GIGABIT/FAST ETHERNET SWITCH/ROUTER

TYPE SW3-L3

USER GUIDE

V06 - February 2019

M0SW3M1902Iv07

ZIV
Antonio Machado,78-80
08840 Viladecans, Barcelona-Spain

Tel.: +34 933 490 700
Fax: +34 933 492 258
Mail to: ziv@zivautomation.com

www.zivautomation.com

SAFETY SYMBOLS

!

⚠

WARNING OR CAUTION:

This symbol denotes a hazard. Not following the indicated procedure, operation or alike could mean total or partial breakdown of the equipment or even injury to the personnel handling it.

NOTE:

Information or important aspects to take into account in a procedure, operation or alike.

CONTENTS

Page

Page

1 INTRODUCTION

1.1 GENERAL

The SW3-L3 is a Gigabit/Fast Ethernet switch/router specially designed to perform switching functions (L2) and IPv4 routing functions (L3).

Level 2 capabilities enable deployment of big scale LANs when the main requirements are:

- Port density,
- switching performance, and
- logical complexity.

Level 3 capabilities offer:

- Routing functionality between two or more configured VLANs, with each VLAN being made up of a set of local ports (Ethernet and Gigabit Ethernet).
  The routing process is performed in hardware, that is, at wire speed for unicast traffic.

The SW3-L3 supports the SNMPv1, SNMPv2c and SNMPv3 management protocols, the RIPv1, RIPv2, OSPFv2 and BGPv4 routing protocols, the VRRP redundancy protocol, as well as other protocols and services such as LLDP, GARP/GMRP, IGMP, DHCP, NTP/SNTP, TACACS+ and RADIUS.

As a level 2 switch, SW3-L3 brings the necessary capabilities to implement the automation of electrical substations according to the IEC 61850 standard.

The SW3-L3 supports standard IEEE 1588v2 clock synchronization (Precision Time Protocol), in Transparent Clock (TC) P2P mode.

The SW3-L3 can be managed locally and remotely, through a local console, Telnet server and SSH server, or through a built-in web server, HTTP or HTTPS.

The SW3-L3 stores an internal backup copy of the application software so, in case of some incidence, the operation of the equipment is guaranteed by running the backup software.

1.2 MAIN CHARACTERISTICS

Some of the SW3-L3 most important features are described below.

❖ **Grouping of services and architectures.**

Services may be grouped and discriminated, some not being accessible with others, through the configuration of different VLANs.

Each VLAN is different from the others thanks to a specific identifier, called VID, which is included in the VLAN tag and specified in the standard IEEE 802.1q. It permits several VLANs to share resources, either switching devices such as the SW3-L3, or links between switching units, guaranteeing that each VLAN traffic will remain isolated from the others.

The standard 802.1q admits three types of frames: untagged frames, tagged frames with the VLAN (VID) identifier and the priority (tagged) or only the priority (priority tagged, VLAN = 0).

The SW3-L3 may adapt to different network architectures, such as: star, double star, ring, double ring, and linked rings.

FIGURE 1 Traffic separation

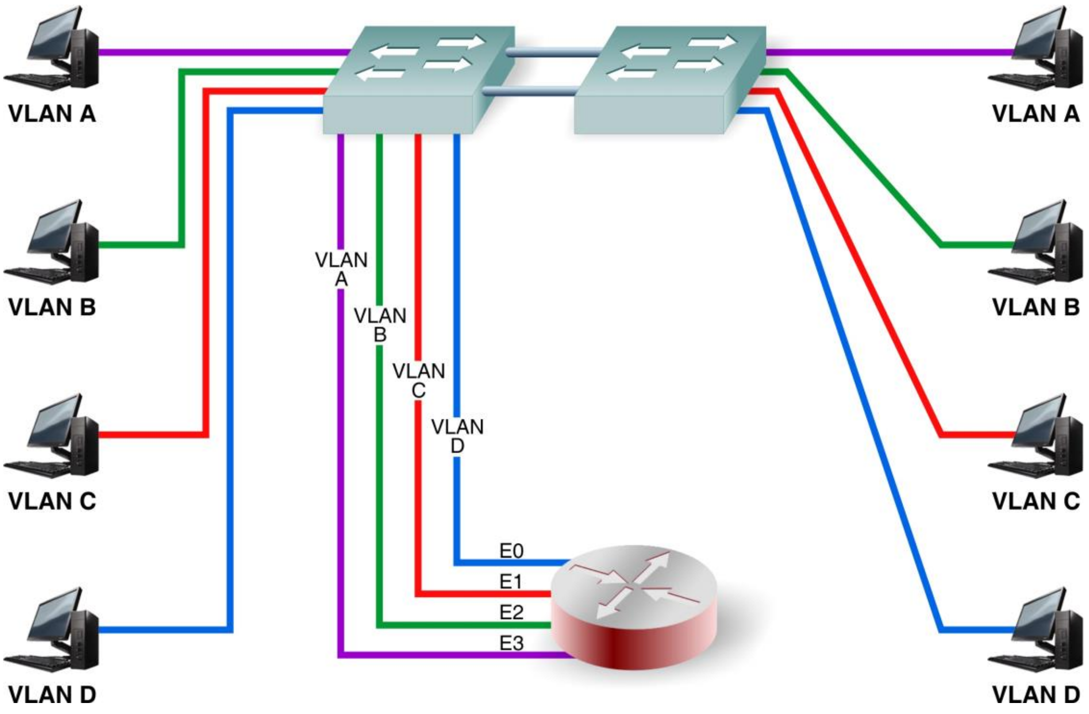


FIGURE 2 Star topology

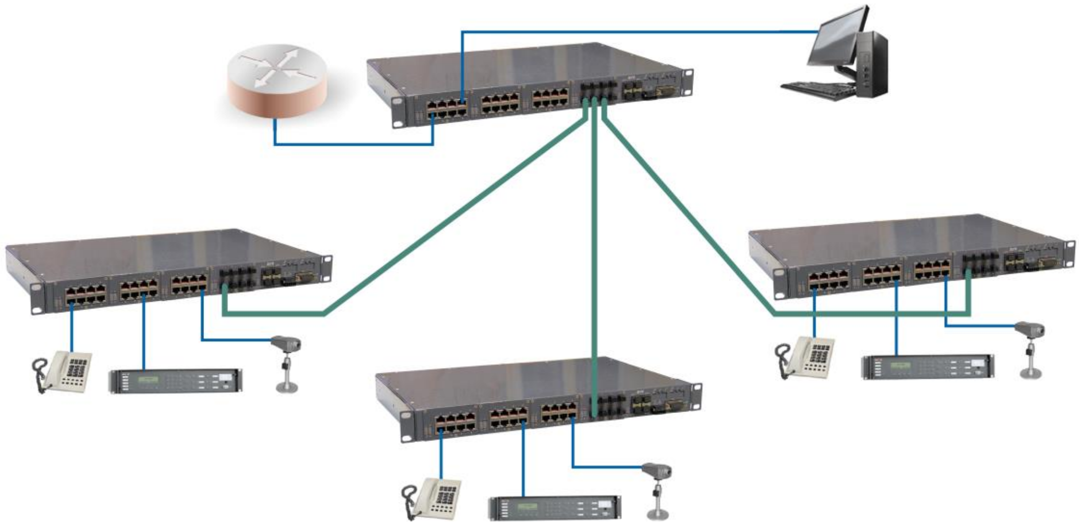
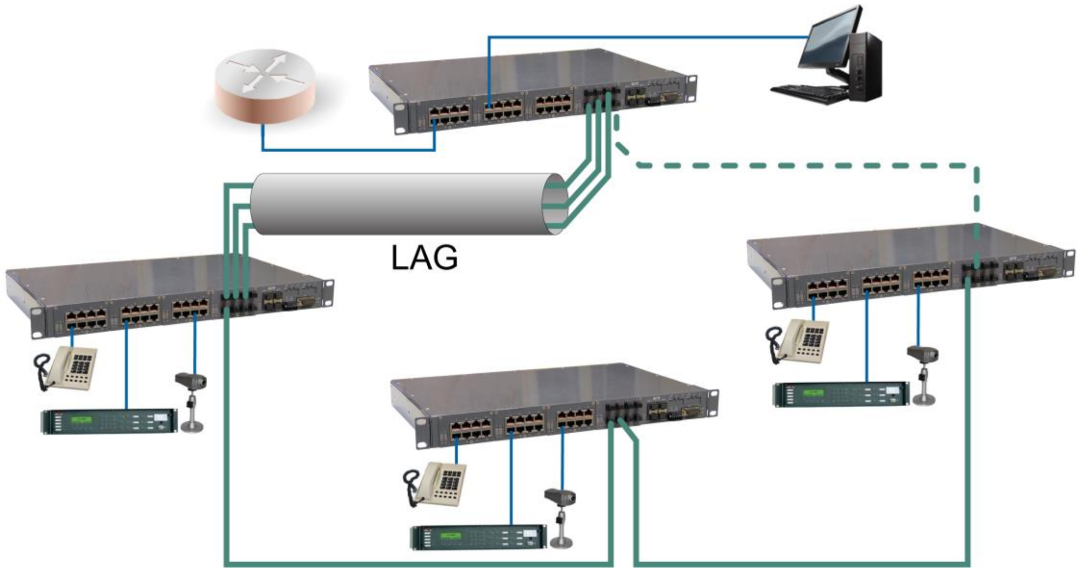


FIGURE 3 Rings



- **Link Aggregation by LAG function.**

  The Link Aggregation Group (LAG) function allows grouping several links into a single aggregated link identifier. FIGURE 3 illustrates an example of link aggregation. From the point of view of the STP/RSTP protocol, the connection entity is the LAG group identifier. In this way, the different links that are part of the LAG are not handled individually and are not considered a loop, and thus it provides the aggregated bandwidth.

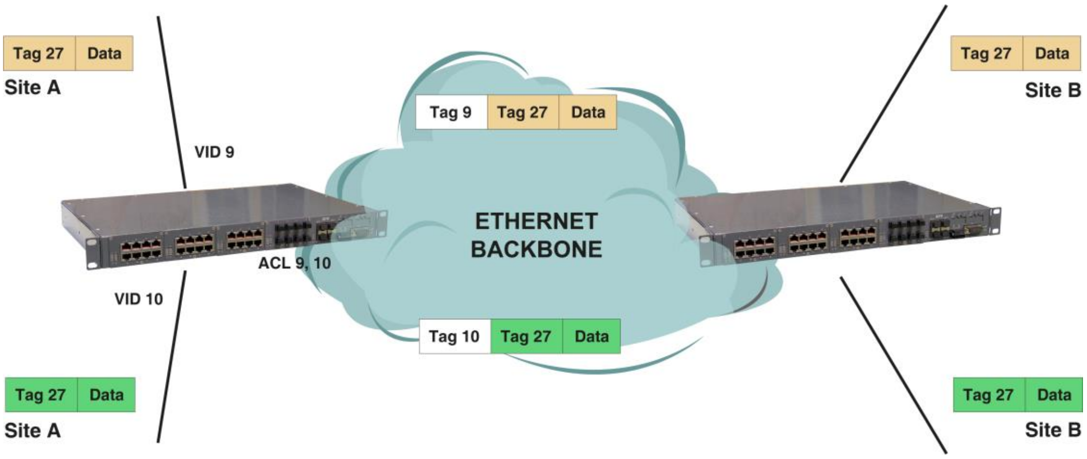
  Link aggregation can be created for any of the planned interface functions: user (edge, untag), inter-switch link (trunk or native) and those associated to the Q-in-Q functionality (access and core). Once the LAG is selected, the set of parameters of the interface selected as *Leader* determines the behaviour of the group.

- **Q-in-Q operation.**

  The SW3-L3 includes two functions that provide Q-in-Q operation (double-tagged). In this operation mode, the frames include the original tag (C-TAG), either generated by the client equipment or assigned by the switch itself at the moment is received, and a second tag, the tag of the provider (S-TAG), which will be the tag used in the network of the service provider.

  The 802.1Q tunnels are a useful tool to reuse the identification VID values of the VLAN, or for transiting data over third-party networks.

FIGURE 4 Q-in-Q operation



- **Advanced RSTP implementation.**

  The SW3-L3 not only complies with the STP and RSTP protocols for resolving loops in the network and operation in rings, but it also exceeds the recovery times obtained through said protocols. Thus, the SW3-L3 guarantees recovery times lower than 4 ms per link via the RSTP standard in case of failure.

