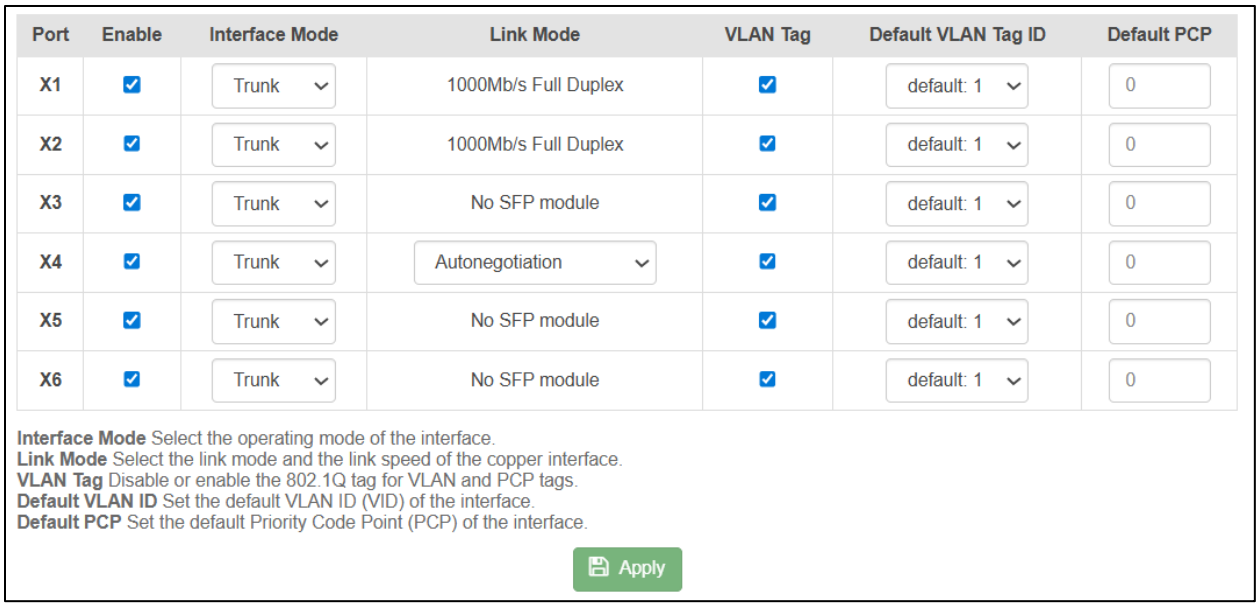
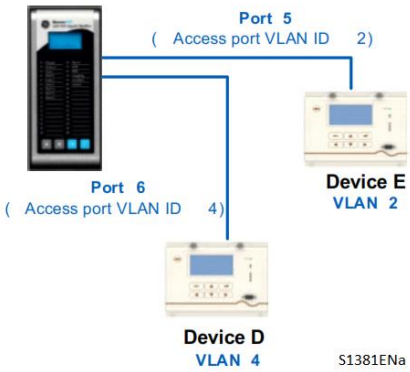
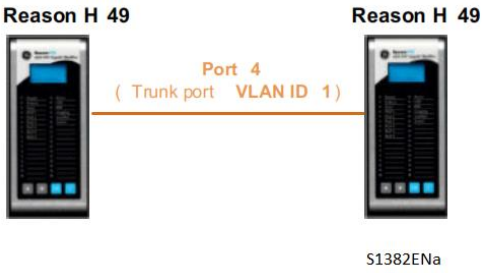



**Figure 74: Reason H49 Web User Interface – Interface Configuration**

***Note:***
*When the device is configured in QuadBox mode, ports 5 and 6 are deactivated, thus are not displayed in the list.*

Caution:
Be careful not to disable the port you are using for configuring the device. In the same manner, do not disable all the ports since it will not be possible to connect to the device afterwards. If, for any reason, you have disabled all the ports, reboot manually the device to reload the "Startup" configuration that is supposed to be correct.

Set the interface attributes as detailed in the table below.

| Attribute | Description |
|---|---|
| **Enable** | Check the box to enable a port. |
| **Interface Mode** | Reason H49 interfaces can be configured either as access ports or trunk ports, as follows:<br>**Access**: An access port can have only one VLAN configured on the interface; it can carry traffic for only one VLAN.<br>**Reason H 49**<br>  <br> |
| | **Trunk:** A trunk port can have two or more VLANs configured on the interface; it can carry traffic for several VLANs simultaneously. Usually, trunk link connection is used to connect two switches or switch to router.<br>  <br> |

**Warning:**
**An incorrect VLAN setting on access ports may cause communication failure with Reason H49. In such a case, you shall reset the switch to factory-default configuration, as explained in section "Revert to Default Factory Configuration".**

| | |
|---|---|
| **Link Mode** | Auto-negotiation must be selected as the Link Mode for copper SFP.<br>All other options will be disabled. |
| **VLAN Tag** | Check the box to enable the 802.1Q tag for VLAN and Priority Code Point (PCP) tags |
| **Default VLAN ID** | Enter the default VLAN ID (VID) for untagged devices that connect to that port |
| **Default PCP** | Enter the default Priority Code Point of the interface (0 to 7) |

***Note:***
*Refer to Appendix 3 for additional information about VLAN frame process.*

#### 7.5.2.1.1 REVERT TO DEFAULT FACTORY CONFIGURATION

You may experience communication failure if VLAN is not properly configured on the Access port. A common method to troubleshoot switching issues consists in reverting Reason H49 to default factory configuration by replacing the raw image stored at switch's memory.

When factory reset is required, the first step to be done is requiring GE Vernova for the raw file of the switch (**h49-x.x.x.x-buildxx-xx.tar.gz** file).

After this file is received:

- Copy the **h49-x.x.x.x-buildxx-xx.tar.gz** file to a PC.
- Unzip the file until you get the **h49-x.x.x.x-buildxx.raw** file.
- Download and install **Win32DiskImager.exe** application from the link https://sourceforge.net/projects/win32diskimager/.

  This free of charge program is designed to write a raw disk image to a removable device.

**Caution:**
**Disconnect all the power supply connectors before removing the switch case.**

- Disconnect all the power supply connectors.
- Remove the switch case by unscrewing the eight (8) cross-head screws as shown on the following figure:

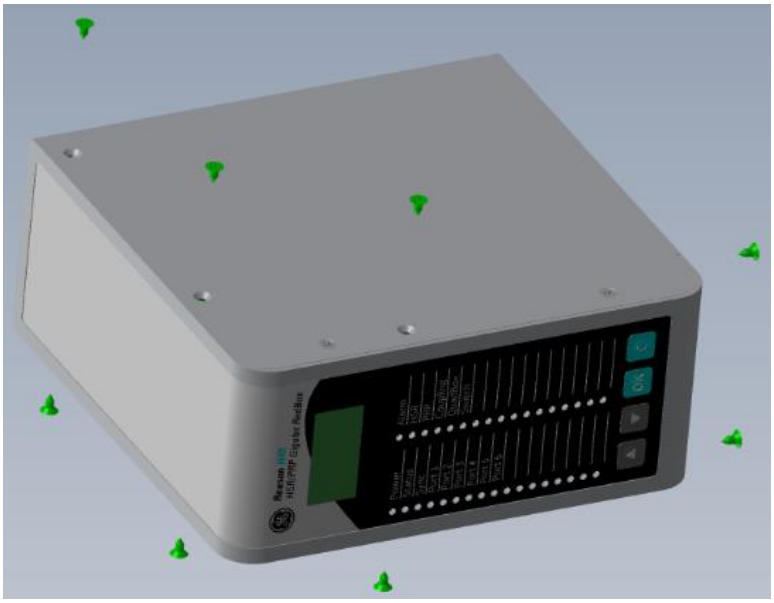


**Figure 75: Reason H49 – Location of M6 Screws to be removed**

- Remove the Micro SD card from the SRPV3 board:

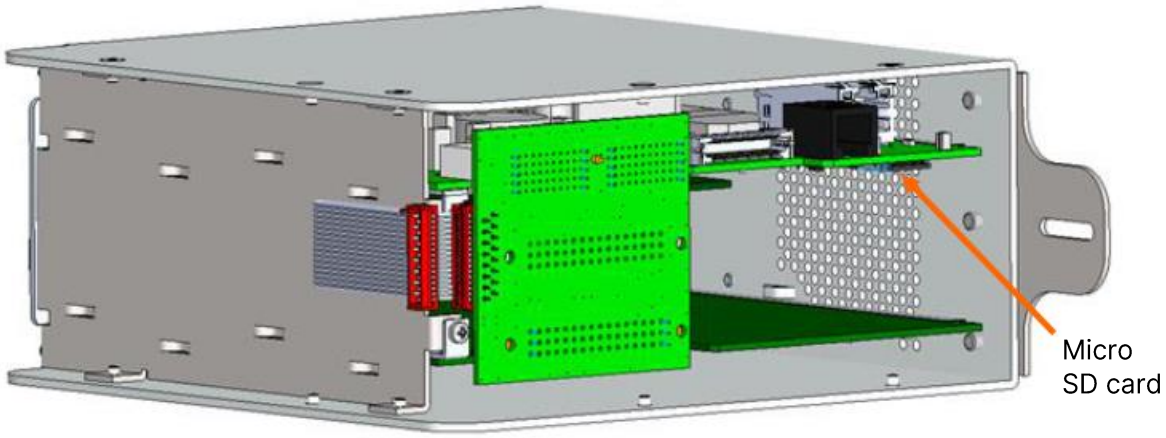



**Figure 76: Reason H49 – Location of the Micro SD Card**

- Insert the Micro SD card into your Windows PC's card reader. You may use an SD card adapter to fit into the SD card slot.
- Run the unzipped Win32DiskImager.exe application.
- From the **Device** drop-down list, select the SD card (ensure that the correct driver is selected):

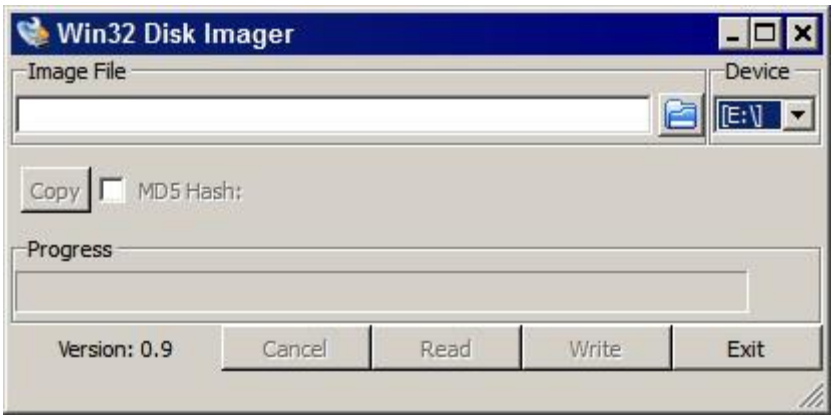



**Figure 77: Win32DiskImage Program – Select the SD Card Driver**

- Click the folder icon to open the file explorer. Set the **Files of type** to *.* and then, select the unzipped raw file. Click **Open**.

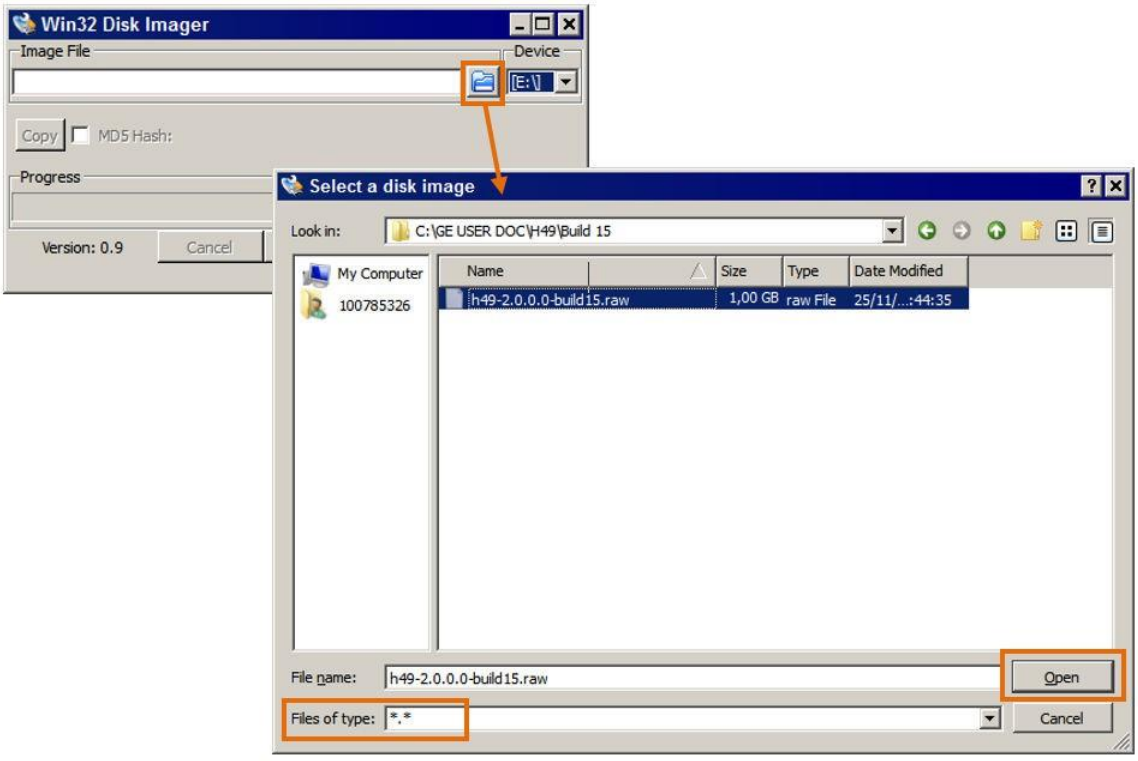



**Figure 78: Win32DiskImage Program – Select the Raw Image of the Switch**

- Click **Write** to copy the RAW image on the SD card.

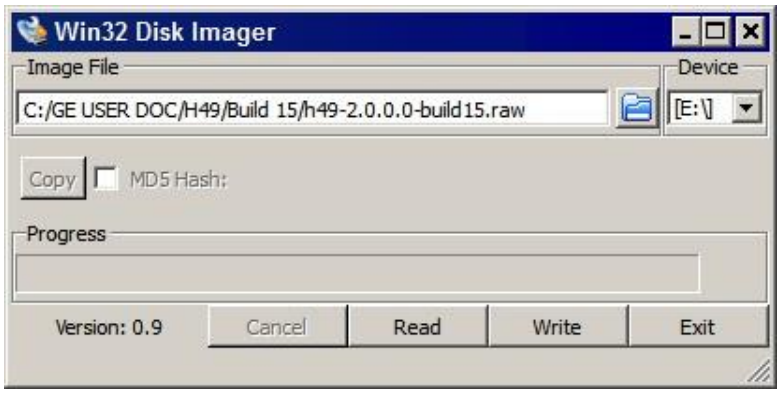



**Figure 79: Win32DiskImage Program – Start the File Copy**

A confirmation message appears on screen. Click **Yes** to continue.


**Figure 80: Win32DiskImage Program – Confirm Overwrite process**

- The raw file is being copied on the SD card.

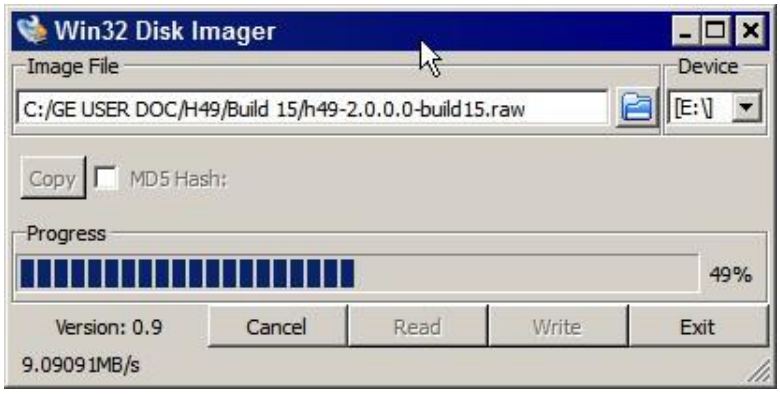



**Figure 81: Win32DiskImage Program – Overwrite process in progress**

- Once the process is complete, click **OK**.


**Figure 82: Win32DiskImage Program – Overwrite process done successfully**

- In the task bar of your PC, click the  icon to safely remove hardware and eject media.
- Remove the Micro SD card from your PC and insert it into the SRPV3 board.
- Screw the eight (8) M6 screws on the switch case.

#### 7.5.2.1.2 INSULATION RESISTANCE AND EARTH CONTININUITY CHECKS

If the unit is disassembled to access the internal Micro SD card, then the following checks must be made after the unit is reassembled and before use.

**Caution:**
**These tests must only be carried out by a maintenance operative having appropriate technical training and experience necessary to be aware of hazards to which that operative may be exposed in performing installation / maintenance and of measures to reduce the risks to that person or other persons.**

The unit must be unpowered and electrically isolated from the installation wiring by removing all connections with the exception of the safety Protective Conductor Terminal (PCT) connection to the equipment case, which may be left in place.

Ensure that all case fixings have been reinserted and tightened to the correct torque.

**Insulation Resistance Check**

- Connect the following pins together to form isolation groups on the unit under test:

| H49 Terminal Connections | Terminals | Isolation Group |
|---|---|---|
| **Primary Power Supply Input – Slot C** | 23 and 24 | 1 |
| **Secondary Power Supply Input – Slot B** | 1 and 2 | 2 |
| **Alarm Relay – Slot A** | 1,2 and 3 | 3 |

- Using an insulation resistance tester and taking care to follow the manufacturer's safety precautions, test between the following isolation groups with the output set to 500 V DC:

| Test # | First Isolation Group | Second Isolation Group |
|---|---|---|
| 1 | Primary Power Supply Input – Group 1 | Groups 2 and 3 connected to Case PCT |
| 2 | Secondary Power Supply Input – Group 2 | Groups 1 and 3 connected to Case PCT |
| 3 | Alarm Relay – Group 3 | Groups 1 and 2 connected to Case PCT |

- Verify that the insulation resistance of each test is >100MΩ.
- If any of the test measurements are <100MΩ then the root cause must be identified and rectified before the unit can be returned to active service.