- **Critical services and security.**

  The different services have their level of importance. For example, sending orders to open a switch has priority over the traffic from a telephone connection. The SW3-L3 has Quality of Service (QoS), which identifies critical services, guaranteeing that all traffic receives the appropriate priority.

  On the other hand, the SW3-L3 implements different security features that prevent unauthorized access to the traffic system, such as: port disabling, traffic restriction according to MAC addresses, authentication protocols (TACACS+, RADIUS), etc.

- **Broadcast traffic limitation.**

  In order to avoid the network flooding, the SW3-L3 selects maximum volume limits for different combinations of broadcast, multicast, and flooding messages, in each one of their ports.

- **Multicast traffic.**

  The SW3-L3 has two protocols for adapting the multicast traffic to the desired interfaces. The protocols are:

  - **GARP/GMRP (IEEE 802.1D 2004).** The GMRP clients request to the SW3-L3 the selective transmission of the multicast traffic desired by each of them.
  - **IGMP.** The SW3-L3 manages multicast traffic based on the IGMP messages exchanged by the client devices and the multicast routers (IGMP Snooping). To be operative, the GARP/GMRP protocol must be INACTIVE.

  The SW3-L3 also selects the multicast flows in an explicit and manual way (static configuration).

- **Port mirroring.**

  The SW3-L3 resends traffic copies of one or more ports to another one, the monitoring port, being able to select incoming or outgoing traffic copies in each monitored port in an independent manner.

- **IP routing.**

  The SW3-L3 is an IPv4 router for unicast traffic. The data for the routing function may have two sources; static data of a permanent nature (configured by the user) and dynamic data, obtained by the equipment itself through executing the standard routing protocols: RIP, OSPF and BGP. All these protocols can be active simultaneously.

  In addition to routing function, the equipment has the VRRP redundancy protocol, so that it may be part of one or various virtual routers.

- **Traffic filtering.**

  All traffic processed by the SW3-L3 takes into account the filtering rules that the user might configure so that routing operations are subject to restrictions as: ***input interface***, ***output interface*** (from the routing table), ***IP address of origin network***, ***IP address of destination network*** or the ***service*** *(tcp, udp)*, the latter supports the use of a range of ports, both destination and origin.

  Filtering rules admit conditions in many fields.

1.3 EQUIPMENT COMPOSITION

The SW3-L3 is provided in a 19" shelf that is 1 standard unit (s.u.) in height, prepared for rack mounting.

It includes a serial maintenance interface (DCE mode) and an I/O connector (see section 2.8), and can include 4 front or rear Gigabit Ethernet SFP bays, and up to front or rear 32 ports without PTP (Precision Time Protocol) or, instead of the previous ones, up to 24 IEEE 1588 (Precision Time Protocol) ports.

The SW3-L3 has a 4-block mechanical structure for the installation of the ports. See in section 1.4.2, *Equipment interfaces*, the types of blocks available and their requirements.

The main power supply may be isolated DC or multirange (V_{DC} and V_{AC}). The SW3-L3 may include an isolated DC or multirange (V_{DC} and V_{AC}) redundant power-supply option and, in the front port model, a PoE power-supply option for the direct connection of IP devices (IEEE 802.3 af) in eight electrical ports (1 to 4 of block 1 and 1 to 4 of block 2).

1.4 TECHNICAL SPECIFICATIONS

1.4.1 SW3-L3 characteristics

- Full Duplex Wired Speed switching core.
- Port speed automatic detection.
- STP and RSTP for resolving loops in the network and operation in rings.
- Multiple VLANs management (250 simultaneously).
- QoS. The SW3-L3 can use the priority fields included in the IEEE 802.1p tag, such as the DSCP identifier included in the IP header.
- Broadcast and Multicast (Broadcast Storm Control) traffic limitation.
- MAC access control lists and 802.1x user authentication.
- Q-in-Q operation (double-tagged).
- Link aggregation by LAG function, static, according to IEEE 802.1ad.
- Port mirroring.
- Links in VLAN Native mode.
- Interoperability with IEDs (Intelligent Electronic Device) that complies with the IEC 61850 requirements.
- Compatible with standard IEEE 1588v2 clock synchronization (Precision Time Protocol) in Transparent Clock (TC) P2P mode.
- Routing capabilities for unicast traffic.
    - RIPv1, RIPv2, OSPFv2 and BGPv4 routing protocols.
- Traffic filtering (Access Control List) and IPv4 traffic filtering.

1.4.2 Unit interfaces

- 1 service console (DCE mode).
- 4 Gigabit Ethernet SFP bays (see section 1.4.3, *Accessories*), front or rear.
- One I/O connector with one digital input and output that can be managed via SNMP. The digital output can be configured as an alarm.
- Front or rear ports.
- The ports are grouped into two different classes that cannot be mixed together: up to 32 ports without PTP (Precision Time Protocol) or up to 24 ports with PTP.
- The chassis has a mechanical structure **of up to four blocks** for the installation of the ports.
  For the ports without PTP, the block types to be combined are the following:
  - Block of **8** ports type **10/100Base-Tx** with **RJ-45** connector.
  - Block of **8** ports type **10/100Base-Tx** with **RJ-45** connector and **PoE** in the first four ports (always front).
  - Block of **4** or **8** ports type **100Base-Fx multimode** (1300 nm) with **MT-RJ** connector.
  - Block of **2** or **4** ports type **100Base-Fx multimode** (1300 nm) with **ST** connector.
  - Block of **2** or **4** ports type **100Base-Fx multimode** (1300 nm) with **SC** connector.
  - Block of **4** or **8** ports type **100Base-Fx multimode** (1300 nm) with **LC** connector.
  - Block of **4** or **8** ports type **100Base-Lx singlemode** (1300 nm) with **LC SM** connector.

The blocks must be installed consecutively, from left to right, without leaving empty slots.

If there are electrical ports, they must always be in the first position.

If only fiber optic ports are used, a maximum of 24 ports are supported.

No port blocks with 4 connectors MT-RJ, 2 connectors ST, 2 connectors SC or 4 connectors LC (LC SM) should be installed in the first position.

The **PoE power-supply** option for the direct connection of IP devices (IEEE 802.3 af) is available in electrical and front ports. A maximum of 8 PoE ports is supported, distributed in two groups of four (**1 to 4 of block 1** and **1 to 4 of block 2**).

For the ports with PTP, the block types to be combined are the following:

- Block of **6** ports type **10/100Base-Tx** with **RJ-45** connector.
- Block of **4** ports type **10/100Base-Tx** with **RJ-45** connector and **2** Gigabit Ethernet **SFP** bays.
- Block of **4** ports type **10/100Base-Tx** with **RJ-45** connector and **2** ports type **100Base-Fx multimode** (1300 nm) with **MT-RJ** connector.
- Block of **4** ports type **10/100Base-Tx** with **RJ-45** connector and **2** ports type **100Base-Fx multimode** (1300 nm) with **LC** connector.
- Block of **4** ports type **10/100Base-Tx** with **RJ-45** connector and **2** ports type **100Base-Lx singlemode** (1300 nm) with **LC SM** connector.
- Block of **4** ports type **10/100Base-Tx** with **RJ-45** connector and **2** ports type **100Base-Fx multimode** (1300 nm) with **ST** connector.
- Block of **4** ports type **10/100Base-Tx** with **RJ-45** connector and **2** ports type **100Base-Fx multimode** (1300 nm) with **SC** connector.

The blocks must be installed consecutively, from left to right, without leaving empty slots.

1.4.3 Accessories

- Gigabit/Fast Ethernet SFP modules.

  The following list corresponds to verified modules, which comply with the temperature criteria.

  - SFP 1000BaseT (4CZ07980001)
    type of connector: RJ-45

  - SFP 1000BaseSx (4CZ07980002)
    type of connector: LC
    type of fiber: multimode
    wavelength: 850 nm
    typical maximum distance: 550 m

  - SFP 1000BaseZx (4CZ07980004)
    type of connector: LC
    type of fiber: singlemode
    wavelength: 1530 nm
    typical maximum distance: 80 km

  - SFP 1000BaseLx (4CZ07980005)
    type of connector: LC
    type of fiber: singlemode
    wavelength: 1310 nm
    typical maximum distance: 10 km

  - SFP 100BaseEx (4CZ07980008)
    type of connector: LC
    type of fiber: singlemode
    wavelength: 1310 nm
    typical maximum distance: 40 km

  - SFP 100BaseFx (4CZ07980006)
    type of connector: LC
    type of fiber: singlemode
    wavelength: 1310 nm
    typical maximum distance: 10 km

  - SFP 100BaseFx (4CZ07980007)
    type of connector: LC
    type of fiber: multimode
    wavelength: 1310 nm
    typical maximum distance: 2 km

- Optical fiber pigtails.

  - Flat RJ45 STP CAT6 cable, 3m length (4GL03000141).
  - Multimode fiber MTRJ-MTRJ, 2m length (4CZ05000010).
  - Multimode fiber MTRJ-SC, 2m length (4CZ05000011).
  - Multimode fiber MTRJ-ST, 2m length (4CZ05000012).
  - Multimode fiber MTRJ-LC, 2m length (4CZ05000013).
  - Multimode fiber LC-LC, 2m length (4CZ05000014).
  - Singlemode fiber LC-LC, 2m length (4CZ05000015).

1.4.4 Equipment management

- Local and remote access, through a local console, Telnet server and SSH server, or through a built-in web server, HTTP or HTTPS.

1.4.5 Additional services

- SNMP (SNMPv1, SNMPv2c and SNMPv3) agent.
- NTP server and NTP/SNTP client.
- TACACS+ client.
- RADIUS client.
- GARP/GMRP (IEEE 802.1D 2004).
- IGMP snooping.
- DHCP server and client.
- DHCP Relay.
- VRRP.
- LLDP (IEEE 802.1AB 2016).
- TLS 1.0.

1.4.6 Certifications

- CE.
- Designed for industrial applications.
- Designed for Electrical Substations.

1.4.7 Mechanical characteristics

Mechanical enclosure:	shelf that is 19" wide and 1 standard unit (s.u.) high.
Dimensions:	Height: 44 mm; Width: 440 mm; Depth: 287 mm.
Weight:	3.4 kg
IP protection level:	IP 2xB
Material:	Grey (RAL 7024) zinc-plating iron.

For more mechanical details, see chapter 2, *Mechanical and electrical characteristics.*

1.4.8 Operating conditions

- Power supply: 36-72 Vdc or multirange (80-360 Vdc, 80-260 Vac).

  Redundant power-supply option and, in front port model, **PoE power-supply option** in eight electrical ports (1 to 4 of block 1 and 1 to 4 of block 2).

  DC operation is protected by diode against polarity inversion. Multirange model is also protected against polarity inversion.

- Consumption: Maximum consumption at 48 Vdc: 40 W.

  Maximum PoE consumption to be distributed for every group of four electrical ports: 12 W.

- Temperature range: From -25ºC to +70ºC

- Relative humidity: Not greater than 95%, in accordance with IEC 721-3-3 class 3K5 (climatogram 3K5).

- Electrical safety: In accordance with EN 60950 standard.

- R.F. emissions: in accordance with EN 55022 standard.

- Dielectric strength: in accordance with EN 60255-5 standard.

- Electromagnetic compatibility.

  - Electrostatic discharge immunity test:
    in accordance with EN 61000-4-2 standard.

  - Radiated, radio-frequency, electromagnetic field immunity test:
    in accordance with EN 61000-4-3 standard.

  - Electrical fast transient/burst immunity test:
    in accordance with EN 61000-4-4 standard.

- Surge immunity test:
  in accordance with EN 61000-4-5 standard.

- Immunity to conducted disturbances, induced by radio-frequency fields:
  in accordance with EN 61000-4-6 standard.

- Power frequency magnetic field immunity test:
  in accordance with EN 61000-4-8 standard.

- Damped oscillatory magnetic field immunity test:
  in accordance with EN 61000-4-10 standard.

- Harmonics and interharmonics including mains signalling at a.c. power port, low frequency immunity tests:
  in accordance with EN 61000-4-13 standard.

- Damped oscillatory wave immunity test:
  in accordance with EN 61000-4-18 standard.

- Voltage dips, short interruptions and voltage variations immunity tests:
  in accordance with EN 61000-4-11 standard.

- Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests:
  in accordance with EN 61000-4-29 standard.

➢ Other standards that are also met.

- Environmental and testing requirements for communications networking devices in electric power substations:
  in accordance with IEEE 1613 standard.

- Communication networks and systems for power utility automation:
  in accordance with IEC 61850-3 standard.

1.5 WARNINGS

1.5.1 Warnings before installing ⚠

!

1. The installation of the SW3-L3 in Electrical Substations or Secondary Substations is generically subject to the fulfilment of all the safety measures and prevention of risks established for this type of work by the electricity company that will use these devices and the Safety standards (EN 50110).

2. In order to install and handle the SW3-L3 the following points must be complied with:
   - Only qualified personnel appointed by the electricity company that owns the installation should carry out the installation and handling of the SW3-L3.
   - The environment in which it is to operate should be suitable for the SW3-L3, fulfilling all the conditions indicated in section 1.4.8.

3. ZIV will not accept responsibility for any injury to persons, installations or third parties, caused by the non-fulfilment of points 1 and 2.

1.5.2 Equipment safety considerations ⚠

!

1. There are two power-supply models:
   - 48 Vdc, isolated.
   - Multirange Vdc/Vac.

   When using the multirange power supply the earth connection must be made before connecting any other power-supply cable.

   In the isolated 48 Vdc model this connection is not compulsory but it is strongly advisable.
2. ZIV will not accept responsibility for any injury to persons or third parties, caused by the non-fulfilment of point 1.

!

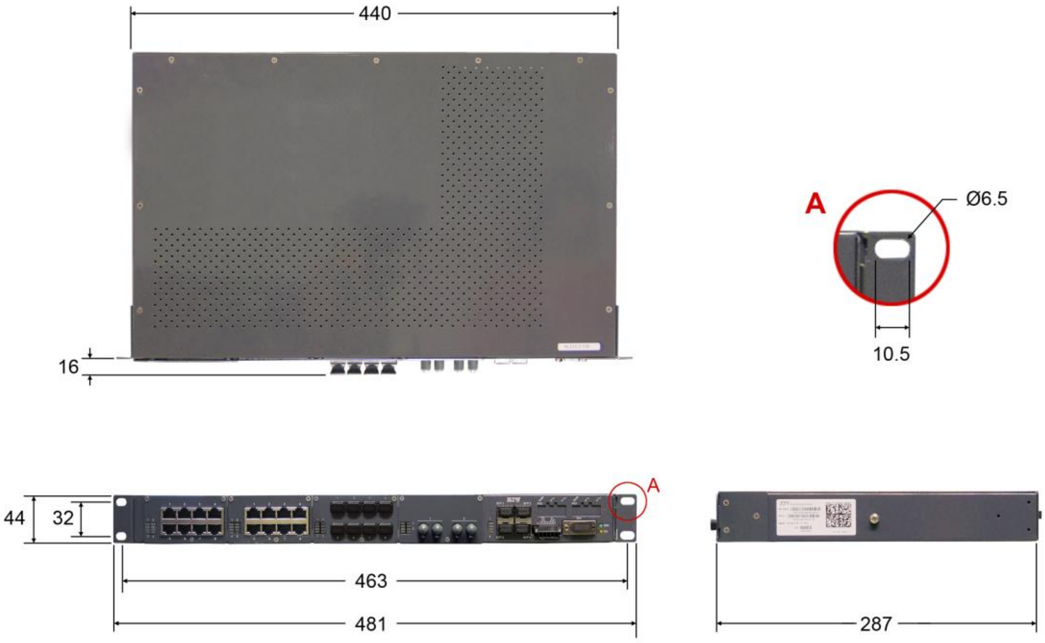
1. The terminal contains components sensitive to static electricity, the following must be observed when handling it:
   - Personnel appointed to carry out the installation and maintenance of the switch SW3-L3 must be free of static electricity. An anti-static wristband and/or heel connected to earth should be worn.
   - The room housing the SW3-L3 must be free of elements that can generate static electricity. If the floor of the room is covered with a carpet, make sure that it is anti-static.
2. ZIV will not accept responsibility for any damage to the equipment caused by the non-fulfilment of point 1.

2 MECHANICAL AND ELECTRICAL CHARACTERISTICS

The diverse elements comprising the Gigabit/Fast Ethernet switch/router type SW3-L3 are supplied in a shelf that is 19" wide and 1 standard unit (s.u.) high, which is prepared for rack mounting.

FIGURE 5 shows the general dimensions in mm of the SW3-L3, as well as the position of the fastening holes.

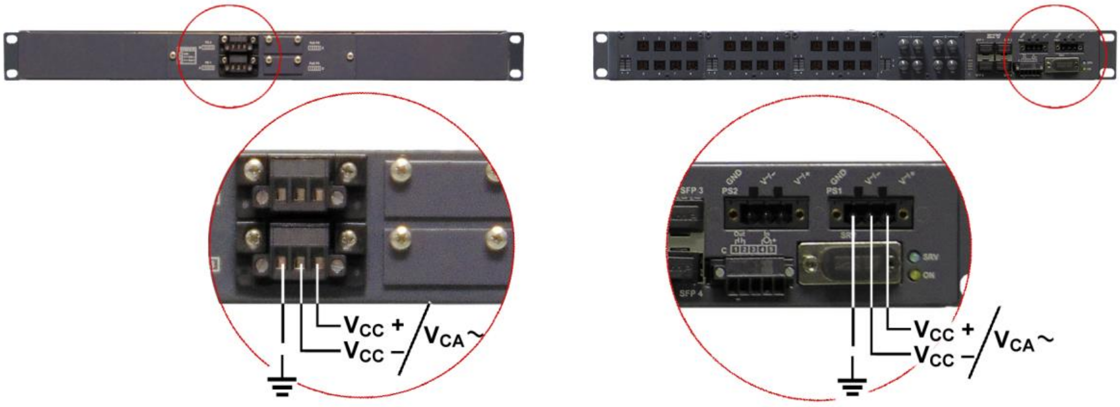
FIGURE 5 General dimensions in mm of the SW3-L3



The SW3-L3 is powered with a nominal voltage of 48 V_{DC} (isolated) or allows DC and AC supply-voltage operation (80-360 Vdc, 80-260 Vac), through the connector shown in FIGURE 6.

The female connector supplied with the equipment is suitable for rigid or flexible conductors of up to 2.5 mm^2.

FIGURE 6 Location of the main power-supply connector (PS 1) and secondary power-supply connector (PS 2)



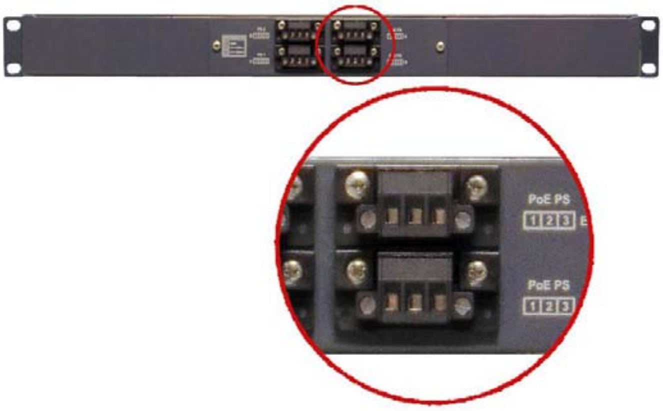
a) Rear view of shelf with front ports

b) Rear view of shelf with rear ports

In the SW3-L3 front port model, eight 10/100Base-Tx ports (1 to 4 of block 1 and 1 to 4 of block 2), admit the **PoE power-supply option**, which is performed through the connector shown in FIGURE 7. The PoE interfaces provide power supply to the client equipment using their own Ethernet cable, for example, IP telephones (IEEE 802.3 af).

> The SW3-L3 may include two power-supply sources: main (PS 1) and alternative (PS 2) and, in front port model, the PoE power supply (PoE PS).

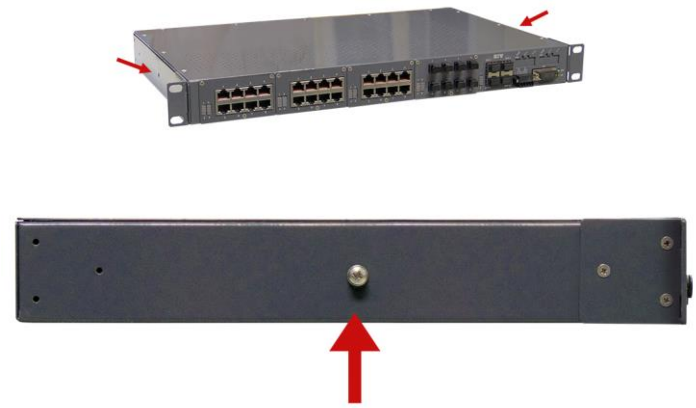
FIGURE 7 Location of the PoE power-supply connector (PoE PS) in shelf with front ports



⚠ An earth connection is available (see FIGURE 8). When using the multirange model, this connection must be made before connecting any other power-supply cable.

In the isolated 48 Vdc model this connection is not compulsory but it is strongly advisable.

FIGURE 8 Location of the earth connection



The SW3-L3 may have 4 Gigabit Ethernet SFP bays and up to 32 ports without PTP (Precision Time Protocol) or up to 24 IEEE 1588 (Precision Time Protocol) ports.

The SW3-L3 has a 4-block mechanical structure for the installation of the ports. See in section 1.4.2, *Equipment interfaces*, the types of blocks available and their requirements.

Sections 2.1 to 2.8 give the electrical characteristics of the connectors and their use.

FIGURE 9 shows an example of a front view of the SW3-L3 with 4 Gigabit Ethernet SFP bays and with 26 **front** ports without PTP, the first 16 in 10/100Base-Tx (RJ-45) configuration, the following 8 in 100Base-Fx (multimode, MT-RJ) configuration and the last two in 100Base-Fx (multimode, ST) configuration.

FIGURE 9 Front view of the SW3-L3 shelf with 26 **front** ports without PTP and 4 SFP bays

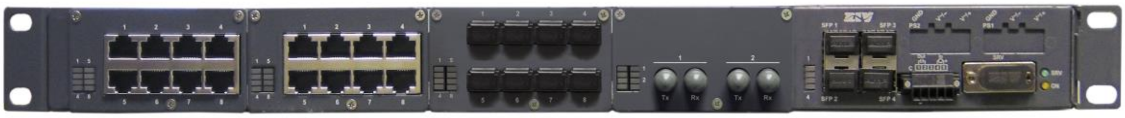


FIGURE 10 shows an example of a rear view of the SW3-L3 with 4 Gigabit Ethernet SFP bays and with 24 **rear** ports without PTP, the first 16 in 100Base-Fx (multimode, MT-RJ) configuration and the last 8 in 100Base-Fx (multimode, ST) configuration.

FIGURE 10 Rear view of the SW3-L3 shelf with 24 **rear** ports without PTP and 4 SFP bays

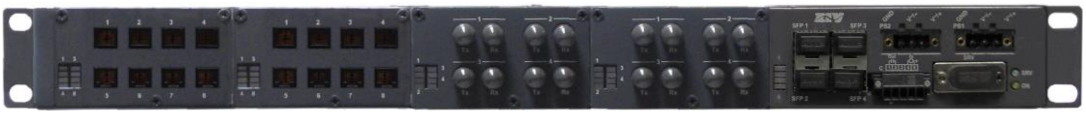
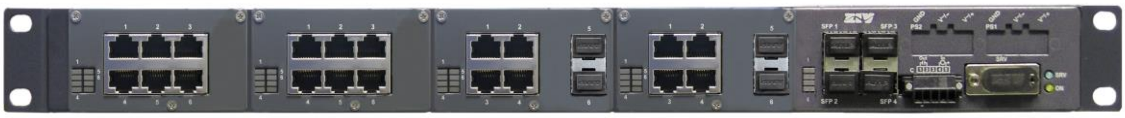


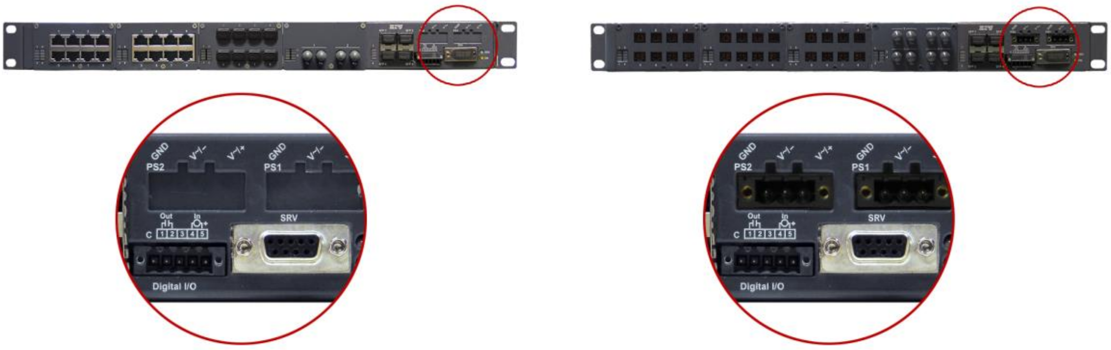
FIGURE 11 shows an example of a front view of the SW3-L3 with 4 Gigabit Ethernet SFP bays and 24 ***front*** IEEE 1588 (Precision Time Protocol) ports, the first 12 in 10/100Base-Tx (RJ-45) configuration, and the last 12 in 10/100Base-Tx (RJ-45) configuration and Gigabit Ethernet SFP.