**Earth Continuity Check**

- Using a continuity tester or Digital Multimeter, check that the resistance from the PCT to all other conductive case components on the unit is <1Ω.
- If any of the test measurements are not <1Ω then the root cause must be identified and rectified before the unit can be returned to active service.

### 7.5.2.2 VLAN

A physical network can be split into logical segments to create multiple Virtual Local Area Networks (VLANs). A VLAN gathers a group of devices that may be located anywhere on a network, but which communicate as if they were on the same physical network.

Setting up a Virtual Local Area Network (VLAN) is more flexible than traditional networks and easier to manage:

- Ease the relocation of devices on networks (no re-cabling)
- Extra security: devices within each VLAN can only communicate with other devices on the same VLAN. If a device on VLAN A needs to communicate with devices on VLAN B, the traffic must pass through a routing device.
- Restricted traffic: with traditional networks, traffic is directed to all network devices, regardless of whether or not they need it and may cause network congestion. VLANs are set up to contain only those devices that need to communicate with each other.

VLANs can manage traffic flow through Reason H49 to improve bandwidth utilization and security. To configure virtual LANs in Reason H49, click **Network** > **VLAN**.

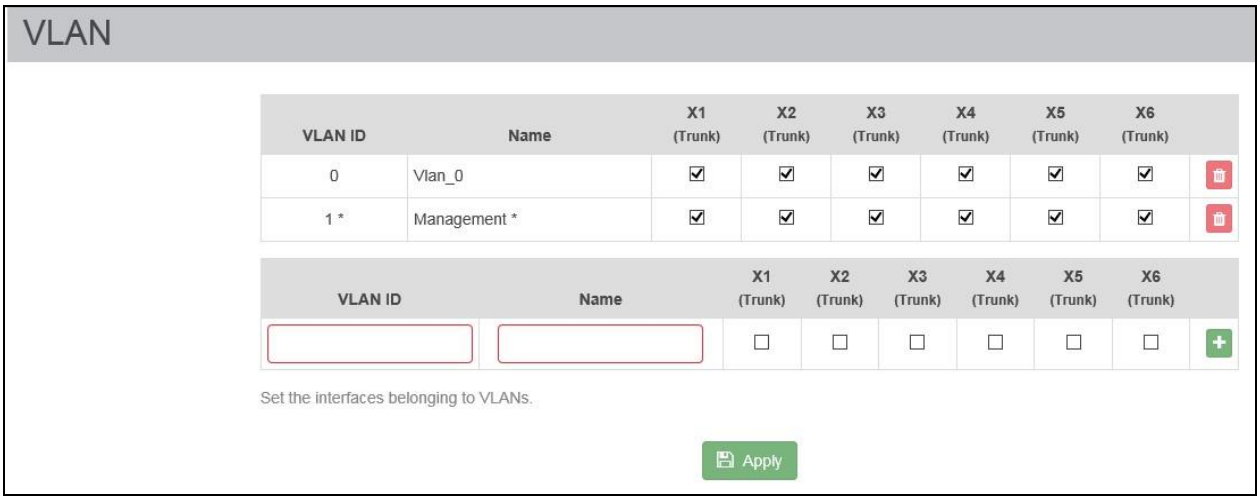



**Figure 83: Reason H49 Web User Interface – VLAN Configuration**

Reason H49 can manage up to 4096 configurable Virtual LANs. Each VLAN (starting from 2) can handle up to six VLAN ports.

Set the Virtual LAN attributes, as described below:

| Attribute | Description |
|---|---|
| **VLAN ID** | For tag-based VLANs, this is the ID to look for in the tag. It identifies the individual VLANs you create on your network. The VLAN ID must be specified in the range from 1 to 4094.<br>VLAN 0 is not used for VLAN routing but only to carry priority information.<br>VLAN 4095 is not allowed by the 802.1Q standard. It is not displayed in the page. |
| **VLAN Name** | Enter a unique name to identify the VLAN. This is used for display purposes only. |
| **X1 to X6** | Check the box for each port you wish to include in this VLAN. |

***Note:***
*In QuadBox configuration, the ports 5 and 6 might be disabled. Thus, we highly recommend checking the interfaces implied in the VLAN configuration against the selected redundancy mode.*

It is possible to remove a VLAN by clicking on the corresponding **Remove** icon.

***Note:***
*Refer to Appendix 3 for additional information about VLAN frame process.*

### 7.5.2.3 MULTICAST FILTERING

Ethernet protocol supports multicast messages. A multicast is a packet sent by one host to multiple hosts.

The multicast filtering is a mechanism where information is filtered and then addressed to a group of destination hosts simultaneously.

Only those hosts that belong to a specific multicast group will receive the multicast message as show.

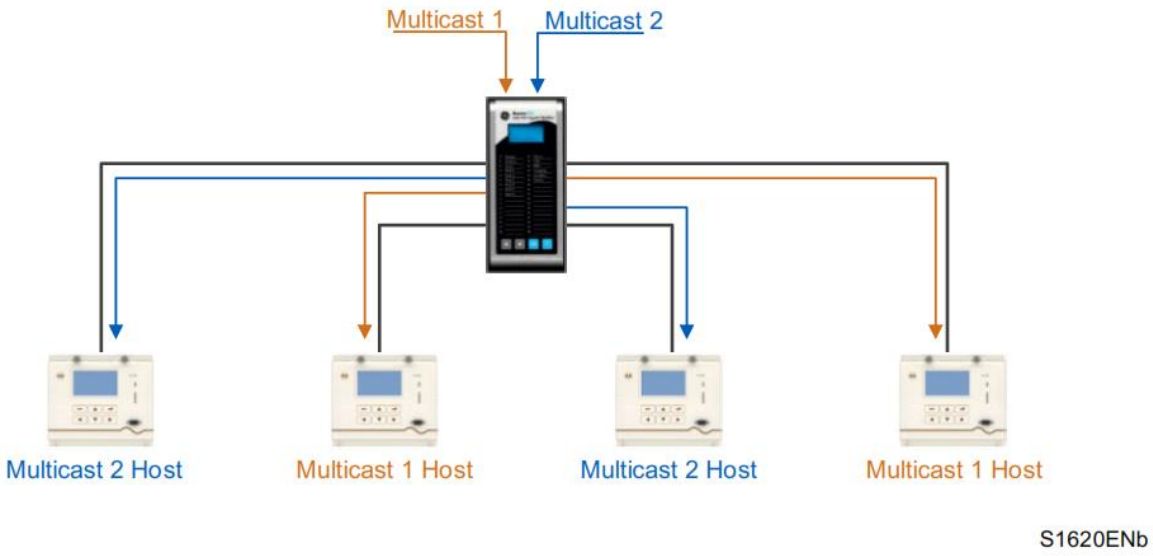



**Figure 84: Multicast Filtering Principles**

Reason H49 supports adding MAC addresses manually to restrict or filter multicast traffic automatically.

The filter relies on a range of MAC addresses applied to one or more device ports (interfaces).

To manage Multicast filtering rules, click **Network** > **Multicast Filtering**.

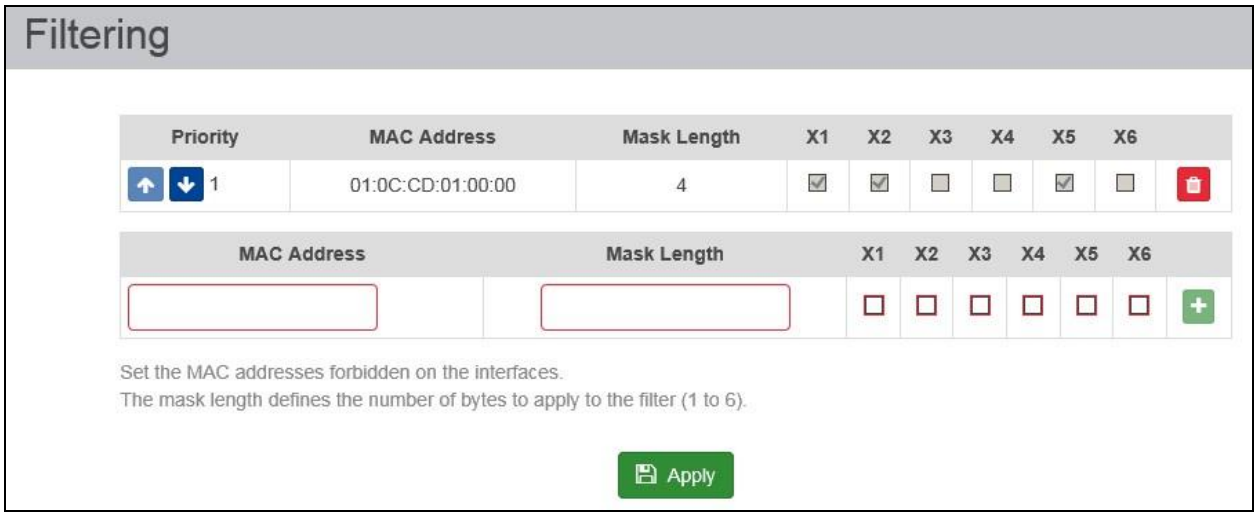



**Figure 85: Reason H49 Web User Interface – Multicast Filtering Configuration**

Add multicast MAC addresses manually:

| Attribute | Description |
|---|---|
| **MAC Address** | MAC addresses to create the filters |
| **Mask Length** | Number of bytes to apply to the filter (1 to 6) |
| **X1 to X6** | Ports over which the frame is allowed. On the non-selected ports the frame is not allowed. |

### 7.5.2.4 PRIORITY

Reason H49 provides a mechanism for prioritizing Ethernet frames by using Priority Code Points.

Four priority queues (from 0 to 3) are present in Reason H49 (3 being the highest priority) and eight Priority Code Point (PCP) can be distributed among the queues.

- To configure priority queues, click **Network > Priority**.

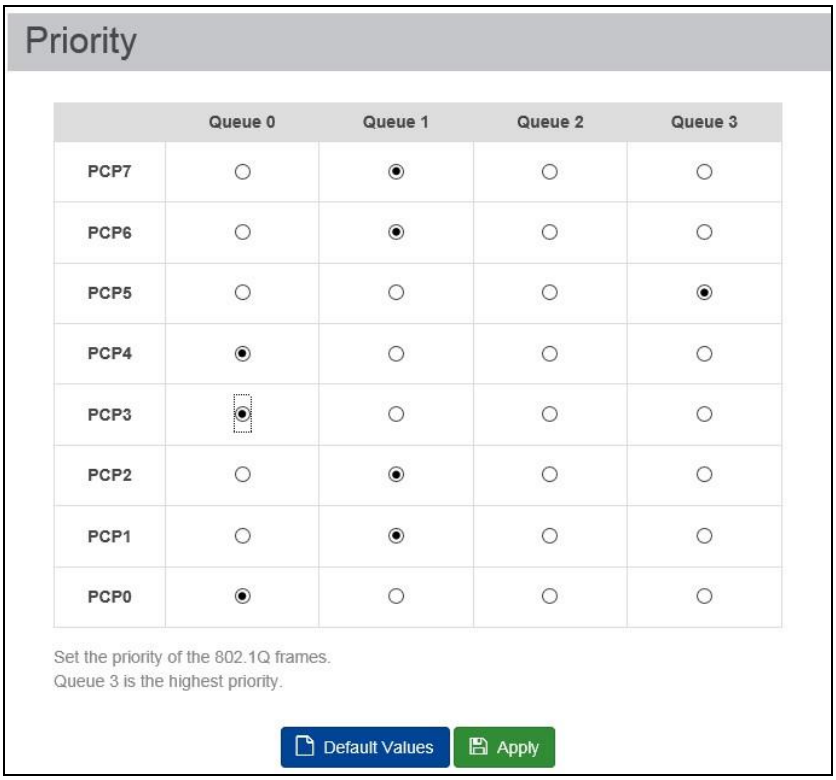



**Figure 86: Reason H49 Web User Interface – Priority Configuration**

Set the priority mechanism as described below:

| Attribute | Description |
|---|---|
| **Queue 0 to Queue 3** | Select the queue for which the PCP is set.<br>A given queue can be associated with 0 or more PCPs |
| **PCP0 to PCP7** | Priority Code Point (PCP)<br>Only one Queue can be selected for each row. |

Click the **Default Values** button to reset the H49 to factory defaults:

- **Queue 3**: PCP6 ; PCP7
- **Queue 2**: PCP4 ; PCP5
- **Queue 1**: PCP2 ; PCP3
- **Queue 0**: PCP0 ; PCP1

## 7.5.3 SECURITY

This section is divided into four pages:

- Security settings
- User Accounts
- LDAP Server
- Syslog server

### 7.5.3.1 SECURITY SETTINGS

To configure security settings, click **Security > Security Settings**.

From this page, you can set the user and system management parameters and manage TLS and trusted certificates.

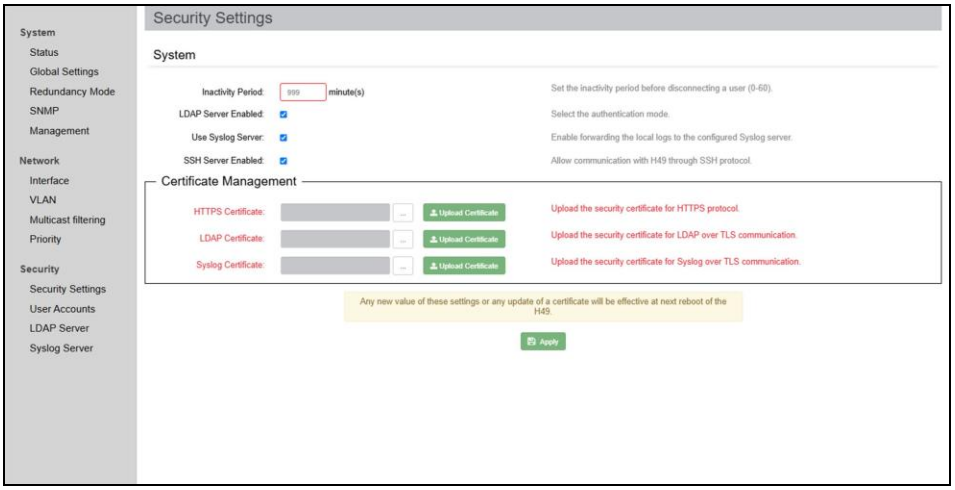



**Figure 87: Reason H49 Web User Interface – Security Configuration**

#### System

Set the system security settings as described below:

| Attribute | Description |
|---|---|
| **Inactivity Period** | Sets the inactivity period before disconnecting a user.<br>If Period equals 0, then no disconnection time will be applied. |
| **LDAP Server Enabled** | Enables / disables the use of LDAP server.<br>Local authentication uses the set of user and roles defined in the **User Accounts** page, while LDAP uses the configuration defined in LDAP page.<br>If LDAP server is enabled, then the LDAP server provides both authentication and roles assigned to user accounts.<br>if the roles assigned to a user change, the user needs to re-login to apply the new roles. |
| **Use Syslog Server** | Reason H49 device keeps a local log file.<br>This option makes it possible to forward the local logs to the configured Syslog server. Server attributes are configured in Syslog page. |
| **SSH server Enabled** | Enables / Disables the SSH server connection. |

**Caution:**
**It is recommended to keep SSH Server enabled while configuring sensible settings that could prevent login via the Web application (e.g., HTTPS certificates). When SSH is disabled the Web Application is the only way to communicate with the H49.**

**Caution:**

**To manage system certificates from the Security Settings page, you must be a Security Administrator.**
**Ensure that the certificate resides on the file system of the computer where your browser is running.**

For more details about certificates to be used, refer to Certificate Management section. To upload certificates, perform the following steps:

- Click the "**…**" button to navigate to the folder that contains the desired certificate, then select the relevant certificate and click **Upload Certificate**.
- Click **Apply** to save the modifications


**Figure 88: Reason H49 Web User Interface – Certificate Management**

### 7.5.3.2 USER ACCOUNTS

As an administrator, you can configure local user accounts and **local user account** policy from the **Security > User Accounts** menu.