FIGURE 11 **Front** view of the SW3-L3 shelf with 24 IEEE 1588 (Precision Time Protocol) ports and 4 SFP bays



As shown in FIGURE 12, there is a maintenance connector, identified as SRV, at the right of the SW3-L3, for accessing the equipment through a console, and an I/O connector.

FIGURE 12 Location of the SRV maintenance connector and the I/O connector



a) Front view of shelf with front ports

b) Rear view of shelf with rear ports

Section 2.8 gives the electrical characteristics of the I/O connector.

Section 2.7, *SRV port*, gives the electrical characteristics of the maintenance connector and its use. The connector has a protective cap.

2.1 10/100BASE-TX (RJ-45) PORTS

The cable used to connect a 10/100Base-Tx port should be an unshielded twisted 4 pair category five cable (UTP-5) with 8-pin RJ-45 connectors. The cable length should not be more than 100 m.

The UTP-5 cable is made up of eight copper wires that form the four twisted pairs, covered in different coloured insulating material. FIGURE 13 shows the colour of the wires that make up each one of the pairs, according to ANSI/TIA/EIA-568-A standard.

FIGURE 13 Unshielded twisted pair category five cable (UTP-5) with RJ-45 connector according to ANSI/TIA/EIA-568-A standard

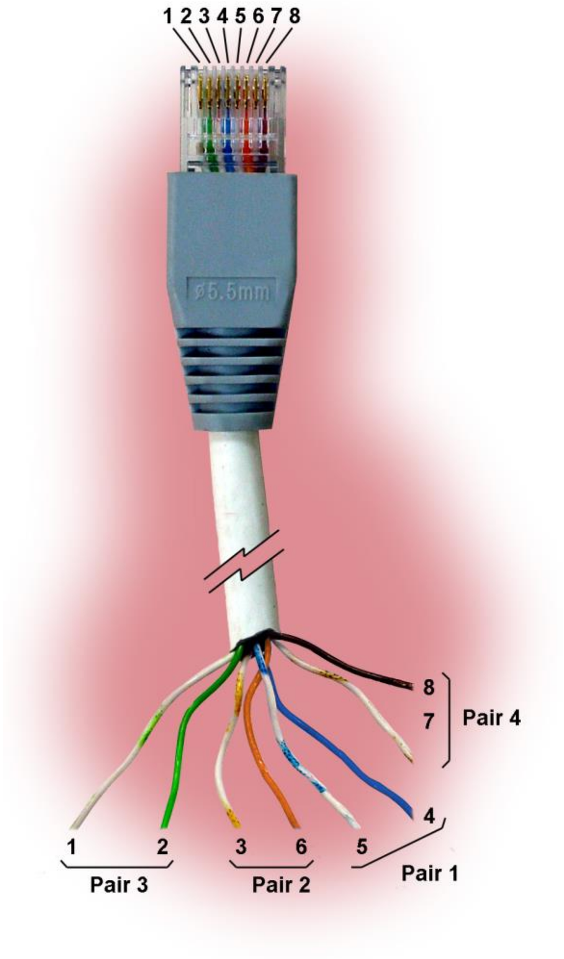
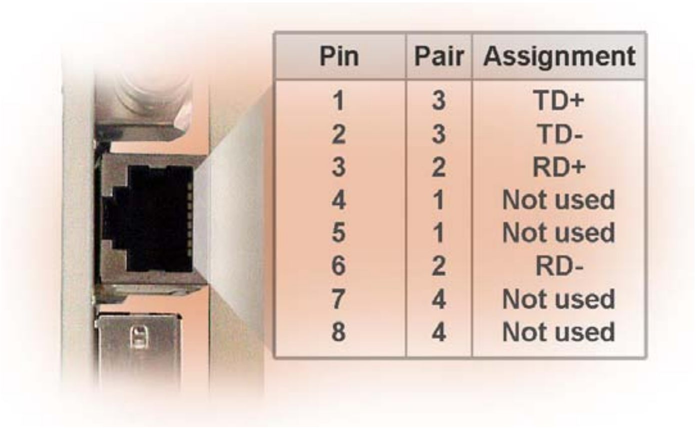


FIGURE 14 shows the use of each one of the pins of the RJ-45 connector, as well as the pair it belongs to according to ANSI/TIA/EIA-568-A standard, in the 10/100Base-Tx LAN interface.

FIGURE 14 Signals of the RJ-45 connector in the 10/100Base-Tx LAN interface

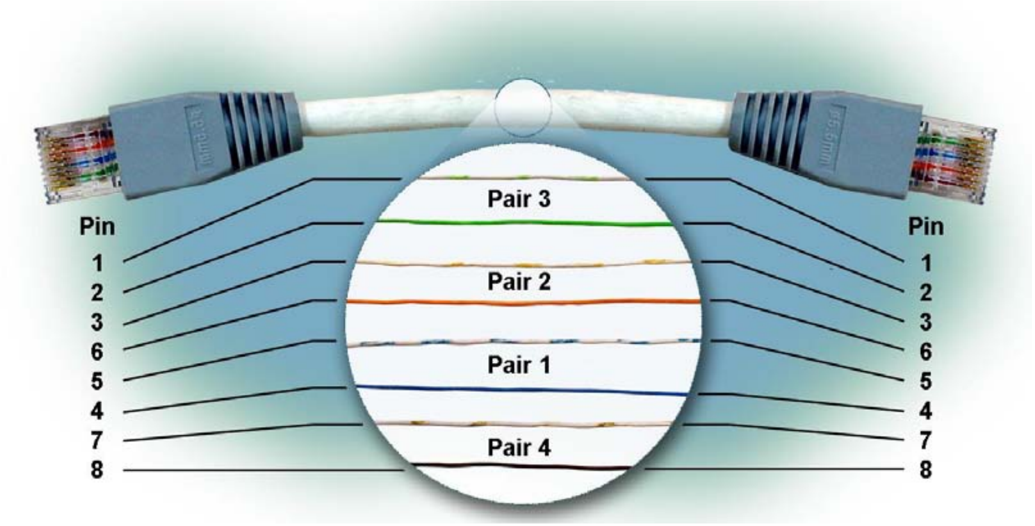


Pin	Pair	Assignment
1	3	TD+
2	3	TD-
3	2	RD+
4	1	Not used
5	1	Not used
6	2	RD-
7	4	Not used
8	4	Not used

In the eight 10/100Base-Tx ports that admit the PoE power-supply option (1 to 4 of block 1 and 1 to 4 of block 2), pair 1 is used for the V_{DC}PoE+ connection, and pair 4 is used for the V_{DC}PoE- connection.

Straight-through cables must be used, see FIGURE 15, where the 4 pairs correspond at both ends of the cable.

FIGURE 15 Straight-through cable



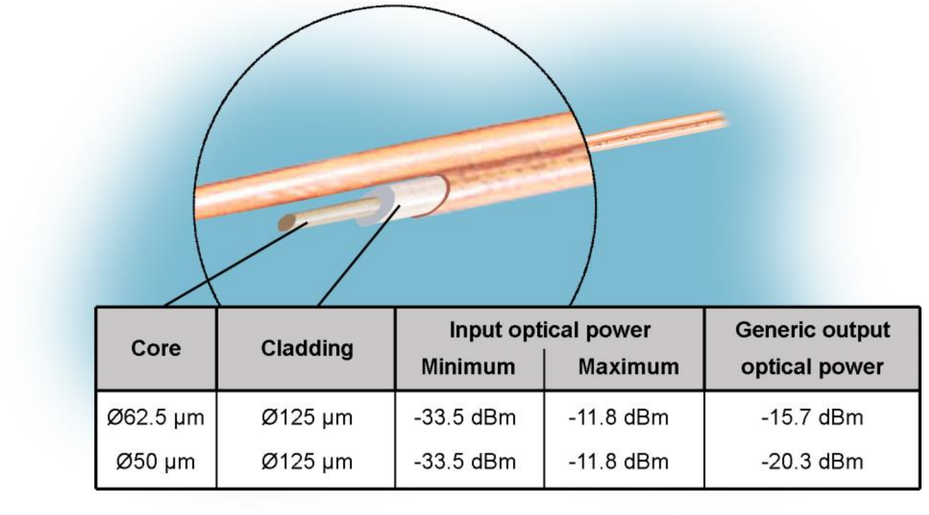
2.2 100BASE-FX (MULTIMODE, MT-RJ) PORTS

In each 100Base-Fx port of this type, it should have an MT-RJ type connector. The cable required to make the connection should be a fiber optic cable made up of two multimode optical fibers, one to transmit data and the other to receive it. Each of the fibers should be 125 µm in diameter. The core and the cladding of the fiber are included in this diameter, as can be seen in FIGURE 16. The core can be 50 µm or 62.5 µm in diameter. The wavelength used should be 1300 nm (multimode). The cable length should not be more than 2 km.

FIGURE 16 shows the most important input and output optical power characteristics according to the type of multimode fiber used.

All the MT-RJ type connectors have a protective cap.

FIGURE 16 Multimode optical fiber



Core	Cladding	Input optical power		Generic output optical power
		Minimum	Maximum	
Ø62.5 µm	Ø125 µm	-33.5 dBm	-11.8 dBm	-15.7 dBm
Ø50 µm	Ø125 µm	-33.5 dBm	-11.8 dBm	-20.3 dBm

2.3 100BASE-FX (MULTIMODE, ST or SC) PORTS

In each 100Base-Fx port of this type, it should have a ST or SC type connector. The cable required to make the connection should be a fiber optic cable made up of two multimode optical fibers, one to transmit data and the other to receive it. Each of the fibers should be 125 µm in diameter. The core and the cladding of the fiber are included in this diameter, as can be seen in FIGURE 16. The core can be 50 µm or 62.5 µm in diameter. The wavelength used should be 1300 nm (multimode). The cable length should not be more than 2 km.

FIGURE 16 shows the most important input and output optical power characteristics according to the type of multimode fiber used.

All the ST or SC type connectors have a protective cap.

2.4 100BASE-FX (MULTIMODE, LC) PORTS

In each 100Base-Fx port of this type, it should have a LC type connector. The cable required to make the connection should be a fiber optic cable made up of two multimode optical fibers, one to transmit data and the other to receive it. Each of the fibers should be 125 µm in diameter. The core and the cladding of the fiber are included in this diameter, as can be seen in FIGURE 16. The core can be 50 µm or 62.5 µm in diameter. The wavelength used should be 1300 nm (multimode). The cable length should not be more than 2 km.

FIGURE 16 shows the most important input and output optical power characteristics according to the type of multimode fiber used.

All the LC type connectors have a protective cap.

2.5 100BASE-LX (SINGLEMODE, LC) PORTS

In each 100Base-Lx port of this type, it should have a LC singlemode type connector. The cable required to make the connection should be a fiber optic cable made up of two singlemode optical fibers, one to transmit data and the other to receive it. Each of the fibers should be 125 µm in diameter. The core and the cladding of the fiber are included in this diameter. The core is 9 µm in diameter. The wavelength used should be 1300 nm (singlemode). The cable length should not be more than 10 km.

The most important input and output optical power characteristics are:

Input optical power		Output optical power	
Minimum	**Maximum**	**Minimum**	**Maximum**
-25 dBm	-8 dBm	-15 dBm	-8 dBm

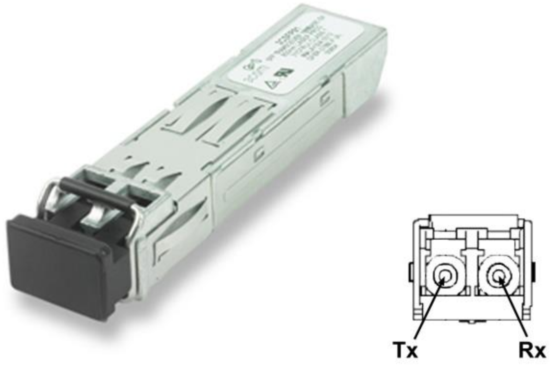
All the LC singlemode type connectors have a protective cap.

2.6 SFP PORTS

The bays available in the front plate of the equipment admit the installation of SFP (Small Form Factor Pluggable) modules, which provide optic Gigabit Ethernet interfaces to the switch; the characteristics of the fiber optic to be used, as well as the type of connector, will depend on the SFP model used. See the available modules in section 1.4.3, *Accessories*.

Bays have a protective cap.

FIGURE 17 SFP modules



Inserting procedure of an SFP module

The inserting procedure of an SFP module is the following:

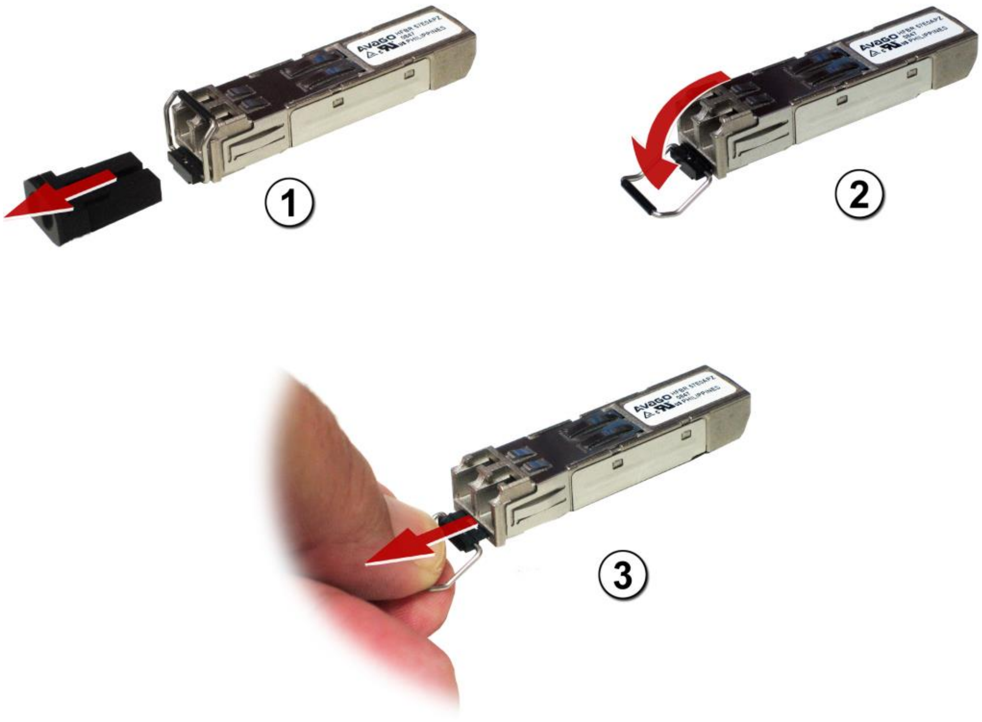
1. Remove the protective packaging of the SFP module.
2. Check that the SFP module is the correct one for your network configuration.
3. Hold the module between your thumb and forefinger.
4. Insert the module into the corresponding SFP slot on the front panel of the equipment.
5. Remove the protective caps from the optical ends of the module.
6. Insert the fibers, in the optical ends of the module, keeping in mind the TX and RX data transmission directions (see FIGURE 17).

Removing procedure of an SFP module

The removing procedure of an SFP module is the following:

1. Disconnect the optical fiber from the connector of the SFP module.
2. Pull down the transceiver security lever.
3. Whilst the security lever down, remove the port from the module (if the SFP does not slide out of the slot easily, make a slight oscillating motion from one side to another, while firmly pulling the SFP outward).

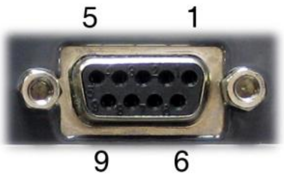
FIGURE 18 Removing an SFP transceiver



2.7 SRV PORT

The electrical characteristics of the maintenance connector and its use are indicated below. The connector has a protective cap.

FIGURE 19 Location of the SRV maintenance connector



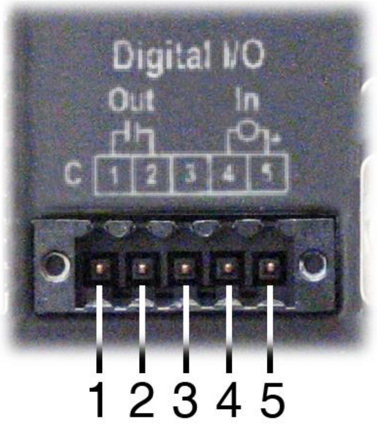
Pin	RS-232
2	RD
3	TD
5	GND

	SRV CONNECTOR (DCE mode)
Interface type	ITU-T V.24/V.28 (EIA RS-232)
Connector	DB9 female
Data	Asynchronous
Speed	115200 bit/s
Protocol	CLI (system console)

2.8 I/O CONNECTOR

The I/O connector input and output are galvanically isolated, and can be managed via SNMP. The pin-out and the main physical characteristics of the connector are indicated below.

FIGURE 20 Location of the I/O connector



Pin	Use
1	Output -
2	Output +
3	Not connected
4	Input -
5	Input +

INPUT (pin 4 & 5)		OUTPUT (pin 1 & 2)	
Input Inactive	In. Voltage < 8 Vdc (between pins 4 & 5)	**Output Active**	Impedance <26 Ω (between pins 1 & 2)
Input Active	In. Voltage > 10 Vdc (between pins 4 & 5)	**Output Inactive**	Impedance> 500 MΩ (between pins 1 & 2)
Max. voltage	250 Vdc Protected against overvoltages >270 Vdc	**Max. voltage**	250 Vdc Protected against overvoltages >270 Vdc No Vac can be applied
Max. DC current draw	12 mA	**Max. DC current**	150 mA
Polarity	Pin 4 is the reference for INPUT- and pin 5 for INPUT+ Protected against wrong polarities	**Polarity**	Pin 1 connected to OUTPUT-- and pin 2 to OUTPUT+
Switching time ON/OFF	~1 ms	**Switching time ON/OFF**	2 ms

3 LED SIGNALLING

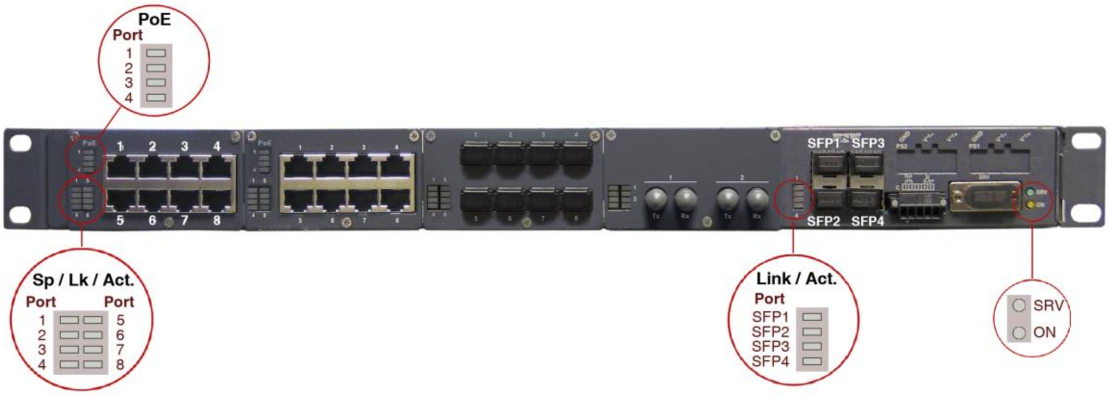
The SW3-L3 has two basic LEDs (SRV and ON) and several specific LEDs associated with SFP modules and Fast Ethernet or IEEE 1588 (Precision Time Protocol) ports.

The location and identification of the LEDs are indicated in the following sections.

3.1 SW3-L3 WITH FRONT PORTS WITHOUT PTP

FIGURE 21 shows a front view of the SW3-L3 with front ports without PTP, showing the detail of the different LEDs. They are described below.

FIGURE 21 Detail of the different LEDs in the SW3-L3 with **front** ports without PTP



Basic LEDs

Srv LED

Amber. It flashes when there is emission or reception activity by the SRV serial service interface.

On LED

Red. It is permanently lit when the equipment is powered with an external power-supply voltage.

LEDs associated with PoE (ports 1 to 4 of block 1 and ports 1 to 4 of block 2)

PoE LED

Two-coloured. There is a LED per interface associated with each PoE port. When there is no connected equipment, the four amber LEDs are lit permanently in blocks 1 and 2, as long as there is PoE power supply (PoE PS connector). When IP equipment using PoE power supply (IEEE 802.3af) is connected, the corresponding green LED will be lit permanently, while the LEDs for the ports that do not consume PoE power supply will remain off.

LEDs associated with SFP ports

Link/Act. LED

Two-coloured. There is one LED per SFP interface. It flashes in the case of emission or reception activity in the interface. It lights up in green at 1 Gbit/s and in amber at 100 Mbit/s.

LEDs associated with 10/100Base-Tx (RJ-45) ports

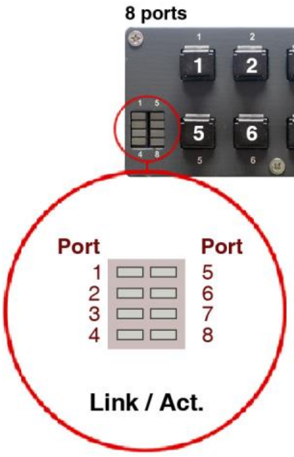
Sp/Lk/Act LED

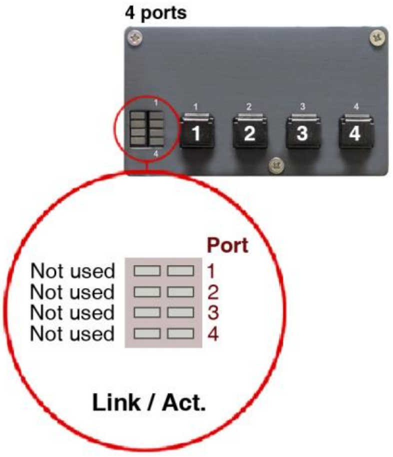
Two-coloured. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface. It lights up in green at 100 Mbit/s and in amber at 10 Mbit/s.

LEDs associated with 100Base-Fx (multimode, MT-RJ) ports

Link/Act. LED

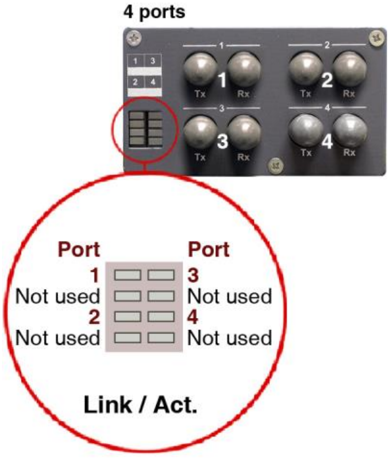
Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.

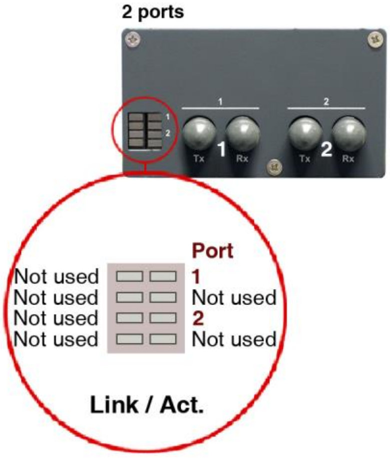




LEDs associated with 100Base-Fx (multimode, ST) ports

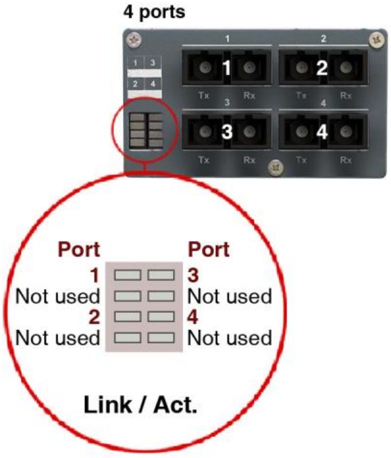
Link/Act. LED	Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.