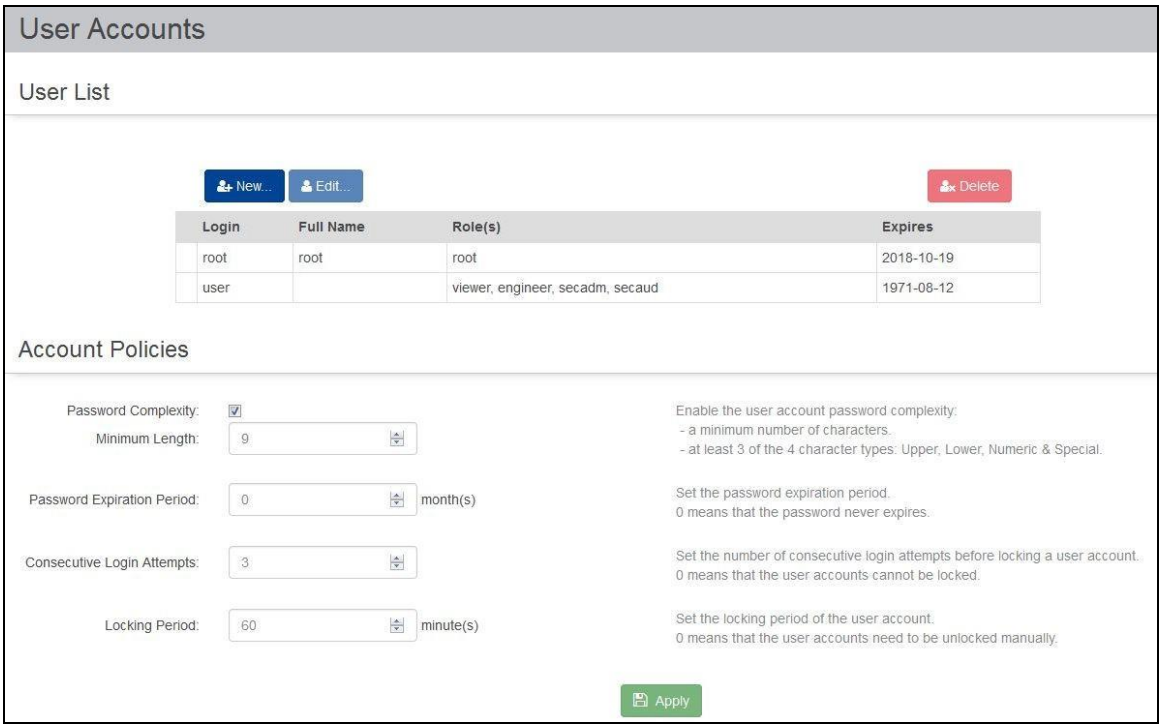



**Figure 89: Reason H49 Web User Interface – Local User Account Configuration**

***Note:***
*Password Expiration Period setting is only used for new user accounts.*

***Note:***
*This page allows the user to create, edit and remove local user accounts. These user accounts are used only if no LDAP account management has been defined or if the LDAP server is not accessible. If local authentication is used, then its associated authorization will also be local.*

***Note:***
*When LDAP is enabled, LDAP user accounts will follow the LDAP server account policies.*

**Caution:**

**As a system administrator, you MUST NOT edit or change your own password from the Security > User Accounts menu as your new password will not be taken into account by the system.**
**To change your administrator password, click on the user icon in the top- right corner of the web application and then select Account Settings.**

Set the user account properties as described below:

| Attribute | Description |
|---|---|
| **Password Complexity** | Enables account password complexity. When checked, user's password shall fit the following restrictions:<br>Minimum length of password<br>At least four (4) character types: Upper, Lower, Numeric & Special |
| **Minimum Length** | Sets the minimum number of characters required when Password Complexity is checked. You can select a value between 3 and 20 |
| **Password Expiration Period** | Password expiration period defined in months between 0 and 24.<br>0 means that the passwords never expire. |
| **Consecutive Login Attempts** | Number of consecutive login attempts before locking a user account.<br>0 means that this policy is disabled.<br>The maximum number of attempts is 10. |
| **Locking Period** | Set the locking period of the user accounts.<br>0 means that the user account will be locked until a user with appropriate privileges manually unlocks it. |

The following data is displayed for the existing **local** accounts:

| Attribute | Description |
|---|---|
| **Status** | Shows the current account's status.<br>No icon shown: There is no special issue concerning the account.<br>  <br>The account has been disabled by the security administrator (see Edit User Account section).<br>  <br>The account has been locked by the system after some login attempts. The user has to wait until the end of the security time (see Locking Period in Security Settings section). However, the security administrator can manually unlock the account (see Security Settings section). |
| **Login** | Account's login |
| **Full Name** | Account's name |
| **Role(s)** | Roles assigned to the corresponding account |
| **Expires** | Password expiration date |

Three action buttons are also provided in this page allowing the following functions:

- **New**: creates a new local account
- **Edit**: modifies the selected account
- **Delete**: removes the selected account

### Create a new user Account

The **User Accounts** window allows the user to create a new local user. Login and password are mandatory whereas the other fields are optional.

- To create a new local user account, click **New**:

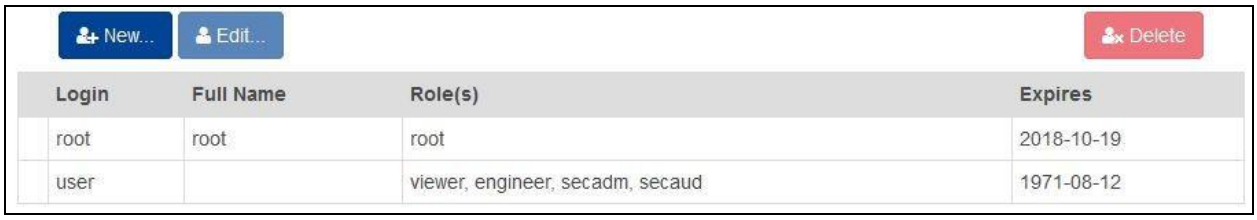



**Figure 90: Reason H49 Web User Interface – Create Local User Account**

In the **Account Settings** popup, complete the following attributes:

| Attribute | Description |
|---|---|
| **Login** | Unique login name |
| **Full Name** | User's name |
| **Password** | User's password. Automatic default password is generated when opening the New window.<br>Special characters will not be accepted. |
| **Roles** | User's role:<br>**Viewer**<br>**Engineer**<br>**Security Administrator**<br>**Security Auditor** |
| **Disable the user account** | A new disabled account can be generated by checking this option. |

- Click **Save** to save the new user account. Modifications are immediately applied.
- Click **Cancel** to cancel the user account creation. The entries are lost and the window is closed.

***Note:***
*Local accounts are accessible only if no LDAP server is defined or if it is disabled or unreachable.*

### Edit a User Account

All user accounts are modifiable (name and password), including the default factory account.

To edit an existing local user account:

- Select the account to be modified and then, click **Edit**.


**Figure 91: Reason H49 Web User Interface – Edit a Local User Account**

In the **Account Settings** popup, make the relevant changes.

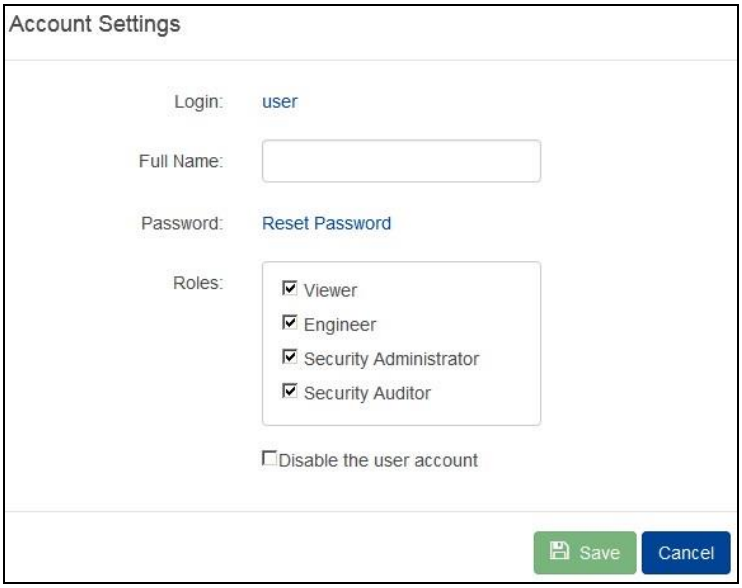



**Figure 92: Reason H49 Web User Interface – Change Settings of a Local User Account**

If the selected user's account is locked, an unlock button is available for users with **Security administrator** role. A **Reset password** option is also available for users with **Security administrator** role. In this case, the system generates a new automatic password that the user can update.

It is highly recommended to change the reset password upon the first utilization of the user account. If the roles assigned to a user change, the user will need to re-login in order to apply the new roles.

### Account Settings

Users can update their own account settings. These attributes are accessible by clicking on the user icon in the top- right corner of the web server application:

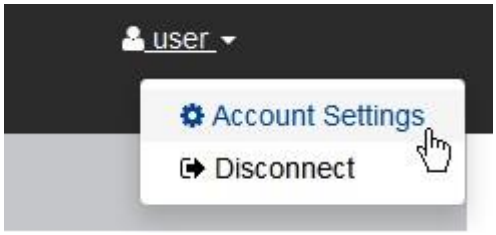



**Figure 93: Reason H49 Web User Interface – User Account Settings Icon**

The attributes displayed in the **Account Settings** window are:

- Login
- Full Name

- Current Password
- New Password
- Confirm Password

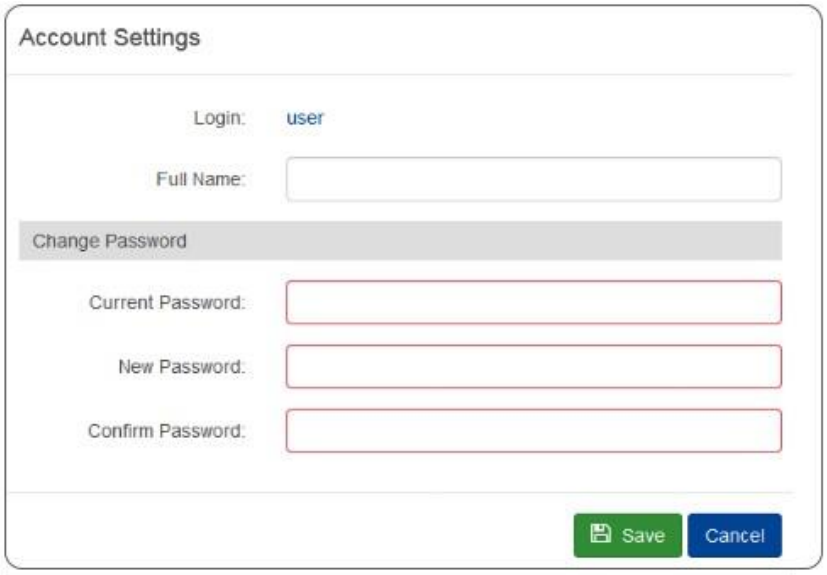



**Figure 94: Reason H49 Web User Interface – Account Settings**

### 7.5.3.3 LDAP SERVER

This page allows configuring the LDAP server for central authentication (Refer to section 8.1.4.1 Central Authentication for more information).

The information in this page is used when the LDAP authentication mode is selected in the **Security > Security Settings** page (see Security Settings section), this section describes how to enable/disable LDAP and how to import TLS certificate.

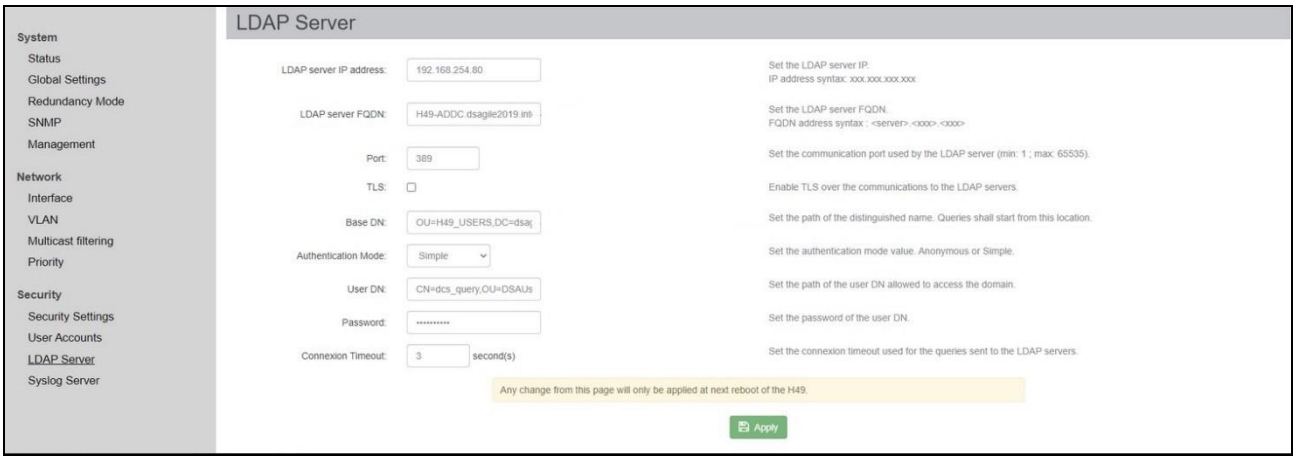



**Figure 95: Reason H49 Web User Interface – LDAP Server Settings**

| Attribute | Description | Examples |
|---|---|---|
| **LDAP Server IP address** | LDAP Server's IP address | 192.168.254.80 |
| **LDAP Server FQDN** | Complete domain name of the LDAP Server using the Fully Qualified Domain Name (FQDN). | H49-ADDC.dsagile2019.intern |
| **Port** | Communication port used by the LDAP servers | 389 |
| **TLS** | Enables the TLS encryption over the LDAP communication channel. If TLS is checked, a certificate must be installed (See Security Settings section) | |
| **Base DN** | Base Distinguished Name in the LDAP server | OU=H49_USERS,DC=dsagile2019,DC=intern |
| **Authentication Mode** | Authentication access mode to the LDAP server:<br>Simple<br>Anonymous | |
| **User DN** | User account authorized to request data to the LDAP server. It shall be provided if the Simple Authentication Mode is selected. | CN=dcs_query,OU=DSAusers,OU=DSAgile,DC=dsagi le2019,DC=intern |
| **Password** | Password associated to User DN | |
| **Connection Timeout** | Connection timeout in seconds used for the queries sent to the LDAP server.<br>After timeout, the client considers that the requested server is out of service. | 3 |

In any case, the Reason H49 switch cannot edit the passwords associated to LDAP-managed accounts.

> ***Note:***
> *If the LDAP server is temporarily unreachable, you may experience access issues to user management features (User Account creation...) from the H49. The operation can take time due to LDAP connection timeout.*

### 7.5.3.4 SYSLOG SERVER

A Syslog server is used for logging any message of events that occur on the host. The list of activities and operations, which are logged, is detailed below:

| General | Authentication | Security | System |
|---|---|---|---|
| Startup log | Login failed (Invalid user account, wrong password, account Locked, session already active, | Security settings updated | System settings updated |
| Shutdown log | Login successful | User account changes (password reset, change of role),<br>User account created, locked, unlocked, removed | Time/date change |
| | Logout (Timeout, User log off) | Role (assigned to and removed from user account) | Firmware/application update |
| | | Certificate management | Database switch |
| | | Central authentication server activity (reachable or not) | System stopped/rebooted |
| | | Syslog server activity (reachable or not) | |

This Syslog Server feature allows the user to configure a Syslog server.Attributes in this page will be taken into account only if the Syslog server has been selected in the **Security > Security Settings** page (see Security Settings section).

| Attribute | Description |
|---|---|
| **Hostname** | Server's IP address or Fully Qualified Domain Name |
| **Port** | Communication port used by the Syslog server |
| **Communication Protocol** | Communication protocol used to send the logs to the Syslog server"<br>UDP<br>TCP<br>TCP/TLS |
| **Maximum Rate per Second** | Maximum number of messages sent per minutes to the Syslog server |

When UDP is used:

- If the log server is reachable, then the log messages are sent to the server "on-the-fly"; in other words, messages are not buffered and sent in batch to the server.

When TCP or TCP/TLS is used:

- If the log server is unavailable, the log messages are temporarily buffered and they are sent to the server upon service reestablishment.

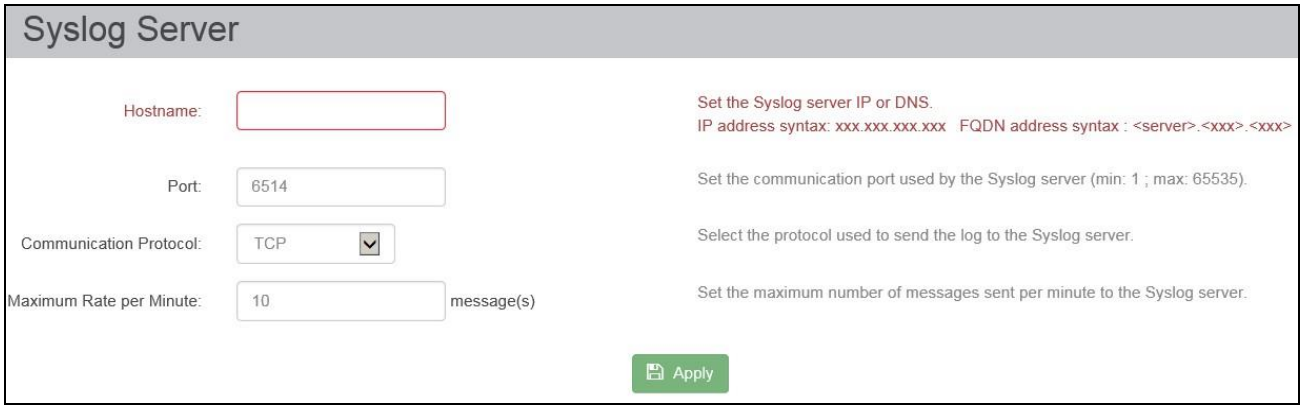



**Figure 96: Reason H49 Web User Interface – Syslog Server Settings**

## 7.5.4 BACKUP RESTORE

This chapter describes the procedure to backup and restore the H49 settings to make possible a quick and easy restoration of the device in case of failure (or disaster).

Unlike the proprietary YAML configuration file import/export feature (Refer to section **7.4.1.5 Management**). This functionality allows to backup/restore exhaustively the system settings (system settings, cybersecurity configuration, certificates, SNMP) in a backup file archive.

Configuration Backup and Restore are operated only from the CLI (Refer to the section **12.1.4 CLI Commands** for further information). The configuration Backup/Restore functionality is available only for users with **Engineer** role.

**Warning:**
**The restoration of a Backup archive can be done only at the same firmware version as the one on which it has been generated.**

**Warning:**
**Each H49 has a unique MAC address, so a restore operation performed on an H49 won't alter its MAC address.**

### 7.5.4.1 BACKUP OPERATION

This section describes how to generate and export an H49 configuration backup archive from an H49.

***Note:***
*If the firmware or the settings have been updated, it is mandatory to create a new backup.*

#### 7.5.4.1.1 GENERATE H49 BACKUP CONFIGURATION ARCHIVE

Start an ssh session with a user with the **Engineer** role and enter the following CLI command:

```
firmware --backup
```

This command generates a configuration backup archive file named **h49_conf_backup.dat** in the H49 **/tmp** directory.

#### 7.5.4.1.2 EXPORT AN H49 BACKUP CONFIGURATOIN ARCHIVE FROM AN H49

To store a backup archive file out of an H49 for further use. it must be exported from an H49. This can be done through SCP. On an H49, the backup archive file **h49_conf_backup.dat** is located in **/tmp** directory

It is recommended to store the backup archive file in a secure place with associated useful information (backup date, firmware version, device identification…).

***Note:***
*As example, from a Windows 10 PC, this can be done with the native SCP Windows command as explained below.*

Start the "Windows Command prompt" and send the command:

```
scp -o "UserKnownHostsFile=/dev/null" -o "StrictHostKeyChecking=no"
user@192.168.254.254:/tmp/h49_conf_backup.dat C:\02-Config\H49
```

- "H49 user account" (here user)
- "H49 IP address" (here 192.168.254.254)
- "PC destination folder" (here C:\02-Config\H49)

After this command execution, the password of "user" account from H49 will be required before the configuration backup archive file "**h49_conf_backup.dat**" is available on your PC.