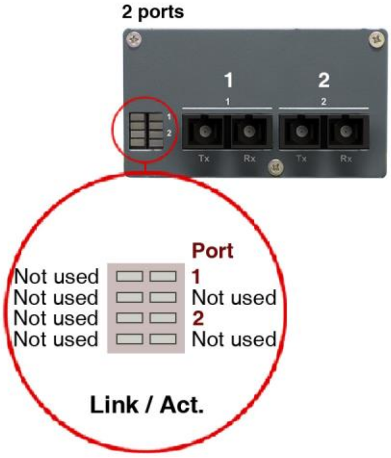




LEDs associated with 100Base-Fx (multimode, SC) ports

Link/Act. LED	Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.

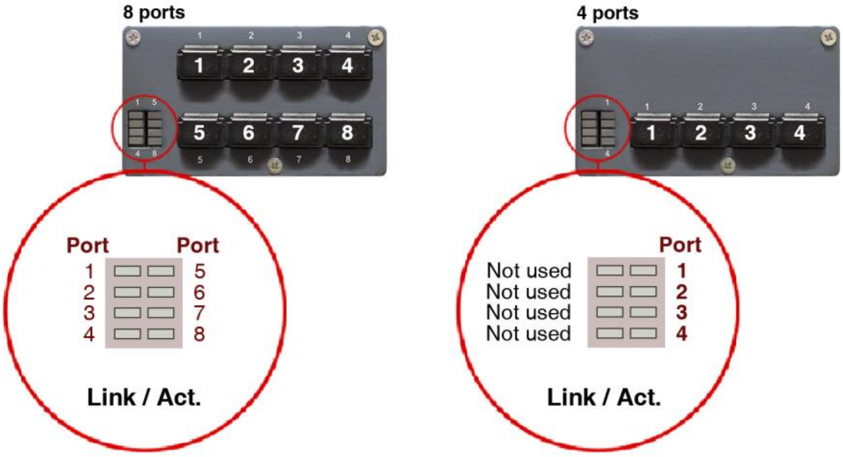




LEDs associated with 100Base-Fx (multimode, LC) or 100Base-Lx (singlemode, LC) ports

Link/Act. LED

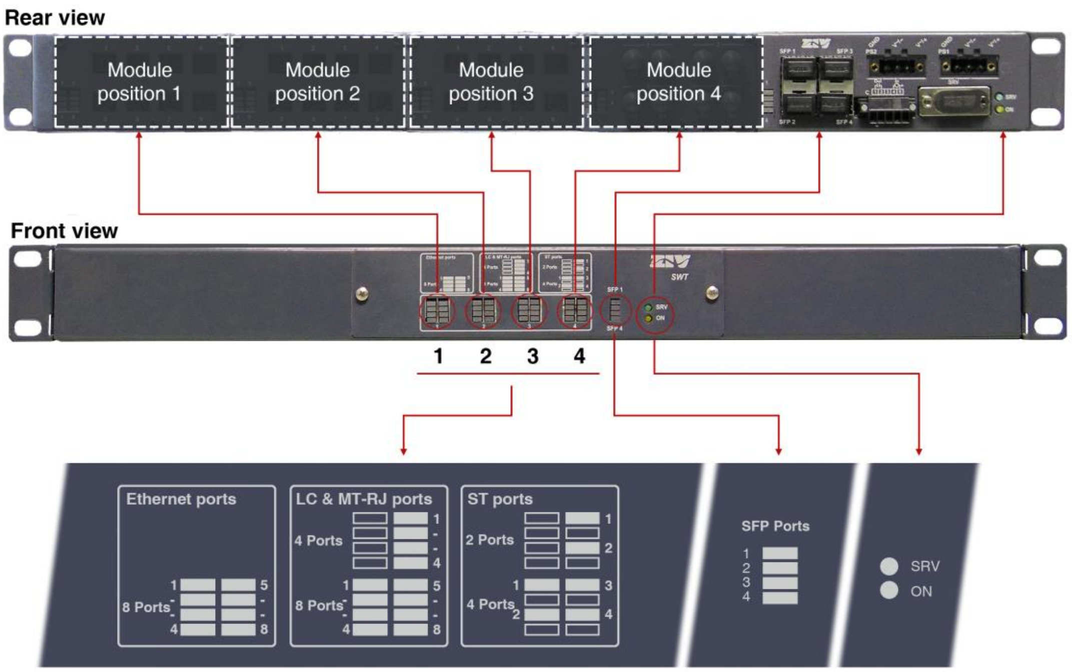
Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



3.2 SW3-L3 WITH REAR PORTS WITHOUT PTP

FIGURE 22 shows a front view of the SW3-L3 with rear ports without PTP, showing the detail of the different LEDs. They are described below.

FIGURE 22 Detail of the different LEDs in the SW3-L3 with **rear** ports without PTP



Basic LEDs

SRV LED — Amber. It flashes when there is emission or reception activity by the SRV serial service interface.

ON LED — Red. It is permanently lit when the equipment is powered with an external power-supply voltage.

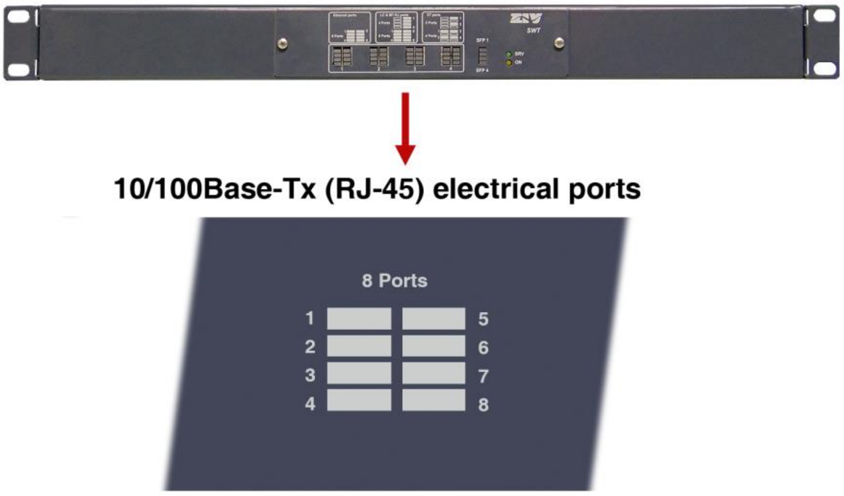
LEDs associated with SFP ports

SFP (1 to 4) LED — Two-coloured. There is one LED per SFP interface. It flashes in the case of emission or reception activity in the interface. It lights up in green at 1 Gbit/s and in amber at 100 Mbit/s.

LEDs associated with 10/100Base-Tx (RJ-45) ports

Ethernet ports LEDs

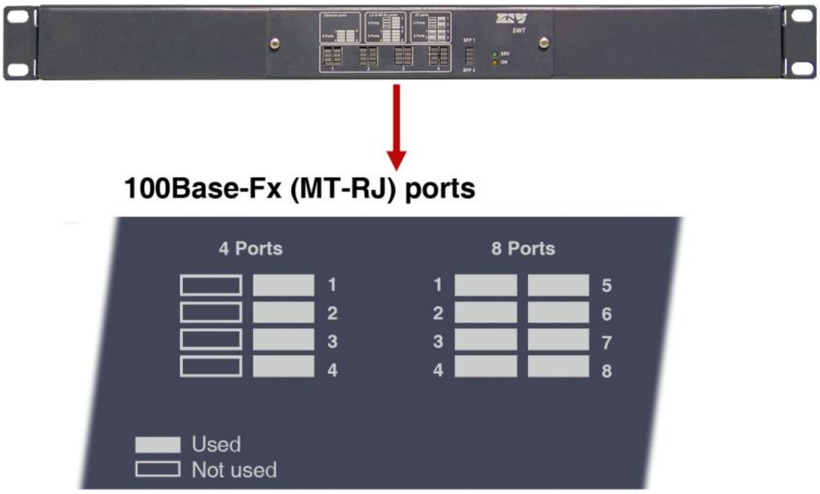
Two-coloured. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface. It lights up in green at 100 Mbit/s and in amber at 10 Mbit/s.



LEDs associated with 100Base-Fx (multimode, MT-RJ) ports

MT-RJ ports LEDs

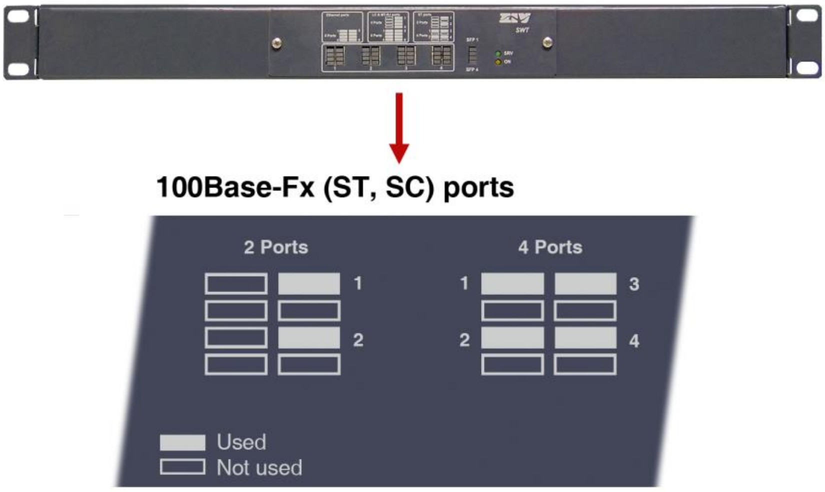
Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



LEDs associated with 100Base-Fx (multimode, ST or SC) ports

ST or SC ports LEDs

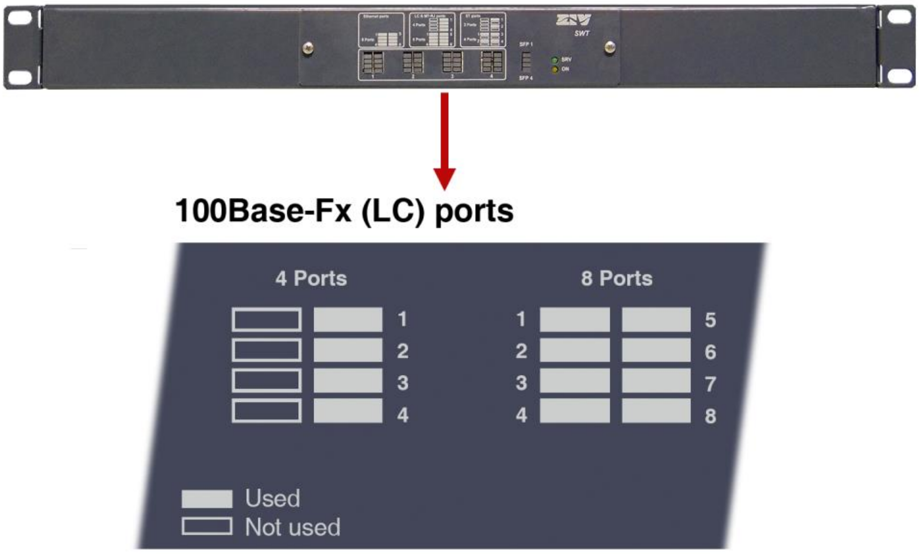
Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



LEDs associated with 100Base-Fx (multimode, LC) or 100Base-Lx (singlemode, LC) ports

LC ports LEDs

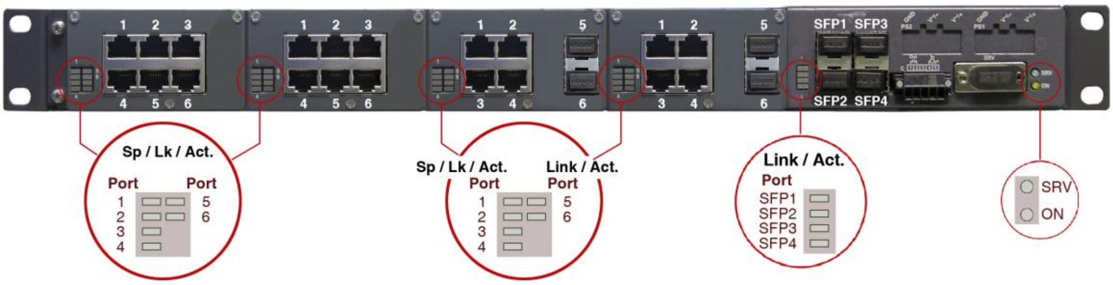
Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



3.3 SW3-L3 WITH FRONT PTP PORTS

FIGURE 23 shows a front view of the SW3-L3 with front PTP ports, showing the detail of the different LEDs. They are described below.