### 7.5.4.2 RESTORE OPERATION

This section describes the steps to import an H49 configuration backup archive to a H49 and how to restore it.

**Warning:**

**Before proceeding to restore the H49 firmware configuration on a new H49, install the same firmware version as on the original H49. This can be done in either of two ways:**

- **Via the SD card: Refer to section 7.4.2.1.1 <Revert to Default Factory Configuration>**

  **- or -**

- **Via the Web Application: Refer to section 7.4.1.5 - Management <Firmware Update"> (Do not check the "save the configuration" option.)**

**Warning:**

**Once the H49 firmware installed, the H49 will be in default "SWITCH" mode with the default IP (192.168.254.254).**

#### 7.5.4.2.1 IMPORT AN H49 BACKUP CONFIGURATION ARCHIVE FROM A PC TO AN H49

Before importing an H49 configuration backup file, a user with **Engineer** role must be created to perform the import and restore actions.

To restore an H49 configuration backup archive file, it first must be imported in the H49 **/tmp** folder as a file named **h49_conf_backup.dat**. This operation can be performed through SCP.

***Note:***
*As example, from a Windows 10 PC, this can be done with the native SCP Windows command as explained below.*

Start "Windows Command prompt" and send the command:

```
scp -o "UserKnownHostsFile=/dev/null" -o "StrictHostKeyChecking=no" C:\02-Config
\H49\h49_conf_backup.dat user@192.168.254.254:/tmp
```

"PC source backup file" (here C:\02-Config\H49\h49_conf_backup.dat)

"H49 user account" (here user)

"H49 IP address" (here 192.168.254.254)

After this command execution, the password of "user" account from H49 will be required before the configuration backup archive file "**h49_conf_backup.dat**" is available in your H49 "**/tmp**" folder.

#### 7.5.4.2.2 RESTORE H49 BACKUP CONFIGURATION ARCHIVE

Start an ssh session with a user with **Engineer** role and enter the following CLI command:

```
firmware --restore
```

A reboot of the H49 is required to get all the restored settings applied. This can be done with the CLI command:

```
Reboot
```

Warning:
Before rebooting, put back the cables as they were on the replaced H49.

# 8 CYBERSECURITY

## 8.1 CHAPTER OVERVIEW

Cyber security has become an urgent matter in many industries where advanced automation and communications networks play a crucial role and where high reliability is of paramount importance.

Cyber security relies on processes and practices designed to protect networks, computers, programs and data from attack, damage, or unauthorized access.

Various standards and recommendations apply to substation cyber security and consist in maintaining the Availability, Integrity and Confidentiality of the substation data and automation processes. This chapter contains the following sections:

## 8.2 REASON H49 CYBER SECURITY IMPLEMENTATION

At the Reason H49 level, the following cyber security measures have been implemented:

- Encryption and Credential
- Secured File Transfer
- Authorization
- Authentication
- Password Management
- Security Log Management
- Other Security Measures

### 8.2.1 ENCRYPTION AND CREDENTIALS

Usernames and passwords are secured and are NERC compliant.

### 8.2.2 SECURED FILE TRANSFER

Files are exchanged through a secure file transfer protocol such as:

- **Secure Shell (SSH)**, provides confidentiality and integrity of data in client-server architectures by encrypting data
- **SSH File Transfer Protocol / Secure File Transfer Protocol (SFTP)**, provides secure file transfer capabilities. This is an extension of the Secure Shell protocol (SSH) protocol.
- **HyperText Transfer Protocol Secure (HTTPS)** for secure communication over a computer network widely used on the Internet. Connections are encrypted by Transport Layer Security (TLS) or Secure Sockets Layer (SSL)

Non-secured protocols are disabled.

### 8.2.3 AUTHORIZATION

Authorization is both the process of a security administrator granting rights to users and the process of checking user account permissions for access to devices.

The permissions define both the environment the user sees and the way he/she can interact with it.

When successfully authenticated, the user can only perform actions for which privileges have been explicitly granted to him/her. These permissions are set by a security administrator and stored locally or on the authentication server.

#### 8.2.3.1 ROLE-BASED ACCESS

Reason H49 uses the concept of Roles and Rights. This process consists in assigning local authorized users to one predefined roles and is known as Role-Based-Access Control (RBAC).

A role is a collection of privileges. Different roles and different access rights can be associated with a user. This action is done in the **Security > User Accounts** page of the web user interface:

The available roles are:

| Attribute | Description |
|---|---|
| **Viewer** | A "Viewer" can only display data or read information. A "Viewer" is not authorized to change other passwords, nor to visualize the security logs. |
| **Engineer** | An "Engineer" can only access data useful to run the system. He/she works in the substation and can act on a sub-system. He/she has observer rights plus specific rights to trigger commands.<br>The "Engineer" is not authorized to change other passwords, nor to visualize the security logs. |
| **Security Administrator** | The "Security Administrator" is responsible of the Security policy. He/she is ONLY allowed to reset passwords, define the security parameters, and visualize the security logs.<br>The "Security Administrator" is not allowed to display any data of DS Agile system, load a database nor change a sub-system operating mode. |
| **Security Auditor** | A "Security Auditor" can only display data or read information. A "Security Auditor" is authorized to visualize the security logs. |

***Note:***
*If the roles assigned to a user change, the user must logout and log back in to exercise his/her privileges.*

### 8.2.4 AUTHENTICATION

User authentication is a process that verifies the identity of a user who connects to a device.

Any user interaction with Reason H49 requires authentication through a login and password, whatever the interaction service (protocol) and regardless of the interaction type (read, write).

#### 8.2.4.1 CENTRAL AUTHENTICATION

Reason H49 operates with LDAP for central authentication.

Centralized username/password management reduces the maintenance, as all user credentials are stored in a server and not in each individual device.

To use centralized accounts, check the **LDAP Server Enabled** option in the **Security > Security Settings** page. When central authentication is used, then central authorization is applied. The central authorization service provides the list of user's roles.

The configuration of the LDAP server address, encryption mode, access account, etc. is done in the **Security > LDAP Server** page.

Redundant LDAP server can be configured to ensure system redundancy.

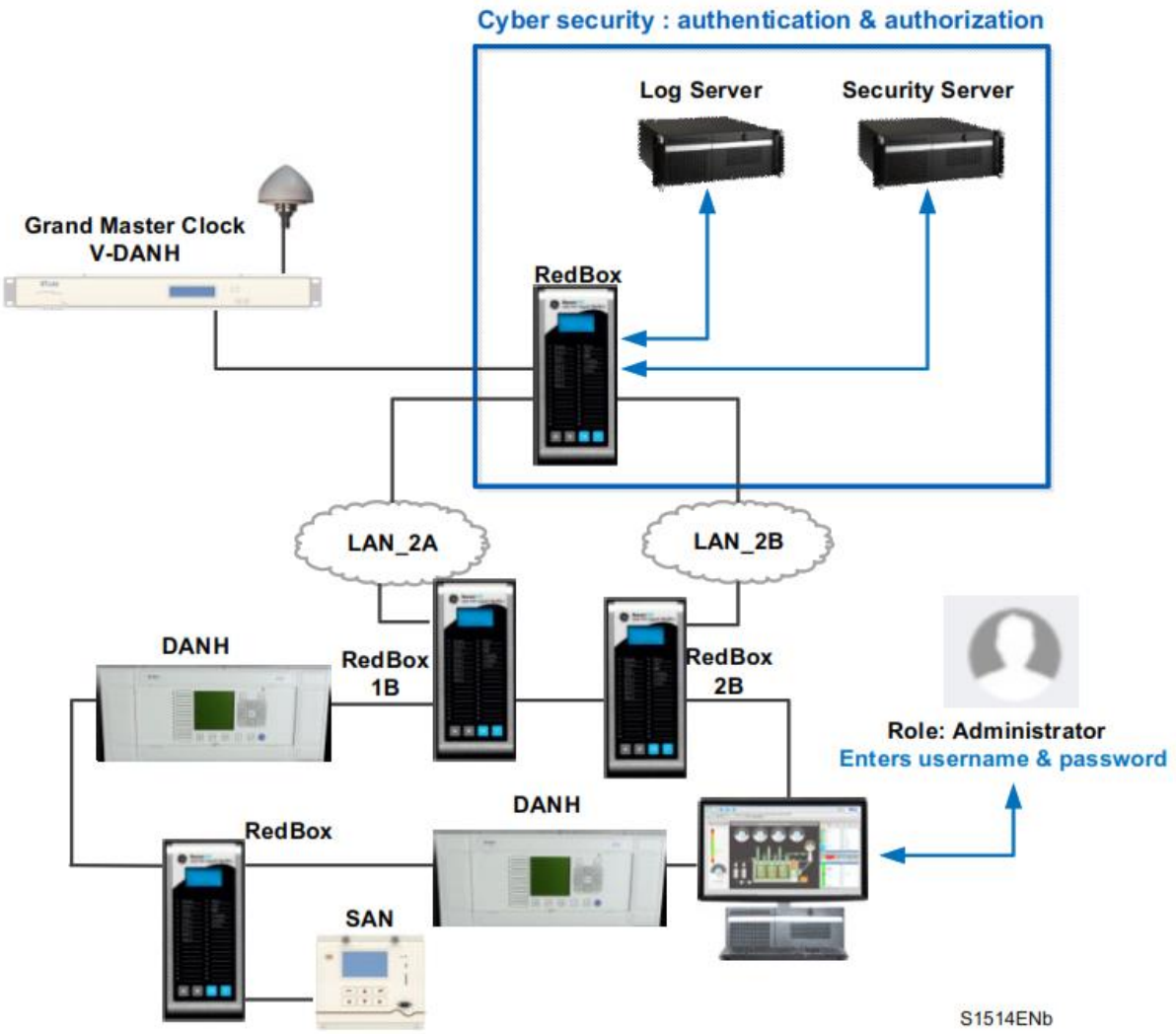



**Figure 97: Network Architecture with Centralized Authentication**

- The user authenticates on the device through the user interface.
- The device checks the credentials provided by the user against the centralized security server that stores user account database.
- The centralized security server answers the device and confirms whether the user has the right to access the device or not (this is the authorization step).
  - Upon successful authentication, the user is granted authorization for access.
  - If an error occurs during the authentication process, a message appears as shown on the following figure.
- Then, the device gives access to the user and loads the user profile according to his/her role.

#### 8.2.4.1.1 LDAP SERVER H49 USERS AND GROUPS CONFIGURATION

This section describes how LDAP server attributes and values for groups and users must be configured to work with H49.

##### 8.2.4.1.1.1 SECURITY GROUPS

LDAP server must define security groups matching with the H49 ones. Each LDAP security group must have its attribute gidnumber defined as below:

| LDAP security group | LDAP gidNumber attribute |
|---|---|
| VIEWER | 1000 |
| ENGINEER | 1001 |
| SECADM | 1002 |
| SECAUD | 1003 |
| ROOT | 0 |

##### 8.2.4.1.1.2 USERS

On LDAP server side, H49 users must be defined with the below LDAP attributes:

| LDAP Attribute | Description |
|---|---|
| **uid** | LDAP username |
| **msSFU30Name** | LDAP username |
| **msSFU30NisDomain** | DC |
| **uidNumber** | User Account identifier (value must be greater than 10000 and be unique for each user account) |
| **gidNumber** | Group identifier (one of the LDAP security group gidnumber attribute value, see above table) |
| **unixHomeDirectory** | Home directory |
| **loginShell** | Login Shell |

***Note:***
*For Central Authentication, a user belongs to only one group (role).*

Example of H49 LDAP user configuration:

| LDAP user account | LDAP user attribute uidNumber | LDAP user attribute |
|---|---|---|
| H49_VIEWER_USER | 10001 | 1000 |
| H49_ENGINEER_USER | 10002 | 1001 |
| H49_SECADM_USER | 10003 | 1002 |
| H49_SECAUD_USER | 10004 | 1003 |
| H49_ROOT_USER | 0 | 0 |

Example of configuration for a user (H49_ENGINEER_USER):

| LDAP attribute to be filled | Value |
|---|---|
| uid | H49_ENGINEER_USER |
| msSFU30Name | H49_ENGINEER_USER |
| msSFU30NisDomain | dsagile2019 |
| uidNumber | 10002 |
| gidNumber | 1001 |
| unixHomeDirectory | /home |
| loginShell | /bin/bash |

#### 8.2.4.1.2 LOCAL AUTHENTICATION

When the centralized authentication is not available or when the "LDAP Server Enabled" option is not selected in the **Security > Security settings** page, Reason H49 uses a local account service for local authentication.

It means that information about user(s) is stored on the system.

> ***Note:***
> *Local user accounts are applied only if no LDAP account management has been defined or if the LDAP server is not accessible. If local authentication is used, then its associated authorization will also be local.*

Local account management (creation, deletion, edition, etc.) is accessible from the **Security > User Accounts** page.

**Default User**

By default, Reason H49 is delivered with a default administrator account.

When connecting to Reason H49 for the very first time via the web server, the user shall use the following default authentication information:

- Login: **user**
- Password: **user**

Then, once connected to the Reason H49 switch, he/she will be invited to enter his/her password in order access the services provided by the device.

> ***Note:***
> *This default account is modifiable by the customer.*

### 8.2.4.2 PASSWORD MANAGEMENT

One of the fundamental principles of cyber security consists in combining a user ID with a password. For Reason H49, password policy is implemented in compliance with IEEE 1686 recommendations.

**Password Complexity**

The password policy is implemented for all local users. This action is done in the **Security > User Accounts** page. Here the security administrator can increment the user's account password complexity by defining restrictions according to the NERC CIP and IEEE 1686-2013 standards:

- Minimum number of characters:
  - Nine (9) with four character types: Uppercase, Lowercase, Numeric and special non-alphanumeric (such as @, !, #, {, etc.}

- Restriction based on weak password dictionary
- Restriction based on password history

> ***Note:***
> *Password complexity can be disabled to accommodate customers that do not require complex passwords.*

### Password Expiration Period
The security administrator can force users to change regularly their password. He/she can set the password lifetime after which it expires.

### Consecutive Login Attempts
The security administrator can set the number of consecutive login attempts before locking a user account and the locking period.

### Inactivity Period
The security administrator can set the inactivity period before disconnecting a user. This avoids leaving the device accidentally open to access by authorized persons. Thus, when the user does not perform an action within the pre-defined interval, he/she will automatically log off.

### Locking Period
After a fixed number of login attempts, the user account is locked out. The system tags it with the  icon.

The user will have to wait until the end of the security time (see **Locking period** in section Security Settings). However, the security administrator can manually unlock the account (see **Unlock** in section Security Settings).

### Change User Password
Users and system administrator can update their own account settings by clicking on the user icon, in the top-right corner of the web application:

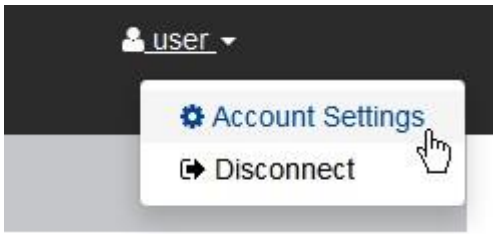



**Figure 98: Reason H49 Web User Interface – User Account Settings Icon**

The following attributes can be modified:

- Full name
- Current password
- New password
- Confirm password

> **Caution:**
> **As a system administrator, use this menu to edit or change your own password.**

**Reset a Password**

To reset a password, the old and new passwords are required.

Only a user with **Security Administrator** privileges can reset a user's password by clicking **Reset password**, in the user **Security > User Account > Account Setting** page.

In this case, the system will automatically generate a new password that can be changed by the user. The new password is then used to connect to the device web application.

> ***Note:***
> *When a user has lost a password, the password cannot be recovered due to the one-way password encryption algorithm.*

### 8.2.4.3 CERTIFICATE MANAGEMENT

Only the users with **Security Administrator** privileges can manage the certificates. Certificates are used in a network to secure communication. This is an electronic document that identifies an entity (machine, server or other) and associates that entity with a key.

#### 8.2.4.3.1 LDAP/SYSLOG

Reason H49 uses certificates to communicate securely with external servers such as the Syslog and LDAP servers. For LDAP and Syslog, certificates allow H49 to check the identity of the server and encrypt communication. A trusted CA (Certificate Authority) certificate is expected. The certificate must be a valid X.509 certificate in PEM format (with ".pem" extension).

PEM files are a text files containing one or more items in Base64 ASCII encoding, each with plain-text headers and footers (e.g., -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----).

#### 8.2.4.3.2 HTTPS

H49 uses also certificates to allow the H49 web application client to communicate securely with it (HTTPS).

For HTTPS, a PKCS#12 encoded file (file with a .pfx extension) is expected, this file must contain a private key and its associated certificates with or without a complete chain.

> ***Note:***
> *In the .pfx certificate, the SAN (Subject Alternative Name) must match the H49 IP address. If H49 IP address is changed, a new certificate must be generated.*

If the PKCS#12 is password protected, then the password will be asked at the certificate import time. On the browser side, authority public certificate must be trusted.

**Warning:**

**Certificate validity period dates must not be past 01/18/2038.**

**Warning:**

**Check that your H49 system date & time are correctly configured and match with your server certificate validity period.**

When the certificate is successfully uploaded, the user is logged off. The certificate will be taken into account right after the web service automatic restart.

#### 8.2.4.3.3 WEB APPLICATION CERTIFICATE IMPORT (LDAP/SYSLOG/HTTPS)

Certificates can be imported either by using the web application (as described below) or by using the CLI (Refer to section **12.1.4.4 Security Commands** for further information).

***Note:***
*It is possible to use the CLI command security -r to restore the default H49 HTTPS self-signed certificate (Refer to section **12.1.4.4 Security Commands**).*

To upload a certificate, in **Security settings** tab, click on **Upload Certificate**. Then select certificate as explained above (.pem for LDAP/syslog or .pfx for HTTPS).

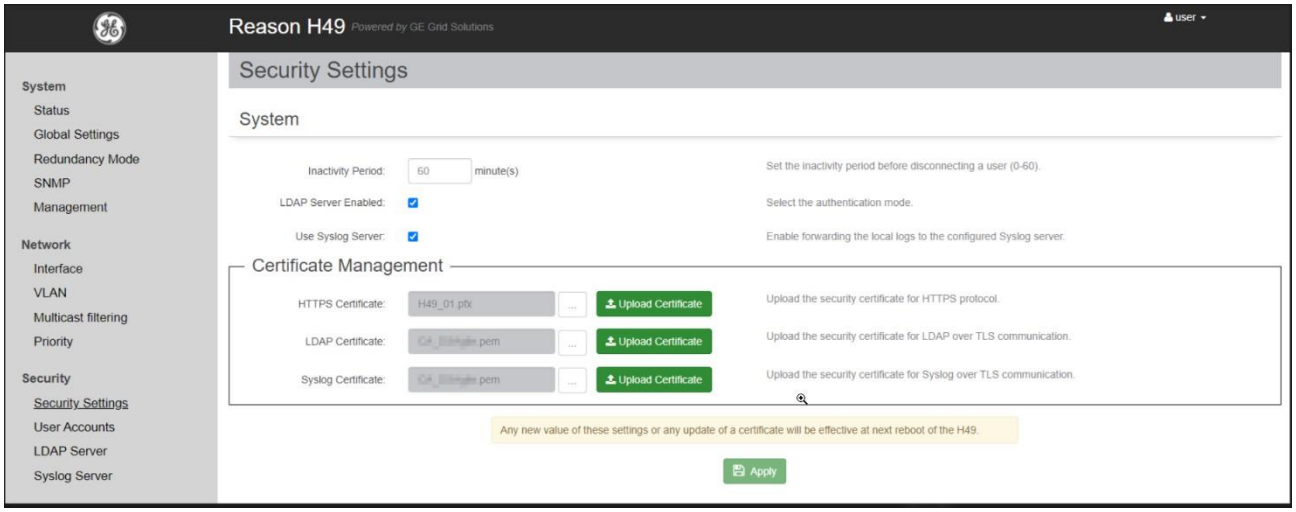



**Figure 99: Reason H49 Web User Interface – Certificate Management**

#### 8.2.4.4 SECURITY LOGS

Any user activity or login attempts whether successful or failed is logged:

- Startup log and Shutdown log
- Successful and failed login attempts
- User account (local) changes (password reset, change of role)
- Database switch
- Firmware / application update
- Manual logout
- Time out logout
- Alarm incident
- Time/date change
- Configuration change

#### 8.2.4.5 LOCAL LOGS

Reason H49 keeps a local log file.

Sensitive information such as passwords is not logged.

#### 8.2.4.6 REMOTE LOGS

Reason H49 supports logging to a remote Syslog server. Refer to the Security Settings section for more details.

At any time, the security administrator can enable/disable logging to a central syslog server. Syslog implementation supports UDP, TCP and TCP over TLS.

- If the log server is reachable, then the log messages are sent to the server "on-the-fly"; in other words, messages are not buffered and sent in batch to the server.
- If the log server is unavailable, the log messages are temporarily buffered and they are sent to the server upon service reestablishment.

Moreover, the bandwidth used for accessing the log server has been configured in order to avoid flooding the network.

#### 8.2.4.7 OTHER SECURITY MEASURES

**Hardening**

Hardening is the process of securing a system by reducing its surface of vulnerability.

This includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services.

By default, Reason H49 configuration is hardened according to CIS (Center for Internet Security) recommendations.

**Disabling Ports**

The availability of unused ports could provide a security risk.

An authorized user with Engineer role can disable unused physical ports. This action is done from the **Network > Interface** page. Every interface is represented by a row in the table.

***Note:***
*When the device is configured in QuadBox mode, ports 5 and 6 are deactivated, thus they are not displayed in the list.*

### Firmware Update

Reason H49 firmware is digitally signed.

When uploading and installing a new firmware version on the device, the package signature is verified before allowing the firmware to be installed.

Cyber security certificates and public and private keys used for the authentication process are stored in the local hardware.

The engineer user can update the device firmware as described in the Management section.

### Configuration Update

The engineer user can update the device by downloading a **Running** and a **Startup** configuration as described in the Management section.

# 9 MAINTENANCE

## 9.1 CHAPTER OVERVIEW

**Caution:**
**Before carrying out any work on this product you should study the contents of the safety and technical data of the GE Vernova Safety Guide SFTY/4L M/H11 (or later issue) and the ratings on the equipment rating label.**

**You should also read the Safety Information section of this document before carrying out work on this product.**

This chapter contains the following sections:

## 9.2 MAINTENANCE PERIOD

Deterioration may occur over time. Because of the electrical and heavy-interference environment, the device should be checked at regular intervals to confirm that it is operating correctly.

The device is self-supervising and so requires less maintenance than earlier devices. Most problems will result in a reboot. However, some periodic tests should be carried out to ensure that they are functioning correctly and that the external wiring is intact. It is the responsibility of the customer to define the interval between maintenance periods. If your organization has a Preventative 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

## 9.3 PRODUCT CHECKS

This section describes the checks to be performed during maintenance.

### 9.3.1 VISUAL CHECKS

These checks should be performed during maintenance operations:

- Check that no components look damaged.
- Check that the RJ45 and optical SFP modules are firmly held in place.

### 9.3.2 FUNCTIONAL CHECKS

Check that the LEDs in the front panel give correct indications (see the Hardware section).

- Check that the network connectors are correctly fitted.

## 9.4 FIRMWARE UPGRADE

Follow the procedure described in the Management section.

## 9.5 ERROR DETECTION

Most of the faults are indicated through the LEDs in the front panel. See the Hardware section for more details on LEDs indication.

Reason H49 supports monitoring access through SNMP. It is the responsibility of the maintenance procedure to regularly monitor the device in order to verify it healthy functioning.

## 9.6 TESTING THE LEDS

Reason H49 provides a mechanism allowing us to test the correct functioning of the LEDs present in the front panel.

- Press "OK" + "C" buttons: all LEDs turn RED,
- Message "LED test / press OK" is displayed on the LCD
- Press "UP" button: all LEDs turn AMBER
- Press "DOWN" button: all LEDs turn GREEN
- Press "OK" button in order to set the device to its normal (LED + LCD)

## 9.7 METHOD OF REPAIR

This product cannot be repaired on-site. Should the product fail, it will need to be replaced with an equivalent device.

### 9.7.1 REPLACING REASON H49

The case and connectors have been designed for ease of use, so removing Reason H49 is very simple.

#### 9.7.1.1 REMOVING REASON H49

Before disconnecting, check that labels correctly identify the connections, and match the descriptions. Note the IP Address, Subnet settings, etc., to configure the replacement.

Proceed by:

1. Disconnecting all the power supply connectors.
2. Disconnecting the alarm contacts connectors.
3. Disconnecting the Ethernet RJ45 connectors.
4. Disconnecting the Ethernet optical connectors.
5. Disconnecting the protective earth connection.
6. Removing the H49 from the DIN rail carefully, paying attention to its weight.

#### 9.7.1.2 INSTALLING A REPLACEMENT PRODUCT

To reinstall a replacement product:

1. Attach the product to the DIN rail.
2. Connect the protective earth connection.
3. Connect the power supply connection(s).
4. Establish an HTTPS connection and set the IP Address, etc.
5. Restore the other connections.

### 9.7.2 REPAIR AND MODIFICATION PROCEDURE

In case of equipment malfunction, the customer shall get in contact with GE Vernova Contact Centre and never attempt to repair the device by own.

Please follow these steps to return the product to us:

1. Get the Repair and Modification Return Authorization (RMA) form.
   An electronic version of the RMA form is available upon request from the GE Vernova contact Center web page: https://www.gevernova.com/grid-solutions/contact.htm
2. Fill in the RMA form.
   a. Fill in only the white part of the form.
   b. Please ensure that all fields marked **(M)** are completed such as:
      - Equipment model
      - Model No. and Serial No.
      - Description of failure or modification required (please be specific)

- Value for customs (in case the product requires export)
- Delivery and invoice addresses
- Contact details

3. Send the RMA form to your local contact.
   For a list of local service contacts worldwide, visit the following web page:
   https://www.gevernova.com/grid- solutions/contact.htm
4. The local service contact provides the shipping information.
   Your local service contact provides you with all the information needed to ship the product:
   - Pricing details
   - RMA number
   - Repair center address
   - If required, an acceptance of the quote must be delivered before going to the next stage.
5. Send the product to the repair center:
   - Address the shipment to the repair center specified by your local contact
   - Make sure all items are packaged in an anti-static bag and foam protection
   - Make sure a copy of the import invoice is attached with the returned unit
   - Make sure a copy of the RMA form is attached with the returned unit
   - E-mail or fax a copy of the import invoice and airway bill document to your local contact.

# 10 TECHNICAL DATA

## 10.1 CHAPTER OVERVIEW

This chapter provides information about Reason H49 general characteristics and certifications.

This chapter contains the following sections:

## 10.2 CONFORMITY

Reason H49 has been designed, manufactured, and certified fully compliant with the generally applicable environmental standards such as:

- IEC 60255-27:2013
- IEEE 1613: 2009, IEEE 1613a:2011, IEEE 1613-1:2013
- IEC 61850-3 ed2.0:2013

## 10.3 ENVIRONMENTAL CONDITIONS

In power plant and substation environments, Reason H49 is intended to be used in the normal service conditions listed below:

| Item | Operating conditions | Storage conditions |
|---|---|---|
| Ambient Air Temperature[5] | -25°C/+55°C | -40°C/+70°C[1] |
| Solar radiation | Negligible | |
| Altitude | ≤ 2 000 m | |
| Relative humidity (24 h average) | From 5 % to 95 % RH[2] | |
| Atmospheric pressure | 86kPa to 106kPa | |
| Air pollution by dust, salt, smoke, corrosive/flammable gas, vapours | No significant air pollution[4] | |
| Vibration, earth tremors | Class 1[3] | |

***Footnotes:***

1 *The GE Vernova Reason H49 should be stored in its supplied packaging.*

2 *No condensation or ice is considered.*

3 *According to IEC 60255-21 series*

4 *These conditions correspond to maximum values given for classes 3C1 and 3S1 in IEC 60721-3-3.*

5 *The ambient air temperature is the maximum or minimum temperature around the enclosure of Reason H49.*

## 10.4 IEC61850-3 CERTIFICATION

This Section describes the points on which the H49 has been certified for IEC 61850-3.

### 10.4.1 DIELECTRIC

| Description | Test Standard | Mode | Group | Test Level |
|---|---|---|---|---|
| **Impulse voltage** | IEC 60255-27:2013<br>IEC 61180-1:1992 | | DC and AC Power ports Binary input/output Alarm output | 5kV+0%,-10% - 1.2/50µs impulse |
| | | | Signal ports (RJ45 + serial com) | 1kV 1.2/50µs impulse |
| **Dielectric voltage** | IEC 60255-27:2013 | | DC and AC Power ports Binary input/output Alarm output | 2kV rms. 50Hz for 1 minute |
| | | | Signal ports (RJ45 + serial com) | 0,5kV rms. 50Hz for 1 minute |
| **Insulation Resistance** | IEC 60255-27:2013 | Earth and all others | Power, input/output, Alarm and serial ports | Test voltage 500Vdc |
| **Protective bonding** | IEC 60255-27:2013 | | Mechanical ports | 60s, Test voltage < 12Vdc or 12 Vrms ac |

### 10.4.2 ELECTROMAGNETIC COMPATIBILITY

#### 10.4.2.1 STANDARD COMPLIANCE

Reason H49 is compliant with European Commission Directive on EMC (IEC 61000-5 standard).

#### 10.4.2.2 DC AUXILIARY SUPPLY

| Description | Test Standard | Group | Test Level |
|---|---|---|---|
| **DC voltage interruptions** | IEC 61000-4-29:2000<br>IEC 60255-26:2013 | DC Power port | Supply Interruptions<br>ΔU 100% for 50ms |
| **DC voltage dips** | IEC 61000-4-29:2000<br>IEC 60255-26:2013 | DC Power port | ΔU 30% for 100ms,<br>ΔU 60% @ 100ms |
| **Voltage ripple on DC Power Supply voltage** | IEC 61000-4-17:2009<br>IEC 60255-26:2013 | DC Power port | AC 100Hz ripple superimposed on DC max. and min. auxiliary supply at 10% of rated DC value. |
| **Burden for DC Power supply** | | DC Power port | PSU 110Vdc/load = Max 16,79VA<br>PSU 220Vdc/load = Max 16,79VA |
| **Inrush current and power-up duration** | | DC Power port | PSU 50Vdc = 9.7 A (100 – 150 ms)<br>PSU 110Vdc = 19.4A (110 ms)<br>PSU 220Vdc = 43.8A (92 ms) |

### 10.4.2.3 AC AUXILIARY SUPPLY

| Description | Test Standard | Group | Test Level |
|---|---|---|---|
| **AC voltage interruptions** | IEC 61000-4-11:2004<br>IEC 60255-26:2013 | AC Power ports | Supply Interruptions<br>ΔU 100% for 5 periods, 50 periods |
| **AC voltage dip** | IEC 61000-4-11:2004<br>IEC 60255-26:2013 | AC Power ports | ΔU 30% for 1 period<br>ΔU 60% for 50 periods |
| **Burden for AC Power supply** | | AC Power ports | PSU 110Vac/load = Max 33,42VA<br>PSU 230Vac/Load = Max 33,42VA |
| **Inrush current and power-up duration** | | AC Power ports | PSU 110Vac = 12,84A (126ms)<br>PSU 220Vac = 14,8A (109ms) |

### 10.4.2.4 AUXILIARY SUPPLY

| Description | Test Standard | Group | Test Level |
|---|---|---|---|
| **Gradual shut down/start-up** | IEC 60255-26:2013 | AC/DC Power port | Shut-down ramp 60s<br>Power off 5 min<br>Start-up ramp 60s |
| **Reversal of DC Power Supply** | IEC 60255-27:2013-10.6.6 | AC/DC Power port | Duration = 60s |
| **Burden for binary input** | | Binary inputs | PSU 110Vdc/load = Max 1VA<br>PSU 220Vdc/load = Max 1VA |

### 10.4.2.5 FAST TRANSIENT

| Description | Test Standard | Mode | Group | Test Level |
|---|---|---|---|---|
| **Fast Transient** | IEC 61000-4-4:2012<br>IEC 60255-26:2013 | CDN | DC and AC Power and Earth ports | Level 4:<br>4kV peak voltage at 5-kHz and 100-kHz repetition freq. |
| | IEC 61000-4-4:2012<br>IEC 60255-26:2013 | Clamp | Signal ports | Level 4:<br>2kV peak voltage at 5-kHz and 100-kHz repetition freq. |

### 10.4.2.6 EMISSIONS

| Description | Test Standard | Group | Test Level |
|---|---|---|---|
| **Conducted Emissions** | IEC 61000-6-4:2011<br>IEC 60255-26:2013 | AC and DC Power Supply | 0,15 MHz to 0,50 MHz: 79 dB(µV) quasi peak & 66 dB(µV) average<br>0,5 MHz to 30 MHz: 73 dB(µV) quasi peak & 60 dB(µV) average |
| | IEC 61000-6-4:2011<br>IEC 60255-26:2013 | Com, RJ45 ports | 0,15 MHz to 0,5 MHz:<br>97 dB(µV) to 87 dB(µV) quasi-peak<br>84 dB(µV) to 74 dB(µV) average<br>53 dB(µA) to 43 dB(µA) quasi-peak<br>40 dB(µA) to 30 dB(µA) average<br>0,5 MHz to 30 MHz:<br>87 dB(µV) quasi-peak<br>74 dB(µV) average<br>43 dB(µA) quasi-peak<br>30 dB(µA) average |
| **Radiated Emissions** | IEC 61000-6-4:2011<br>IEC 60255-26:2013 | Enclosure port | 30 - 230MHz:<br>40dB(µV/m) quasi-peak at 10m and 3m measuring distances.<br>230 - 1000MHz:<br>47dB(µV/m) quasi-peak at 10m and 3m measuring distances.<br>1 GHz to 3 GHz:<br>56dB(µV/m) average at 3m measuring distance.<br>76dB(µV/m) peak at 3m measuring distance.<br>3 GHz to 6 GHz:<br>60dB(µV/m) average at 3m measuring distance.<br>80dB(µV/m) peak at 3m measuring distance. |