FIGURE 23 Detail of the different LEDs in the SW3-L3 with **front** PTP ports



Basic LEDs

Srv LED Amber. It flashes when there is emission or reception activity by the SRV serial service interface.

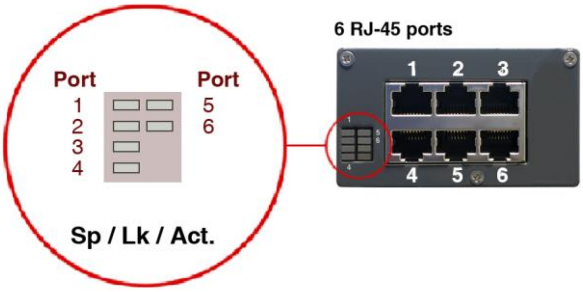
On LED Red. It is permanently lit when the equipment is powered with an external power-supply voltage.

LEDs associated with SFP1 to SFP4 ports

Link/Act. LED Two-coloured. There is one LED per SFP interface. It flashes in the case of emission or reception activity in the interface. It lights up in green at 1 Gbit/s and in amber at 100 Mbit/s.

LEDs associated with the block of six 10/100Base-Tx (RJ-45) ports

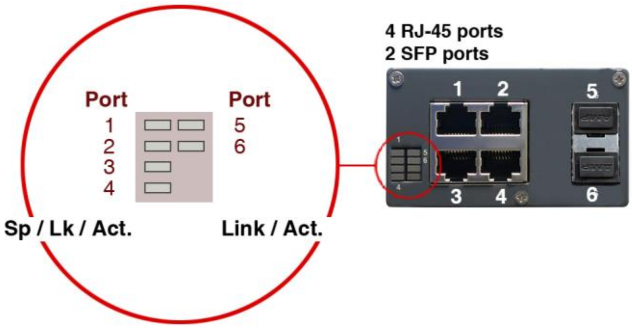
Sp/Lk/Act. LED Two-coloured. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface. It lights up in green at 100 Mbit/s and in amber at 10 Mbit/s.



LEDs associated with the block of four 10/100Base-Tx (RJ-45) ports and 2 Gigabit Ethernet SFP bays

Sp/Lk/Act. LED — Two-coloured. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface. It lights up in green at 100 Mbit/s and in amber at 10 Mbit/s.

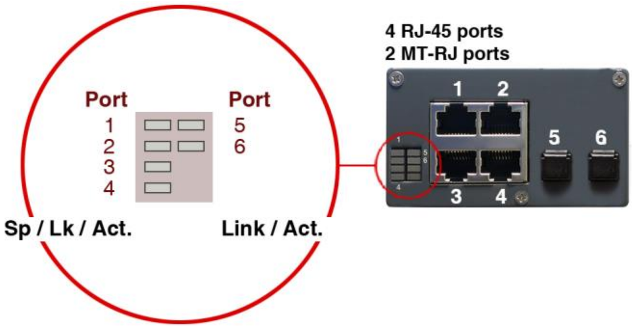
Link/Act. LED — Two-coloured. There is one LED per SFP interface. It flashes in the case of emission or reception activity in the interface. It lights up in green at 1 Gbit/s and in amber at 100 Mbit/s.



LEDs associated with the block of four 10/100Base-Tx (RJ-45) ports and two 100Base-Fx (multimode, MT-RJ) ports

Sp/Lk/Act. LED — Two-coloured. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface. It lights up in green at 100 Mbit/s and in amber at 10 Mbit/s.

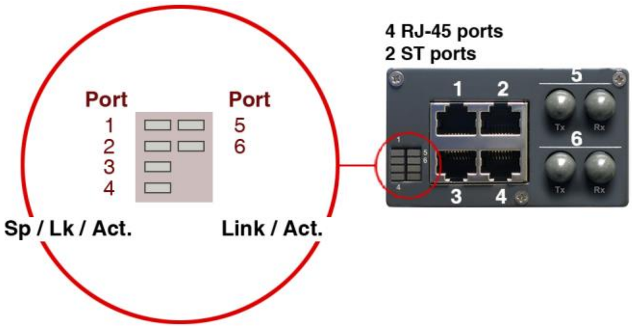
Link/Act. LED — Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



LEDs associated with the block of four 10/100Base-Tx (RJ-45) ports and two 100Base-Fx (multimode, ST) ports

Sp/Lk/Act. LED — Two-coloured. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface. It lights up in green at 100 Mbit/s and in amber at 10 Mbit/s.

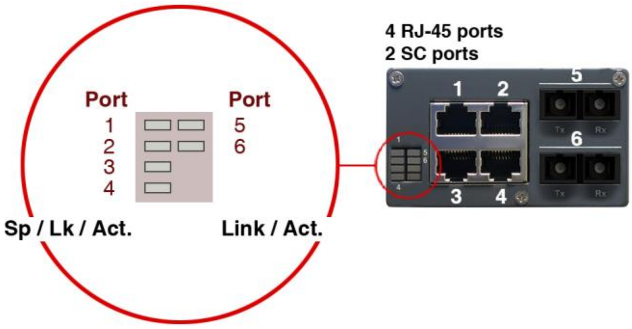
Link/Act. LED — Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



LEDs associated with the block of four 10/100Base-Tx (RJ-45) ports and two 100Base-Fx (multimode, SC) ports

Sp/Lk/Act. LED — Two-coloured. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface. It lights up in green at 100 Mbit/s and in amber at 10 Mbit/s.

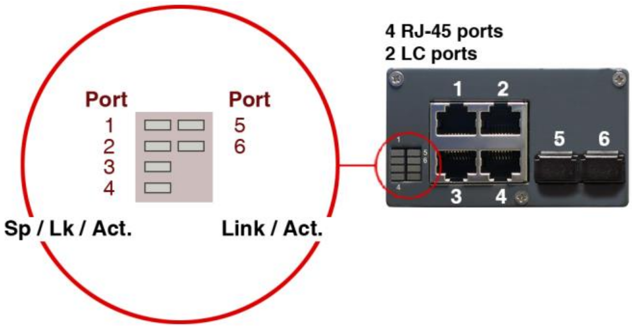
Link/Act. LED — Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



LEDs associated with the block of four 10/100Base-Tx (RJ-45) ports and two 100Base-Fx (multimode, LC) or 100Base-Lx (singlemode, LC) ports

Sp/Lk/Act. LED — Two-coloured. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface. It lights up in green at 100 Mbit/s and in amber at 10 Mbit/s.

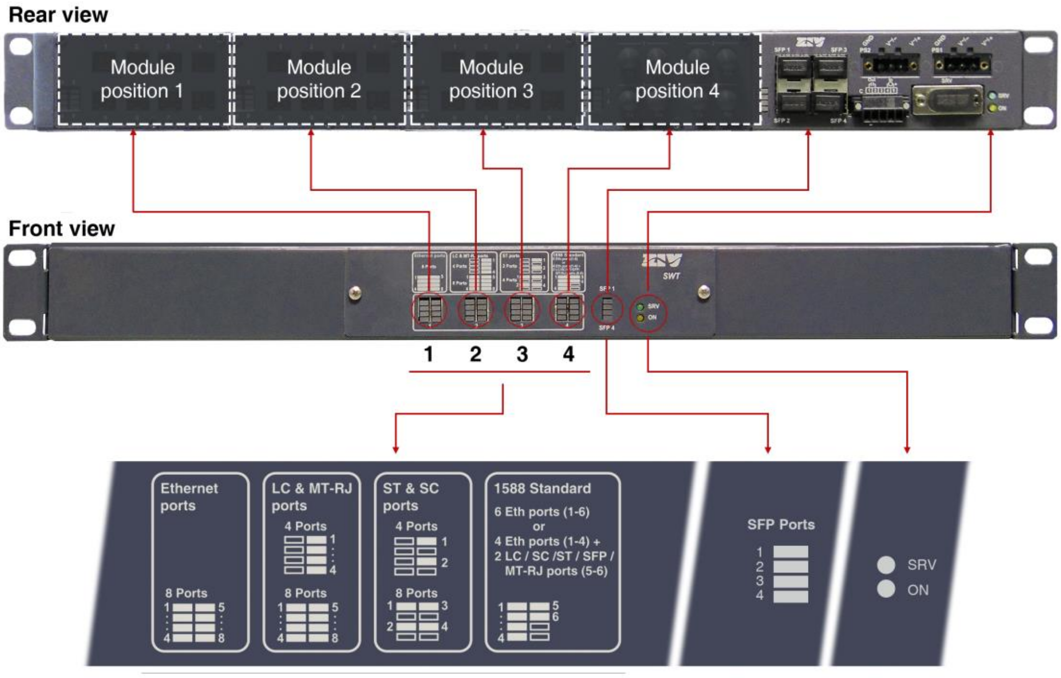
Link/Act. LED — Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



3.4 SW3-L3 WITH REAR PTP PORTS

FIGURE 24 shows a front view of the SW3-L3 with rear PTP ports, showing the detail of the different LEDs. They are described below.

FIGURE 24 Detail of the different LEDs in the SW3-L3 with **rear** PTP ports



Basic LEDs

SRV LED Amber. It flashes when there is emission or reception activity by the SRV serial service interface.

ON LED Red. It is permanently lit when the equipment is powered with an external power-supply voltage.

LEDs associated with SFP ports

SFP (1 to 4) LED Two-coloured. There is one LED per SFP interface. It flashes in the case of emission or reception activity in the interface. It lights up in green at 1 Gbit/s and in amber at 100 Mbit/s.

LEDs associated with 10/100Base-Tx (RJ-45) ports

Ethernet ports LEDs — Two-coloured. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface. It lights up in green at 100 Mbit/s and in amber at 10 Mbit/s.

LEDs associated with 100Base-Fx (multimode, MT-RJ) ports

MT-RJ ports LEDs — Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.

LEDs associated with 100Base-Fx (multimode, ST or SC) ports

ST or SC ports LEDs — Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.

LEDs associated with 100Base-Fx (multimode, LC) or 100Base-Lx (singlemode, LC) ports

LC ports LEDs — Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.

4 ACCESS TO THE EQUIPMENT

The SW3-L3 can be managed locally and remotely, through a console or through a built-in web server. The server operates with the HTTP and/or HTTPS protocol.

4.1 CONSOLE

The equipment provides a user console application called *CLI* (see *Appendix B*), accessible through the SRV connector, a standard DB9 female connector in DCE mode that operates at 115200 bit/s, with 8-bit characters, without parity and with a stop bit.

> The system makes a distinction between upper and lower case characters.

Depending on the user identity, the user console provides full access to all the equipment configuration data.

The console has a small help section about the available commands that is obtained by executing the ***help*** command.

The data are grouped virtually into directories and subdirectories. To browse through the directories the ***cd*** **(*change directory*)** command is used. The value of an individual data item or a group of data is obtained in response to a ***get*** command, indicating the specific data item or giving the value of all the data located in the current directories and subdirectories. To select a new value, it is necessary to execute the ***set*** command, indicating the parameter to be changed and then the desired value; if the value to be configured is not provided, the system will explicitly request it.

The data stored in table form, identified by the inclusion in the variable name of the symbol [], have specific commands for adding and removing rows, which are ***add*** and ***remove*** respectively. To query or establish the value of the data in one row, the row identifier must be included between square brackets in the ***get*** or ***set*** command.

Changes made with the ***set*** command are not operative merely because they have been executed. Effective, immediate use of the changes made is achieved by executing the ***Apply*** command. On the contrary, the ***Save*** commands entails storing the changes made permanently, without requiring their immediate use, but applied in the case of an initialisation.

In this way, the changes are implemented as an operating procedure through the ***Apply*** command, and after checking that the behaviour is correct, it is saved using the ***Save*** command. Consequently in the case of obtaining undesirable results, it is always possible to eliminate the ***Save*** command and reboot the equipment to recover the previous status, even in the case that the changed activated lead to the user not being able to obtain access.

Access can also be obtained to the console remotely through SSH connection and Telnet.

4.2 HTTP SERVER

The HTTP server included provides access to the HTML pages giving access to all the configuration data, see FIGURE 25.

The procedures for the effective configuration of the parameters are identical, that is to say, it is necessary to execute the ***Apply*** command and/or the ***Save*** command, as indicated in the section on using the console, but before executing these commands, the system must be informed that the data have been changed through the ***Send*** command (the button is present in all the HTML pages).