### 10.4.2.7 IMMUNITY

| Description | Test Standard | Mode | Group | Test Level |
|---|---|---|---|---|
| **Conduced disturbances, induced by radiofrequency fields** | IEC 61000-4-6:2013<br>IEC 60255-26:2013 | | DC and AC Power ports, earth port, signal ports | Level 3 : 10V (rms)<br>Disturbance signal 80% AM with a 1KHz sine wave, 150Ω<br>Frequency sweep from 150kHz to 80MHz<br>Spot frequencies: 27 MHz ±0,5% & 68 MHz ±0,5% |
| **Radiated, radio-frequency electromagnetic field** | IEC 61000-4-3:2010<br>IEC 60255-26:2013 | 6 Faces | Enclosure ports | Level 3 : 10V/m (rms)<br>Frequency sweep:<br>from 80MHz to 3000MHz<br>Spot frequencies:<br>80 MHz ± 0,5 %<br>160 MHz ± 0,5 %<br>380 MHz± 0,5 %<br>450 MHz ± 0,5 %<br>900 ± 5 MHz<br>1 850 ± 5 MHz<br>2 150 ± 5 MHz |
| | IEC 61000-4-3:2010 | 6 Faces | Enclosure ports | Level 4 : 30V/m (rms)<br>Frequency sweep:<br>from 800MHz to 960MHz<br>from 1400MHz to 2000MHz |
| **Electrostatic Discharge** | IEC 61000-4-2:2008<br>IEC 60255-26:2013 | | Enclosure ports | Level 4:<br>15kV air discharge.<br>8kV contact discharge. |
| **Surge Immunity** | IEC 61000-4-5:2014<br>IEC 60255-26:2013 | DM | AC/DC Power,<br>Alarm, binary Input/<br>Output Ports | Level 3:<br>Source impedance 2Ω, Line-to-<br>line 2kV,<br>coupling resistor 0Ω, coupling capacitance 18 µF |
| | | CM | | Level 4:<br>Source impedance 2Ω, Line-to- earth 4kV,coupling resistor 10Ω, coupling capacitance 9 µF |

| Description | Test Standard | Mode | Group | Test Level |
|---|---|---|---|---|
| | | DM | Signal ports | Level 4:<br>Source impedance 2Ω, Line-to- ground 4kV,<br>coupling resistor 40Ω,<br>coupling capacitance 0,5 µF |
| **Power frequency magnetic field** | IEC 61000-4-8:2009<br>IEC 60255-26:2013 | | Enclosure port | Level 5:<br>100A/m continuous (≥60s)<br>1000A/m for 1s |
| **Pulsed magnetic field immunity** | IEC 61000-4-9:2001 | | Enclosure port | Level 5:<br>1000A/m peak<br>Applied 6.4/16µs magnetic field pulses in all planes for the EUT in a quiescent state. |
| **Damped oscillatory magnetic field immunity** | IEC 61000-4-10:2001 - 11 | | Enclosure port | Level 5:<br>100A/m peak<br>Applied in all planes at:<br>100kHz, repetition rate ≥ 40Hz, during 60s<br>1MHz, repetition rate ≥ 400Hz, during 60s |
| **Slow damped oscillatory wave** | IEC 61000-4-18: 2011<br>IEC 60255-26:2013 | CM | DC and AC Power | Level 3:<br>2.5kV @100kHz and 1MHz |
| | | DM | DC and AC Power | Level 3:<br>1kV peak voltage @100kHz and 1MHz |
| | | CM | Ethernet ports | Level 3:<br>2.5kV @100kHz and 1MHz |
| **Main frequency voltage** | IEC 61000-4-16-compil: 2011<br>IEC 60255-26:2013 | | DC Power port, Signal ports | Level 4:<br>30 Vrms cont.<br>300 Vrms for 1 s<br>Coupling resistor 200Ω and coupling capacitor 1uF - DC and inputs<br>Coupling resistor 50Ω - Ethernet ports |

### 10.4.3 SAFETY TESTS

| Description | Test Standard | Test Level |
|---|---|---|
| **Functional performance requirements** | IEC 62439-1:2010<br>IEC 62439-3:2016<br>IEC 61850-8-1:2011<br>IEC 61850-90-4:2013<br>IEC 61850-9-3:2016<br>IEC 61588:2009 | PRP, HSR and PTP functional features |
| **Clearance and creepage distances** | | Pollution degree = 2<br>Overvoltage category = III |
| **IP Rating** | IEC 60529: 2013 | IP2x for each face |
| **Flammability of insulation materials, components and fire enclosure** | IEC 60695-11-10 | UL94V-0 |

### 10.4.4 ENVIRONMENTAL TESTS

This section describes the environmental tests.

#### 10.4.4.1 DIELECTRIC

| Description | Mode | Group | Test Level |
|---|---|---|---|
| **Insulation resistance** | Earth and all others | Power, Input / output, Alarm and serial ports | Test voltage 500Vdc |
| **Dielectric type test** | Earth and all others | AC/DC Power, binary input/output, alarm ports | 2kV - before and after environmental tests |
| | Earth and all others | Serial and internet ports | 0,5kV - before and after environmental tests |
| **Protective bonding resistance** | | Mechanical ports | 60s, Test voltage < 12Vdc or 12 Vrms ac before and after environmental |

#### 10.4.4.2 CLIMATIC

| Description | Test Standard | Test Level |
|---|---|---|
| **Dry heat - Max operating temp** | IEC 60068-2-2:2007 | Test Bd: 55°C - 96 hours |
| **Cold - Min operating temp** | IEC 60068-2-1:2007 | Test Ad: -25°C - 96 hours |
| **Dry heat – Max storage temperature** | IEC 60068-2-2:2007 | Test Bd: 70°C - 96 hours<br>Power on @55°C |
| **Cold - Min storage temperature** | IEC 60068-2-1:2007 | Test Ab: -40°C - 96 hours<br>Power on @-25°C |
| **Change of temperature** | IEC 60068-2-14:2009 | Test Nb:<br>Start = 20°C for 1h<br>Lower temperature = –25°C<br>Higher temperature = 55°C |
| **Damp heat - steady state** | IEC 60068-2-78:2012 | Test Cab:<br>40°C ±2 °C - RH 93% ± 3% - 10 days |

| Description | Test Standard | Test Level |
|---|---|---|
| **Damp heat cyclic (12 h+12 h)** | IEC 60068-2-30:2005 | Test Db:<br>+25 °C ± 3 °C - 97 % –2 %+3 % RH<br>+55 °C ± 2 °C - 93 % ± 3 % RH<br>6 of 24 hours (12 h + 12 h) cycles |

### 10.4.4.3 MECHANICAL

| Description | Test Standard | Test Level |
|---|---|---|
| **Vibration response** | IEC 60255-21-1:1988 | Class 2 |
| **Vibration endurance (sinusoidal)** | IEC 60255-21-1:1988 | Class 1 |
| **Shock response** | IEC 60255-21-2:1988 | Class 2 |
| **Shock withstand and bump** | IEC 60255-21-2:1988 | Class 1 |
| **Seismic** | IEC 60255-21-3:1993 | Class 2 |
| **Enclosure protection** | IEC 60529:2013 | IP2x |

## 10.5 IEE1613 CERTIFICATION

| Description | Test Standard | Mode | Group | Test Level |
|---|---|---|---|---|
| **Service conditions** | IEEE C37.90:2007 - B8 | | Device | Installation Zone A |
| **Operational temperature range** | IEEE C37.90:2007 - B8 | | Device | Operating temperature: -25°C to 55°C<br>Storage temperature: -40°C to 70°C |
| **Relative humidity** | | | Device | 55% (for op and no-op temperature) with excursions up to 95% without internal condensation for a maximum of 96 h |
| **Allowable ac component in dc control voltage supply** | | | DC Power port | Alternating component (ripple) of 5% peak or less in the dc control voltage supply, provided the minimum instantaneous voltage is not less than 80% of rated voltage |
| **DC rated control power inputs** | | | DC Power port | Operating successfully over a minimum range of 85% to 110% of rated voltage at rated frequency |
| **AC rated control power inputs** | | | AC Power port | Operating successfully over a minimum range of 85% to 110% of rated voltage at rated frequency |
| **Dielectric power frequency** | | | DC and AC Power ports<br>Binary input/output<br>Alarm output | 2kV, AC between 45Hz and 65Hz, 1min |
| | | | Signal ports (RJ45 + serial com) | 500V, AC between 45Hz and 65Hz, 1min |
| **Impulse voltage** | | | DC and AC Power ports<br>Binary input/output<br>Alarm output | a) Waveform polarity: Positive and negative<br>b) Rise Time: 1.2 µs ± 30% c) Magnitude: 5 kV +0/–10% (circuit rated upper 50V)<br>d) Time to half value: 50 µs ± 20%<br>e) Source impedance: 500 Ω ± 10%<br>f) Output energy: 0.5 joules ± 10% |
| **Fast transient waveform** | IEEE C37.90:2007 - B8 | CM | Power, Input / output, Data com and signal ports | 4kV crest value (tolerance ± 10%) |
| | IEEE C37.90:2007 - B8 | TM | Power and output ports | 4kV crest value (tolerance ± 10%) |

| Description | Test Standard | Mode | Group | Test Level |
|---|---|---|---|---|
| | IEEE C37.90:2007 - B8 | TM | Watchdog | 4kV crest value (tolerance ± 10%) |
| **Surge withstand capability (SWC)** | IEEE C37.90:2007 - B8 | CM | Power, Input/output, Data com and signal ports | 2,5kV crest value (tolerance +0/–10%.) |
| | IEEE C37.90:2007 - B8 | TM | Power and output ports | 2,5kV crest value (tolerance +0/–10%.) |
| **Surge Immunity** | IEC 61000-4-5:2005 | DM | AC/DC Power, Alarm, binary Input/Output Ports | Level 4:<br>Source impedance 2Ω, Line-to-line 2kV,<br>coupling resistor 0Ω, coupling capacitance 18 µF |
| | | CM | | Level 4:<br>Source impedance 2Ω, Line-to earth 4kV,<br>coupling resistor 10Ω,<br>coupling capacitance 9 µF |
| | | CM | Signal Ports | Level 4:<br>Source impedance 2Ω, Line-to-ground 4kV,<br>coupling resistor 40Ω, coupling capacitance 0,5 µF |
| **RF susceptibility tests** | IEEE C37.90.2:2004 B10 | 6 faces | Enclosure ports | a) Field strength = 20 V/m (–0 to +6 dB) un-modulated<br>b) Sine wave amplitude modulation, 80 % AM at 1 kHz rate<br>c) Range of 80 MHz to 1000 MHz.<br>d) Spot frequency tests:<br>- 80, 160 and 450MHz ±0.5%<br>- 900MHz ±5 MHz<br>e) Dwell time >0,5s |

| Description | Test Standard | Mode | Group | Test Level |
|---|---|---|---|---|
| | | 6 faces | Enclosure ports | a) Field strength = 10 V/m (–0 to +6 dB) un-modulated<br>b) Sine wave amplitude modulation, 80 % AM at 1 kHz rate;<br>c) Range of 1000 MHz to 3800 MHz with dwell time >0,5s and frequency sweep test: 1%<br>d) Spot frequency tests:<br>- 1,6GHz and 3,8GHz with dwell time >1s |
| | | 6 faces | Enclosure ports | a) Pulse modulated (50% duty cycle) 8,5 V/m (–0 to +6 dB)<br>b) Range of 1000 MHz to 6000 MHz<br>d) Spot frequency tests:<br>- 1,732GHz<br>- 1,8GHz<br>- 2,31GHz<br>- 2,45GHz and 5,8GHz<br>e) Dwell time >1s |
| **Electrostatic discharge tests** | IEEE Std C37.90.3:2012 - B4 | | Enclosure port | a) Contact discharge (direct/ indirect) = 8 kV<br>b) Air discharge (direct) = 15 kV |
| **Immunity to conducted disturbances induced by RF fields** | IEC 61000-4-6:2003 - 5 | | DC and AC Power ports, earth port, signal ports | Level 3: 10Vemf |
| **Power frequency magnetic field immunity tests** | IEC 61000-4-8:1993 | | Enclosure port | Zone A:<br>100A/m continuous (≥60s)<br>1000A/m - 3s |
| **Damped oscillatory magnetic field tests** | IEC 61000-4-10:2001 | | Enclosure port | Level 5:<br>100A/m peak<br>Applied in all planes at:<br>100kHz, repetition rate ≥ 40Hz, during 60s<br>1MHz, repetition rate ≥ 400Hz, during 60s |

| Description | Test Standard | Mode | Group | Test Level |
|---|---|---|---|---|
| **Immunity to common-mode disturbances** | IEC 61000-4-16:2002 | | DC/AC Power port,<br>Signal ports | Level 4:<br>30 Vrms cont.<br>300 Vrms for 1 s<br>Frequency range = 0Hz to 150kHz<br>Coupling resistor 200Ω and coupling capacitor 1uF - DC and inputs<br>Coupling resistor 50Ω - Ethernet ports<br>AC main frequencies - 50 Hz and 60 Hz. |
| **Vibration** | | | Enclosure port | Class: V.S.2<br>Velocity: <10mm/s<br>Freq range 1Hz to 150Hz |
| **Shock** | | | Enclosure port | Height of fall : 100mm |
| **Device cooling** | | | | Device shall be convection cooled and shall not include internal fans or any other means of forced air circulation. |

## 10.6 GENERAL CHARACTERISTICS

| Item | Description |
|---|---|
| **Rated Insulation Voltage** | 300V |
| **Pollution degree** | 2 |
| **Overvoltage category** | III |

### 10.6.1 MECHANICAL

| Item | Description |
|---|---|
| **Dimensions** | W x H x D = 165 mm x 176 mm x 75 mm |
| **Weight** | 1.3 kg |
| **Mounting** | DIN Rail EN50022 |

### 10.6.2 PRIMARY POWER SUPPLY

| Item | Description |
|---|---|
| **Supply voltage range** | 85 Vac – 230 Vac<br>85 Vdc – 250 Vdc |
| **Power consumption** | 42 VA max (220 Vac) / 18 W max (125 Vdc) |
| **Input Frequency voltage** | The nominal frequency (fn) for the AC auxiliary voltage is dual rated at 50/60 Hz; the operating range is 44 Hz to 66 Hz. |

### AUXILIARY POWER SUPPLY

| Item | Description |
|---|---|
| **Supply voltage range** | 85 Vdc – 250 Vdc |
| **Power consumption** | 18 W max (125 Vdc) |

### 10.6.3 AUXILIARY FAULT RELAYS (OPTICAL PORT ALARM)

| Item | Description |
|---|---|
| **Connector** | NC contact potential free |
| **Max. switching voltage** | 33 Vac; 30 Vdc |
| **Max. switching current** | 5 A |
| **Max. switching power** | 165 VA; 150 W |

### 10.6.4 BIU261D

This section describes the BIU261D certification.

#### 10.6.4.1 POWER SUPPLY INPUT VOLTAGE OPERATIVE RANGE

| Nominal ranges | Operative DC range | Operative AC range |
|---|---|---|
| **85 Vdc – 250 Vdc** | 76.5 Vdc (85-10%) – 275 Vdc (250+10%) | |
| **85 Vac – 230 Vac** | | 76.5 (85-10%) – 253 Vac (230+10%) |

#### 10.6.4.2 MAXIMUM MEASURED BURDEN IN VOLT-AMPERE (VA)

| Item | Power supply voltage | VA |
|---|---|---|
| Maximum burden AC powered on main power supply | 110 Vac | 23.19 |
| Maximum burden DC powered on main power supply | 110 Vdc | 16,16 |
| Maximum burden DC powered on secondary power supply | 110 Vdc | 16,13 |
| Maximum burden for binary input | 110,4 Vdc<br>220,76 Vdc | 0,16<br>0,69 |

##### MAXIMUM MEASURED INRUSH CURRENT (VDC)

| Power input voltage (Vdc) | Measured peak current (A) | Power-up duration (ms) |
|---|---|---|
| 110 | 19.4 | 110 |
| 220 | 43.8 | 92 |
| 50 | 9.7 | 100-150 |

#### 10.6.4.3 MAXIMUM MEASURED INRUSH CURRENT (VAC)

| Power input voltage (Vac) | Measured peak current (A) | Power-up duration (ms) |
|---|---|---|
| 110 | 12,84 | 126 |
| 230 | 14,8 | 109 |

### 10.6.5 ETHERNET MANAGEMENT

| Item | Description |
|---|---|
| **Standards** | IEEE802.3, 802.3u, 802.3x |
| **Forwarding mode** | Store and forward |
| **Memory bandwidth** | 800 Mbps |
| **MAC Address** | 512 |
| **Address learning** | Automatic |
| **Illegal frame** | Dropped per 802.3 |

| Item | Description |
|---|---|
| **Late collision** | Dropped after 512 bit times |
| **Latency** | 20 µs measured at 75 % load with frames length of 64 bytes between the device ports and the redundant ports.<br>250 µs measured at 75 % load with frames length of 1518 bytes between the device ports and the redundant ports. |

### 10.6.6 MANUFACTURER

**GE Vernova**
Worldwide Contact Centre
St Leonards Building
Red Hill Business Park
Stafford ST16 1WT, United Kingdom, UK
Tel: +44 (0) 1785 25 00 70
Fax: +44 (0) 1785 27 09 40
https://www.gevernova.com/grid-solutions/contact.htm

# 11 APPENDICES

## 11.1 CHAPTER OVERVIEW

This section describes use of command lines for configuring and using H49.

This chapter contains the following sections:

## 11.2 APPENDIX 1

The Command Line Interface enables users to configure and manage the features of the Reason H49 switch. The user (or client) issues commands to the program in the form of successive lines of text (command lines) through a Secure Shell (SSH) console.

### 11.2.1 PREREQUISITES

To be able to access the H49 functions from an SSH console, make sure that the PC host and the switch are connected to the same LAN on the same logical subnet. By default, the H49's IP address is **192.168.254.254** and the H49's subnet mask is **255.255.0.0**. To do so:

1. Open the **Control Panel** on your computer.
2. Go to **Network Connections.**
3. Right-click **Local Area Connection** and select **Properties.**
4. Select **Internet Protocol Version 4 (TCP/IP)** and click **Properties.**
5. Select **Use the following IP address** and type a compatible IP address and a sub mask of 255.255.0.0.
6. Click **OK** to save the change. Reboot your PC if prompted.
7. Connect an Ethernet cable between your PC and any port on the Reason H49 switch.

> ***Note:***
> *The device connects to the network through a Small Form-factor Pluggable module (SFP). Refer to the Ethernet Connections section to see the references of the supported RJ45-type SFP module.*

### 11.2.2 ACCESSING THE SSH CONFIGURATION INTERFACE

You may use any SSH tool to access the H49's configuration console.

In our example, one way of accessing the H49 through a Secure Shell (SSH) console is by using the **PuTTY** program, which can be downloaded free of charge from http://www.putty.org/.

- Start the **PuTTY** console.
- Click the **Session** menu from the tree-view on the left-side of the window.
- In the **Host Name (or IP address)** entry field, type the IP address of the switch **192.168.254.254.**
- Set the port to **22.**
- Check the **SSH** connection type and click **Open** to establish the connection.

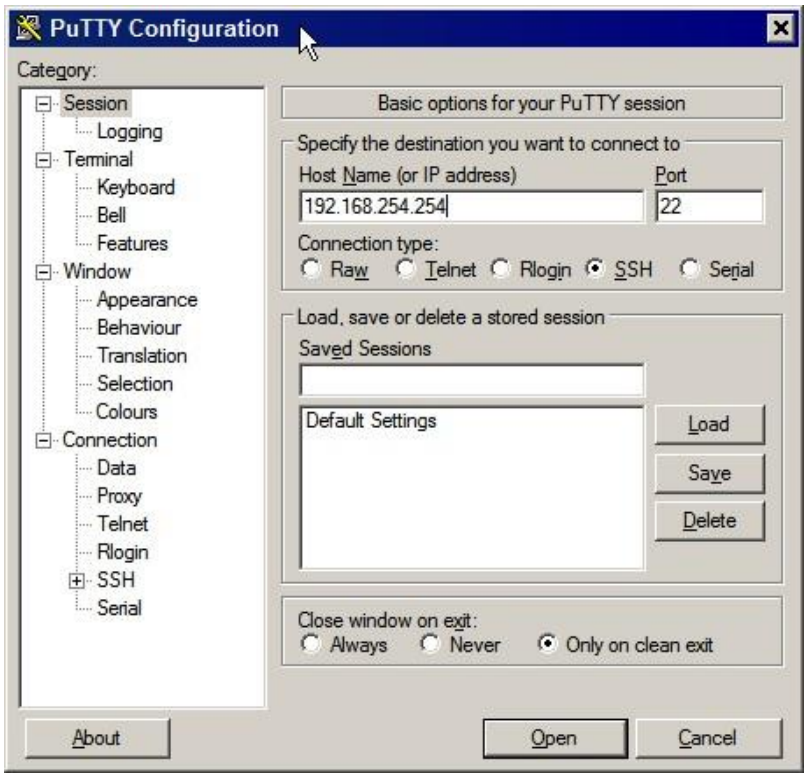



**Figure 100: SSH Console – Establish the connection with the H49**

When starting the SSH console for the first time, a security popup window appears on screen.

- Click **Yes** to accept the SSH key and carry on connecting:


**Figure 101: SSH Console – Add the SSH Key**

### 11.2.3 LOGGING TO THE H49

The console login screen appears. It prompts you for a login name and password.

Use the following default values:

- Login as: type **user** and press **Enter**
- Password: type **user** and press **Enter**

> ***Note:***
> *Login and password are case-sensitive. You can change the user name and the password later in the Command Line Interface.*

If an error occurs during the authentication process, an information message appears on screen, as shown in the following figure.


**Figure 102: SSH Console – Error during the Login Process**

When connecting to Reason H49 for the first time, the system prompts the user to change the default password.

- Enter a new password and confirm:

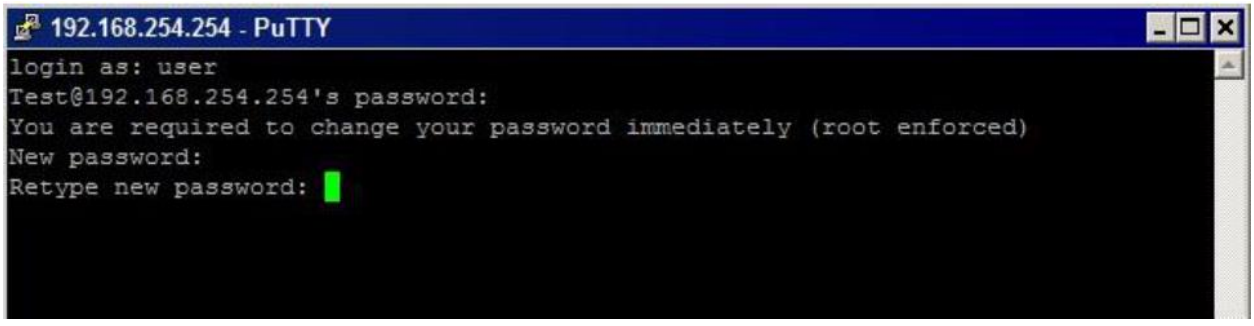



**Figure 103: SSH Console – Enforced Password Policy**

Upon successful authentication, you are granted authorization for access. Read the License agreement and type **Y (**for yes) to agree to the terms:


**Figure 104: SSH Console – Agreement Conditions**

The Reason H49's start screen appears:


**Figure 105: SSH Console – H49 Main Menu**

***Note:***
*To modify the appearance of the SSH console, select **Appearance** under the **Window** menu and change the desired formatting options, or go to **Colours** to change the use of Foreground and Background colours.*

### 11.2.4 CLI COMMANDS

This section gathers the list of command lines that can be used to configure the Reason H49 switch.

A command line is a combination of a command name, a parameter name and a parameter value:

The general format is:

- **command –parameter value**

Example: to set the H49 sub mask, you can type: **system -n 255.255.0.32**

> ***Note:***
> *Command parameters are case-sensitive (for example –S has not the same effect as –s).*

### 11.2.4.1 COMMON PARAMETERS

All commands support the following parameters:

| Parameter | Effect |
|---|---|
| **-d** | Displays the command description |
| **-i** | Displays information about the configuration |
| **-h** | Displays all parameters and values valid for the command |
| **-v** | Displays the command version |
| **-S** | Saves the settings in the startup configuration running to startup)) |
| **-D** | Enables debugging mode. |
| **-iy** | Displays the configuration in YAML format |

### 11.2.4.2 H49 SYSTEM COMMANDS

#### Switch

The switch command allows setting the switching mode of the device:

```
switch [-m <mode>] -S -i
```

| command | parameter | Description | Values |
|---|---|---|---|
| **switch** | **-m** | Sets the switching mode | StoreAndForward, adaptative |
| | **-i** | Displays configuration | |

#### Front Panel

The frontpanel command allows interacting with the front panel:

```
frontpanel –a <ip address> -l <state>
```

| command | parameter | Description | Values |
|---|---|---|---|
| **frontpanel** | **-a** | Sets the device IP address on the front panel | xxx.xxx.xxx.xxx |
| | **-c** | Updates LEDs on the front panel | |
| | **-l** | Enables/disables led chaser | enable, disable |
| | **-y** | Copies the command information in aYAML format | |
| | **-z** | Sets and applies immediately the state of the configuration setting controlling the display of the IP address on the front panel LCD (<enable>=Show / <disable>=Hide).<br>When the equipment is started, if this setting is set to disable in the startup configuration, then the IP address will be displayed on the front panel LCD for 10 seconds before to be hidden. | enable, disable |

### AlarmContact

The alarmContact command allows you to configure the behaviour of the alarm relay:

```
alarmContact [-c <contact>] [-f <state>] -S -i
```

| command | parameter | Description | Values |
|---|---|---|---|
| **alarmContact** | **-c** | Contact number | 1,2 |
| | **-f** | Force Logic Output State | unforced, energized, unenergized |

### Global Status

The system command allows you to configure the global settings of the system.

```
system [-a <IP Address>] [-n <netmask>] [-g <gateway>] [-s <DNS IP Address>] [-m <MAC
Address>] [-t<name>] -S -i
```

| command | parameter | Description | Values | Default |
|---|---|---|---|---|
| **system** | **-a** | Sets the Reason H49 IP Address | | **192.168.254.254** |
| | **-n** | Sets the Reason H49 net mask | 0 to 32 | **16** |
| | **-m** | Sets MAC Address. Restart is needed | | |
| | **-c** | Sets the Reason H49 name | | |
| | **-g** | Sets Gateway IP address | | **0.0.0.0** |
| | **-s** | Sets DNS Server IP Address | | **10.18.0.134** |
| | **-t** | Sets synchronization time | local, ntp, ptp | **ptp** |

The following values can be set the Time zone of the Reason H49:

| command | parameter | Description | Values |
|---|---|---|---|
| **timezone** | **-z** | Sets the time zone | |

### NTP

The following values can be set in the NTP configuration:

| command | parameter | Description | Values |
|---|---|---|---|
| **ntp** | **-a** | Sets the IP address of remote NTP server | |
| | **-c** | Disables or enables the NTP client | enable, disable |
| | **-p** | Sets the poll rate of NTP client | |
| | **-s** | Disables or enables the local NTP server | enable, disable |

### PTP

The following values can be set in the IEEE1588-v2 PTP configuration (VLAN, PCP, Mode).

```
ptp [-m <mode>] [-s <steps>] [-p1 <priority1>] [-p2 <priority2>] [-a <domain>] -o -S -i
```

| command | parameter | Description | Values |
|---|---|---|---|
| ptp | -m | Sets the IEEE1588-v2 operating mode | disable, ordinary, boundary |
| | -f | Sets the IEEE1588-v2 profile | power_2011, default_12 |
| | -l | Sets the IEEE1588-v2 delay | disabled, <p2p> TC peer-to-peer, <e2e> TC end-to-end |
| | -s | Sets the IEEE1588-v2 steps | 1, 2 |
| | -p1 | Sets the IEEE1588-v2 prority1 | 0 to 255 |
| | -p2 | Sets the IEEE1588-v2 priority2 | 0 to 255 |
| | -a | Sets the IEEE1588-v2 domain | 0 to 255 |
| | -n | Sets VLAN used for PTP | 0 to 4094 |
| | -c | Sets PCP used for PTP | 0 to 7 |
| | -o | Sets the PTP synchronization to slave mode. | |

### Redundancy Mode

The following values can be set to configure the Reason H49 Redundancy function:

| command | parameter | Description | Values |
|---|---|---|---|
| redundancy | -l | Sets the interlink ID | HSR-PRP-A, HSR-PRP-B |
| | -n | Sets the network ID | 1 to 6 |
| | -a | Sets redundancy supervision MAC address | |

### SNMP

SNMP is configured by manually editing the file **/etc/snmp/snmpd.conf**

| command | parameter | Description | Values |
|---|---|---|---|
| snmp | -s | Sets the single-quoted ‘configuration_line’ string into the configuration. The associated line is either added or modified if already existing. The line must NOT contain single-quote characters. | See "Supported SNMP settings" |
| | -d | Deletes the specified item (Unique ID, see -i) where ID is of the form CLASS.id as displayed by the -i listing (e.g.,: snmp -d ACCESS@RWGroup/usm/authPriv) or an administration command (**Great care shall be exercised in using such commands**). | |
| | -P | Prepares a new configuration from scratch | |
| | -C | Copies the current configuration to a new configuration | |
| | -L | Adds the single-quoted ‘configuration_line’ to the new configuration. The line must be valid, as it is not checked prior to being inserted in the new configuration... The line must NOT contain single-quote characters. | |
| | -A | Applies the new configuration after editing the config file (restarts the snmp service) | |

### SNMP Setting Details

Use the snmp -s <setting> command to get more information about the given setting.

### Supported SNMP Settings

The following configuration items are currently supported (parsed):

| Supported Configuration Items | | |
|---|---|---|
| • access | • engineIDType | • rwcommunity |
| • agentAddress | • group | • rwuser |
| • agentGroup | • includeAllDisks | • sysContact |
| • agentSecName | • iquerySecName | • sysLocation |
| • agentuser | • load | • sysName |
| • com2sec | • monitor | • sysServices |
| • createUser | • proc | • trap2sink |
| • disk | • rocommunity | • trapsink |
| • engineID | • rouse | • view |

***Note:***

*Unsupported settings are passed directly to the SNMP configuration without further checking. In the same manner, unsupported settings cannot be modified by using the* ***set*** *command; they shall be deleted prior to being re-set.*

*The list of currently supported settings may evolve over time. Use the* ***snmp -i*** *command to see which settings are currently supported. For further detail, please refer to http://www.net-snmp.org/docs/man/snmpd.conf.html.*

### Management

The following values can be set to save the Reason H49 configuration into the startup configuration file. It also makes it possible to load a new configuration without reboot.

```
configuration [-p <configuration>] [-l <filename>] -S
```

| command | parameter | Description | Values |
|---|---|---|---|
| **configuration** | **-p** | Displays the running or startup configuration settings | running, startup |
| | **-l** | Loads the running configuration file (.YAML) | /path/file |
| | **-f** | Sets the network-related settings to the factory default | |

The following values can be set to update the firmware of Reason H49 or change the general configuration for the redundancy mode or manage configuration backup/restore:

```
firmware [-f <update_file_name>.bin] [-h] [-i] [-r <redundancy_mode>] [-U
<upgrade_file>.tar.gz] [-u <url>] [-v] [-S] [-B] [-R]
```

| command | parameter | Description | Values |
|---|---|---|---|
| **firmware** | **-f** | Updates the firmware with a file (.bin) | |
| | **-B** | Generates a configuration backup. | |
| | **-R** | Restores a configuration backup. | |
| | **-r** | Changes the redundancy operating mode.<br>You must restart Reason H49 to apply changes. | HSR, HSR_PRP, PRP, NONE, QUADBOX |
| | **-U** | Upgrades the firmware from a **.tar.gz** file. Restart is needed | |
| | **-u** | Url of the upgrade file (**.tar.gz** file) | |

### 11.2.4.3 NETWORK COMMANDS

This section describes the commands used to manage the network functions.

#### 11.2.4.3.1 MAC ADDRESS TABLE

This command configures the MAC Address table behaviour.

```
macAddressTable [-a <Aging Time>] -S -i
```

| command | parameter | Description | Values |
|---|---|---|---|
| **macAddressTable** | **-a** | Sets the Address Lifetime | |
| | **-b** | Sets the **Aging Base Time** i.e how long MAC addresses remain in the Ethernet switching table.<br>Reason H49 uses a mechanism called aging to store MAC addresses in the Ethernet switching table (the MAC table). When the aging time for a MAC address in the table expires, the address is removed.<br>For each MAC address in the Ethernet switching table, the switch records a timestamp of when the information about the network node was learned.<br>Each time the switch detects traffic from a MAC address that is in its Ethernet switching table, it updates the timestamp of that MAC address.<br>A timer on the switch periodically checks the timestamp, and if it is older than the value set for mac-table-aging-time, the switch removes the node's MAC address from the Ethernet switching table. | |
| | **-f** | Sets the HSR entryForgetTime | 10, 20, 40, 80, 160, 320, 640, 1280 |

#### 11.2.4.3.2 FILTERING

The following values can be set to configure filtering and redirection policy.

This command is also used to create rules to perform specific actions on specific Mac addresses.

```
filtering <interface> -e <entry> -s <state> -a <MAC address> -l <length> -t <type> -f
<interfaces list> -p <priority> -S -i
```

| command | parameter | Description | Values |
|---|---|---|---|
| **filtering** | **-e** | Sets the filter entry | 4 to 9 |
| | **-s** | Sets the filter entry state | enable, disable |
| | **-a** | Sets the filter MAC Address | xx:xx:xx:xx:xx:xx |
| | **-f** | Sets the filter ports allowed (interfaces into which the matching frame can be forwarded). | None<br>SE01<br>CE01<br>CE02<br>CE03<br>CE04<br>CE05<br>CE06 |
| | **-l** | Sets the filter length (mask length from the start of the MAC addresses for incoming frame) | 0 to 48 |
| | **-t** | Sets the filter type (the source or the destination MAC address to compare). | scr, dst |
| | **-p** | Sets the priority queue | 0 to 3 |
| | **-r** | Displays reserved filter fields<br>(to be used with –i) | |

## 11.2.4.4 SECURITY COMMANDS

### Security Settings

The following values can be set in the Security configuration to setup security options about user session and user password policy.

```
security [-I <minutes>] [-l <minutes>] [-a <nb_max_attempts>] [-P <state>] [-L
<length>] [-i] [-f] [-k <path>] [-r] [-c <path>] [-s <path>] [-e <expire_period>]
```

| command | parameter | Description | Values |
|---|---|---|---|
| **security** | **-f** | Reverts the switch to factory settings (Need reboot) | |
| | **-i** | Displays information about user login and password | Username, <null> |
| | **-l** | Lock period in minutes | 1 to 999 |
| | **-a** | Maximum login attempts | 3 to 10 |
| | **-I** | Inactivity period to log off users | 1 to 999 |
| | **-L** | Minimum user's password length | |
| | **-P** | Enables / Disables password policy | Enable, Disable |
| | **-c** | Sets a new LDAP certificate (for SSL/Start TLS) | LDAP certificate file name (See 8.1.6 **Certificate Management** section) |
| | **-r** | Restore the factory default HTTPS certificate for the web application. | |
| | **-s** | Sets a new syslog certificate | Syslog certificate file name (See 8.1.6 **Certificate Management** section) |
| | **-k** | Sets a certificate for Reason web user interface (HTTPS) | HTTPS certificate file name (See 8.1.6 **Certificate Management** section) |

### User Account

The following values can be set to configure and manage all user accounts (create, modify or delete user or user group...).

| command | parameter | Description | Values |
|---|---|---|---|
| **account** | **-c** | Creates a new user | |
| | **-g** | Adds user role | Viewer, engineer, secadm, secaud |
| | **-m** | Modifies group GID | |
| | **-u** | Sets the user login name | |
| | **-n** | Modifies the user login name | |
| | **-f** | Modifies the user full name | |
| | **-p** | Sets a new password for a user | |
| | **-r** | Removes a user | |
| | **-s** | Enables / Disables a user account | Enable, Disable |
| | **-R** | Removes role from a user | |
| | **-U** | Unlocks user account | |
| | **-e** | Sets the expiration period for the specified user account | |

### LDAP Server

The following values can be set in the LDAP configuration to use Central Authentication:

| command | parameter | Description | Values |
|---|---|---|---|
| ldap | -a | Sets the LDAP server's address or FQDN | |
| | -p | Sets the TCP/IP port | |
| | -b | Sets the base dn of LDAP Server<br>Organizational Unit (ou)<br>Domain component (dc) | |
| | -r | Sets the bind domain name to dialog with the LDAP server<br>Common name (cn)<br>Domain component (dc) | |
| | -P | Sets the bind domain name password | |
| | -t | Specifies a timeout in seconds after which calls to synchronous LDAP APIs will abort if no response is received | |
| | -s | Enables/Disables SSL (Certificate is needed. See 8.1.6 **Certificate Management** | no / start_tls |
| | -e | Turns LDAP on | |
| | -x | Turns LDAP off | |

***Note:***
*Refer to Appendix 2 for additional information and examples about use cases applied with ldap CLI command.*

### SysLog Server

The Log command allows you to manage the log feature such as configuring the remote syslog information, enabling / disabling central logs:

| command | parameter | Description | Values |
|---|---|---|---|
| log | -e | Enables central log | |
| | -D | Disables central log | |
| | -S | Sets the remote log server IP or FQDN | <server_ip_address><port> |
| | -P | Sets the TCP/IP port | |
| | -p | Sets the IP protocol for the remote log server (Refer to 8.1.6 **Certificate Management** section for TLS certificate) | udp, tcp, tcp/tls |
| | -r | Sets the maximum of messages/second sent to the remote log server. | |
| | -s | Shows local log file | |

### Banner Text

The following values can be set to configure the login banner text to be displayed at user log on:

| command | parameter | Description | Values |
|---|---|---|---|
| bannertext | -a | IP address of the remote FTP/SFTP server | |
| | -D | Enables the debug mode | |
| | -f | Path / Filename to be used | |
| | -l | Updates the banner text using a local file | /path/filename |
| | -n | User name for the remote FTP/SFTP server | |
| | -m | Updates the banner text with a message | "text" |
| | -p | Protocol to be used for the remote FTP/SFTP server | |
| | -r | Sets the banner text with a remote file. | |
| | -s | Enables/disables the banner | enable, disable |

### Communication Protocol

The following values can be set in the Communication Protocol configuration:

| command | parameter | Description | Values |
|---|---|---|---|
| Communicationprotocol | -f | Sets the port for the FTP protocol | |
| | -u | Defines the insecure protocols (Telnet, ftp) | |
| | -S | Defines the secure protocols (SSH, SFTP) | |
| | -p | Sets the port for secure protocols | |
| | -s | Enables or disables the secure or insecure protocol | |
| | -t | Sets the port for the Telnet protocol | |

## 11.3 APPENDIX 2: COMMAND LINE USE CASES

This section figures out the usage of the H49 command lines with simple examples.

> ***Note:***
> *All variable parameters and values used in this section are chosen arbitrary and only for description purposes.*

### 11.3.1 SYSTEM COMMANDS

This section describes command lines used to manage the system.

#### 11.3.1.1 REDUNDANCY

The example below shows the use of the `redundancy` command line:

| Command | Description |
|---|---|
| `Redundancy -l -n -a` | Sets the Reason H49 redundancy mode, the network ID and the redundancy supervision MAC address |

**Example:**

```
redundancy -l HSR-PRP-A -n 2 -a 01:15:4E:00:01:00
```

#### 11.3.1.2 SYSTEM

The example below shows the use of the `system` command line:

| Command | Description |
|---|---|
| `system -a -n -g -c -t` | Sets the switch IP address, netmask, name and synchronization type together with the gateway IP address |

**Example:**

```
system -a 192.168.254.254 -n 16 -g 0.0.0.0 -c SWH49 -t ptp
```

#### 11.3.1.3 SWITCH

The example below shows the use of the `switch` command line:

| Command | Description |
|---|---|
| `switch -m` | Sets the switching mode |

**Example:**

```
switch -m adaptative
```

#### 11.3.1.4 ALARM CONTACT

The example below shows the use of the `alarmContact` command line:

| Command | Description |
|---|---|
| `alarmContact -c -f -c -f` | Sets the Logic Output State of each contact |

**Example:**

```
alarmContact -c 1 -f unforced -c 2 -f unforced
```

### 11.3.2 NETWORK COMMANDS

This section describes the commands used to manage the network functions.

#### 11.3.2.1 INTERFACE

The example below shows the use of the **interface** command line:

| Command | Description |
|---|---|
| `Interface -i` | Shows the interface status, VLAN settings |

**Example:**

```
root@h49:~# interface -i

Interfaces Status:
------------------
Port    Type      Supported          Status      Link Mode    Autoneg    State         Mode
----    ----      ---------          ---------   ---------    -------    ----------    ----------------------------
CE01    Fibre     100Mb/s            connected   100 full     on         Forwarding    HSR A
CE02    Fibre     100Mb/s            up                       on         Disabled      HSR B
CE03    Fibre     100Mb/s            connected   100 full     on         Forwarding    Standard
CE04    None      10/100/1000Mb/s    up                       on         Disabled      Standard
CE05    None      10/100/1000Mb/s    up                       on         Disabled      Standard
CE06    None      10/100/1000Mb/s    up                       on         Disabled      Standard

Interfaces VLAN Setting:
------------------------
Port    Mode     Default  Default  VlanID  Tagging  PCP0  PCP1  PCP2  PCP3  PCP4  PCP5  PCP6  PCP7
                 VlanId   Pcp      MapId
----    ------   -------  -------  -----   -------  ----  ----  ----  ----  ----  ----  ----  ----
                 0        0        0               0     0     0     0     0     0     0     0
CE01    trunk    1        0        0       on      0     0     1     1     2     2     3     3
CE02    trunk    1        0        0       on      0     0     1     1     2     2     3     3
CE03    trunk    1        0        0       on      0     0     1     1     2     2     3     3
CE04    trunk    1        0        0       on      0     0     1     1     2     2     3     3
CE05    trunk    1        0        0       on      0     0     1     1     2     2     3     3
CE06    trunk    1        0        0       on      0     0     1     1     2     2     3     3

Interfaces VLAN belonging:
--------------------------
Port    VLAN Id  VLAN Name
----    -------  ---------

CE01    0        Vlan_0
CE01    1        default

CE02    0        Vlan_0
CE02    1        default

CE03    0        Vlan_0
CE03    1        default

CE04    0        Vlan_0
CE04    1        default

CE05    0        Vlan_0
CE05    1        default

CE06    0        Vlan_0
CE06    1        default
```

### 11.3.2.2 VLAN

The example below shows the use of the **vlan** command line:

| Command | Description |
|---|---|
| `vlan -c -l -p` | Sets the name of the VLAN, its ID and the ports to be added |

**Example:**

```
vlan -c test -l 5 -s test -p CE01:CE02:CE03:CE04:CE05
```

### 11.3.2.3 MAC ADDRESS TABLE

The example below shows the use of the **macAddressTable** command line:

| Command | Description |
|---|---|
| `macAddressTable -a -b -f` | Sets the MAC address lifetime, aging base time and HSR entry forgetTime |

**Example:**

```
macAddressTable -a 48 -b4 -f 10
```

### 11.3.2.4 NTP

The example below shows the use of the **ntp** command line:

| Command | Description |
|---|---|
| `ntp -s -c -a -p` | Disables or enables the local NTP server and client and sets the IP address of remote NTP server together with the poll rate of NTP client |

**Example:**

```
ntp -s disable -c disable -a 127.0.0.1 -p 3
```

### 11.3.2.5 PTP

The example below shows the use of the **ptp** command line:

| Command | Description |
|---|---|
| `ptp -m -l -f -p1 -p2 -a -s -c -n -S` | Sets the IEEE1588-v2 PTP configuration i.e. the operating mode, delay, profile, domain, and step together with the IEEE1588-v2 prority1 and 2, the priority code point (PCP) of the PTP frames and the VLAN used. |

**Example:**

```
ptp -m ordinary -l p2p -f power_2011 -p1 128 -p2 128 -a 0 -s 2 -c 4 -n 0 -s 1
```

#### 11.3.2.6 TIMEZONE

The examples below show the use of the **timezone** command line:

| Example of command | Description |
|---|---|
| `timezone -z <time zone>` | Sets the H49 time zone |

**Example:**

`timezone -z/Europe/Andorra`

#### 11.3.2.7 BANNER TEXT

The examples below show the use of the **bannertext** command line:

| Example of command | Description |
|---|---|
| `bannertext -M "message"` | Updates the banner text with a message |

**Example:**

`bannertext -M "This is a banner text" of the` **`bannertext`** `command line:`

### 11.3.3 SECURITY COMMANDS

This section describes the command lines used to manage security functions.

#### 11.3.3.1 ACCOUNT

The examples below show the use of the **account** command line:

**Information**

| Example of command | Description |
|---|---|
| `account -i` | Displays information about account configuration |

**Example:**

```
root@h49:~# account -i
User Informations:
                login:  root
             fullname:  root
                roles:  root*
           is blocked:  no
          is disabled:  no
 password last change:  2016-12-13
   password expire on:  2018-07-14
User Informations:
                login:  user
             fullname:  (null)
                roles:  viewer, engineer, secadm, secaud
           is blocked:  no
          is disabled:  no
 password last change:  2016-03-14
   password expire on:  2016-10-13
```

**Figure 106: SSH Console – Information about the account configuration**

### Create a new user

| Example of command | Description |
|---|---|
| `account -u <user_name> -c <user_group> -p <password>` | Creates a new user with a user group and a password |

**Example:**

```
account –u JohnDoe –c secadm –p General
```

## 11.3.3.2 LDAP

The examples below show the use of the **ldap** command line:

### Configure LDAP Server

| Example of command | Description |
|---|---|
| `ldap -a <IP_address>,<FQDN> -p <Port_number>` | Sets the LDAP server address with a FQDN, an IP address and the port of connection |

**Example:**

```
ldap -a 192.168.254.80,H49-ADDC.dsagile2019.intern -p 389
```

### Configure LDAP Base DN

| Example of command | Description |
|---|---|
| `ldap -b <ou>,<dc>,<dc>` | Sets the base DN for the LDAP connection |

**Example:**

```
ldap -b OU=H49_USERS,DC=dsagile2019,DC=intern
```

### Configure User DN and Password and Timeout

| Example of command | Description |
|---|---|
| `ldap -r <cn>,<ou>,<ou>,<dc>,<dc> -P -t` | Sets the user DN to connect to the LDAP database, then configures the password of the user DN and the connection timeout. |

**Example:**

```
ldap -r CN=dcs_query,OU=DSAUsers,OU=DSAgile,DC=dsagile2019,DC=intern -P 'Azerty123!' -t 2
```

***Note:***
*Special characters in LDAP passwords require to be written with " " for instance ldap -P abc**'!'**xyz*

### 11.3.3.3 SECURITY

The examples below show the use of the **security** command line:

#### Information

| Example of command | Description |
|---|---|
| `security -i` | Displays information about security configuration |

**Example:**

```
root@h49:~# security -i
Login Security Informations:
        Inactivity timeout:     600 secondes
           Locking period:      10 secondes
Consecutive login attempts:     3 times

Password Policies Security Informations:
          Policies enabled:     enable
            Capital letter:     enable
                    Number:     enable
          Special character:    enable
               Tiny letter:     enable
             Minimal length:    9
```

**Figure 107: SSH Console – Information about the security configuration**

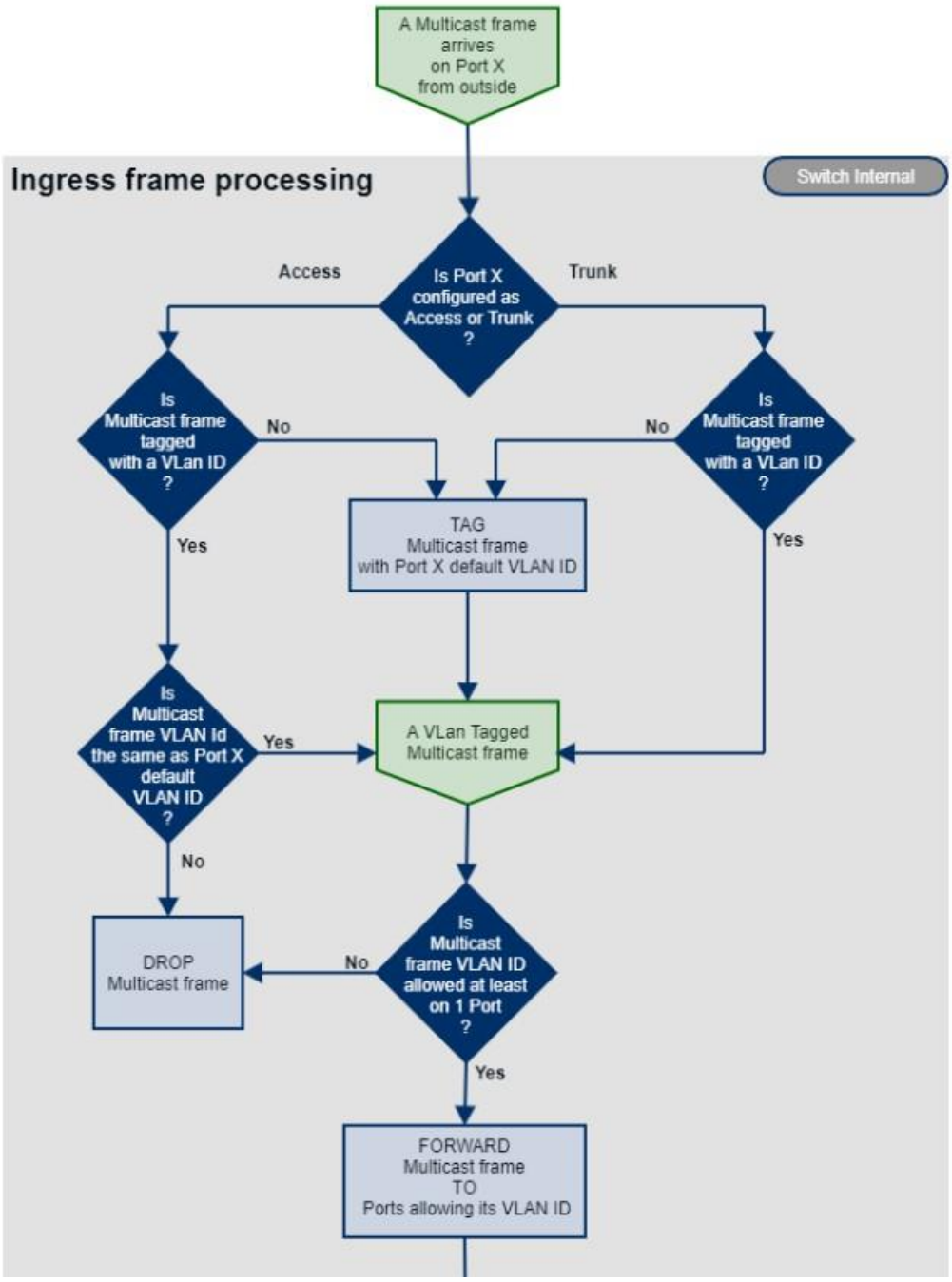
#### Lock Period

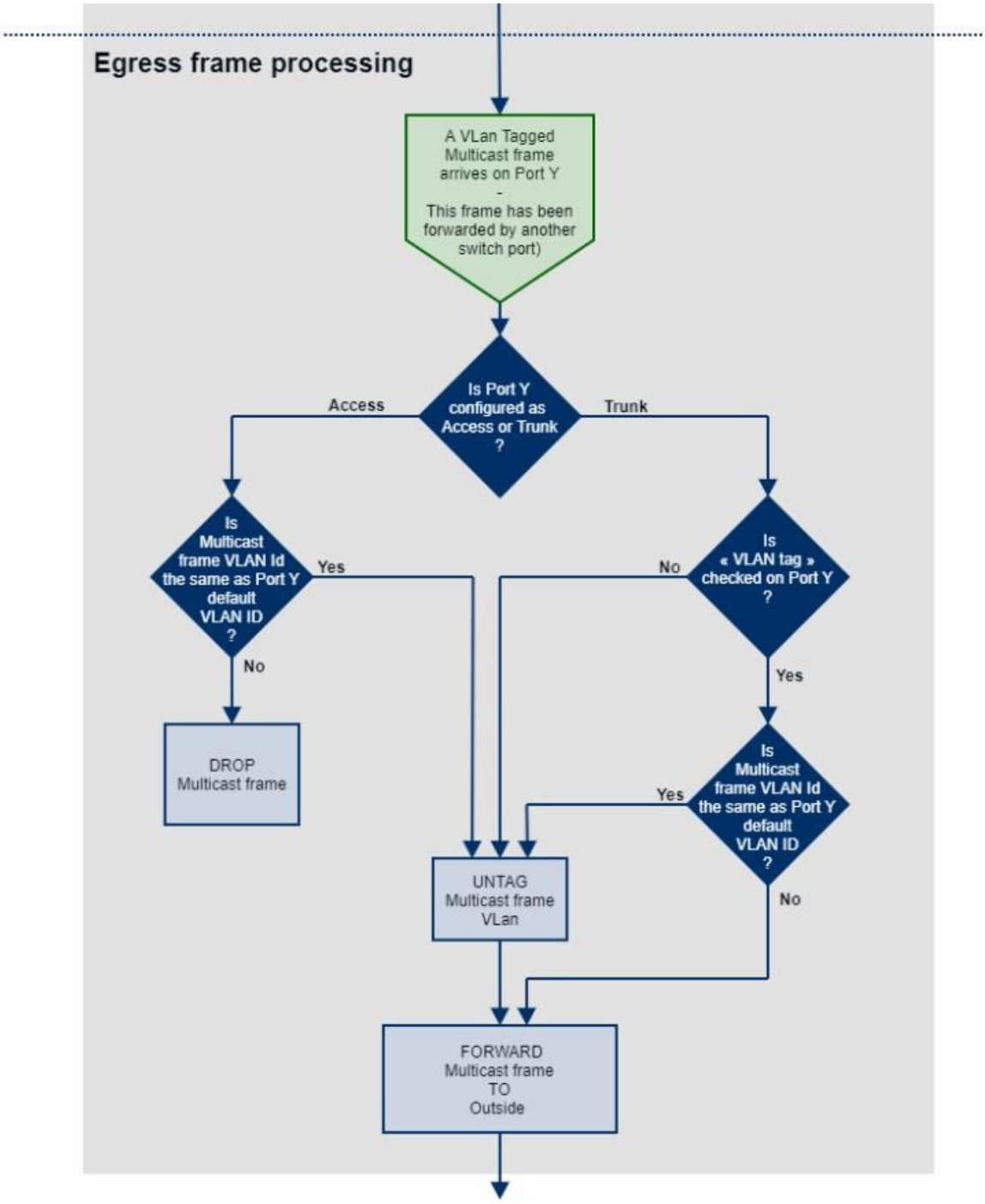
| Example of command | Description |
|---|---|
| `security -l 10` | Sets the lock period to 10 minutes |

**Example:**

```
root@h49:~# security -l 10
```

## 11.4 APPENDIX 3: VLAN FRAME PROCESS




Egress frame processing
A VLan Tagged Multicast frame arrives on Port Y
-
This frame has been forwarded by another switch port)
Is Port Y configured as Access or Trunk ?
Access
Trunk
Is Multicast frame VLAN Id the same as Port Y default VLAN ID ?
Yes
No
DROP Multicast frame
Is « VLAN tag » checked on Port Y ?
No
Yes
Is Multicast frame VLAN Id the same as Port Y default VLAN ID ?
Yes
No
UNTAG Multicast frame VLan
FORWARD Multicast frame TO Outside

GE VERNOVA