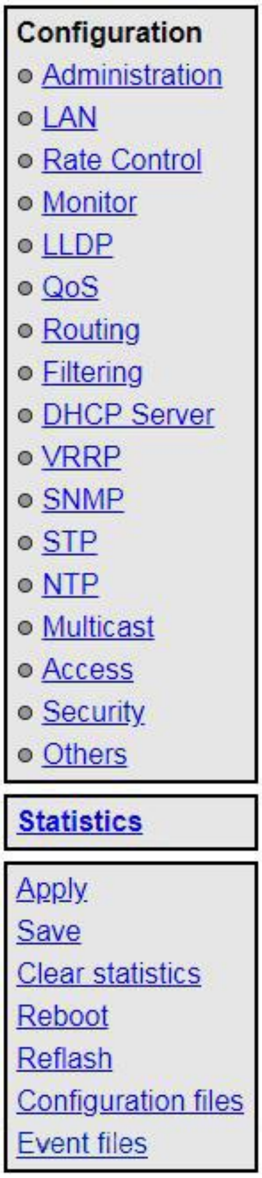
The ***Apply*** and ***Save*** commands are at the bottom of the tree menu and are only visible when the user profile has administration rights.

For information about the ***Reboot, Reflash, Configuration files*** and ***Event files*** commands see sections 5.20, 5.21, 5.22 and 5.23, respectively.

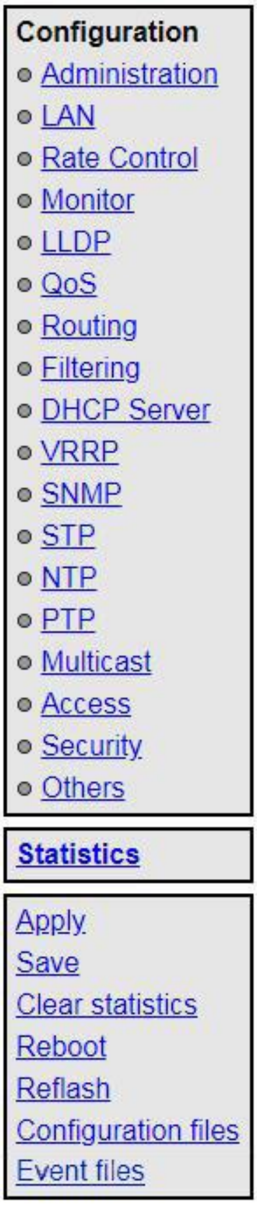
The ***Apply***, ***Save*** and ***Reboot*** commands request confirmation of the operation from the user before it is actually executed.

In the HTML pages the commands for adding and removing elements from the tabled data are explicitly shown as buttons labelled *Add* and *Delete*, located on each of the objects that use them.

FIGURE 25 HTML page tree menu



SW3-L3 version with standard ports



SW3-L3 version with PTP ports

The factory IP address of the equipment is 192.168.0.1, meaning it is possible to access the HTTP server to configure it from the very start (see chapter 5).

It should be borne in mind that if the IP address is changed, the IP address of the client equipment must also be changed accordingly.

5 CONFIGURATION AND MANAGEMENT

Configuration and management of the SW3-L3 is performed through the console and through access to the equipment HTML pages.

All the parameters controlling the equipment operation are described below in detail, using the real HTML pages as an auxiliary graph sample.

Whenever changes are made, regardless of the fact that they are made through the console or the HTTP server, the equipment must be informed what is to be done with them. There are two options:

- the first is to execute the ***Apply*** command, which entails the immediate use of the changes made.

- the second is to execute the ***Save*** command, which means that the changes will be operative once the equipment is rebooted.

If accessing through the HTTP server, after making the changes and before running ***Apply*** or ***Save***, the ***Send*** button must be pushed to allow the equipment to obtain the new desired values.

If running the ***Apply*** command, if the changes are required to be permanent, the ***Save*** command must also be run.

The only exceptions are changes affecting the SNMP configuration. Changes made to the SNMP agent configuration will **only** be active after **RESETTING** the equipment. The ***Apply*** command is not sufficient, and so the changes must previously be saved using the ***Save*** command before requesting the re-initialisation.

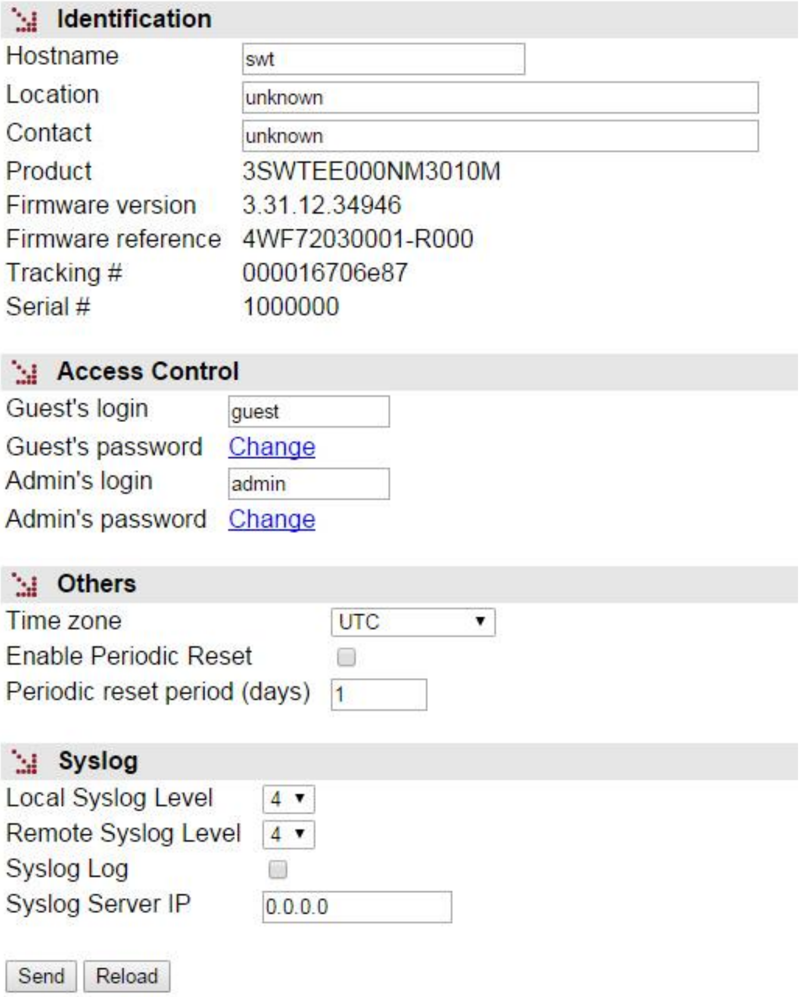
5.1 GENERAL PARAMETERS

The general parameters are grouped on the first page, see FIGURE 26, which is shown when the SW3-L3 validates the user identity.

In addition to the configuration parameters, which will be described in the following sections, as shown in the figure, the system provides information about the equipment software, that is to say, version being executed, and equipment hardware, that is to say, serial and tracking number.

> The tree menu is permanently located on all the pages used by the HTTP server.

FIGURE 26 Main HTML page



Identification

Hostname	swt
Location	unknown
Contact	unknown
Product	3SWTEE000NM3010M
Firmware version	3.31.12.34946
Firmware reference	4WF72030001-R000
Tracking #	000016706e87
Serial #	1000000

Access Control

Guest's login	guest
Guest's password	Change
Admin's login	admin
Admin's password	Change

Others

Time zone	UTC ▾
Enable Periodic Reset	☐
Periodic reset period (days)	1

Syslog

Local Syslog Level	4 ▾
Remote Syslog Level	4 ▾
Syslog Log	☐
Syslog Server IP	0.0.0.0

5.1.1 Equipment identification

The identification zone has three parameters; the equipment name (***hostname***), its location (***location***) and the contact data of the responsible person or company (***contact***). At least one string of text is required, with at least one character.

The ***hostname*** is used automatically as a prompt value on the console.

The identification parameters coincide with those assigned with the same name in the SNMP data.

5.1.2 Access control

Access control allows the user logins and associated passwords to be determined for the two pre-set profiles: **guest** and **admin**.

The guest profile can only access query operations. On the contrary, the admin. profile has access to all the system configuration data.

As summarised in TABLE 1, the default values of these parameters are ***guest*** and ***admin*** as the logins, with ***passwd01*** and ***passwd02*** being the respective passwords.

> It should be borne in mind that the system makes a distinction between upper and lower case characters.

TABLE 1 System default access codes

	Login	**Password**
Guest profile	guest	passwd01
Admin. profile	admin	passwd02

> It is highly recommended to change at least the password of the admin. profile when executing the first configuration in each equipment.
>
> It is advisable to store the new password in some type of register as, should the new password be forgotten, it is not possible to access the web server.

5.1.3 Others

This section deals with three parameters. The first of them selects the hour zone in relation to UTC.

The second parameter, ***Enable periodic reset***, allows users to indicate whether they want to reboot the equipment automatically every so often. This is selected in days through the last parameter, ***Periodic reset period***.

5.1.4 Syslog

This section deals with four parameters. The first of them, ***Local Syslog Level***, selects the maximum level of severity which is stored in the local Log. Valid values are 1 to 8. The default value is 4.

The levels involve storing all information tagged with a level equal to or lower than the level specified.

The levels are:

Level	**Description**
Emergency: Level **1**	Multiple apps/servers/sites. This level should not be used by applications.
Alert. Level **2**	Should be corrected immediately. An example might be the loss of the primary ISP connection.
Critical. Level **3**	May be used to indicate a failure in the system’s primary application.
Error. Level **4**	An application has exceeded it file storage limit and attempts to write are failing.
Warning. Level **5**	May indicate that an error will occur if action is not taken. For example, a non-root file system has only 2GB remaining.
Notice. Level **6**	Events that are unusual but not error conditions.
Informational. Level **7**	Normal operational messages -no action required. For example, an application has started, paused or ended successfully.
Debugging. Level **8**	Info useful to developers for debugging the application.

The second parameter, ***Remote Syslog Level***, selects the maximum severity level to be sent to the Remote Syslog server. Valid values are 1 to 8. The default value is 4. See information about the levels in the previous parameter.

The third parameter, ***Syslog Log***, is a *CheckBox* control. Sending the data to a *Syslog* remote server means that no information is stored locally. This parameter allows local storage to be active simultaneously with external sending, with its own severity level independent of the one used for the remote server. By default, it is NOT selected, which means that a remote server is configured and the traces are **NOT** stored in the local Log.

The last parameter, ***Syslog Server IP***, selects the IP address of the Remote Syslog server to which the information is sent.

> The system can order the selective activation/deactivation of log information associated to some operating blocks (see command **log**).
>
> Through *CLI* it is possible to consult the local log files other than the current one (see command **show**).

5.2 ADMINISTRATION

The equipment has an integrated HTTP server for management purposes. The server supports the HTTP and the HTTPS protocols, and users can selectively enable their use and the respective port.

The equipment also allows to enable FTP and FTPS separately.

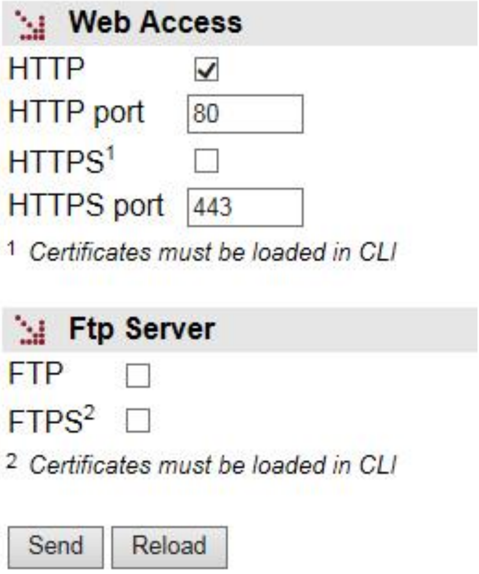
The path that is accessed by FTP within the router is the var / plog where the files can be found:

- Auth
- Auth.0
- Conf.txt
- Conf.xml
- Customer.txt
- Events
- Messages
- Messages.0
- Messages.1

- Messages.2
- Messages.3
- Security
- Security.0

The credentials for accessing the FTP folder are the same as for accessing the equipment.

FIGURE 27 ***Administration*** menu configuration page



Web Access

HTTP ☑

HTTP port 80

HTTPS[1] □

HTTPS port 443

[1] Certificates must be loaded in CLI

Ftp Server

FTP □

FTPS[2] □

[2] Certificates must be loaded in CLI

> The procedure for the installation of the certificates is described in section B.4 of Appendix B, *Data structure in CLI*.

5.3 LAN CONFIGURATION

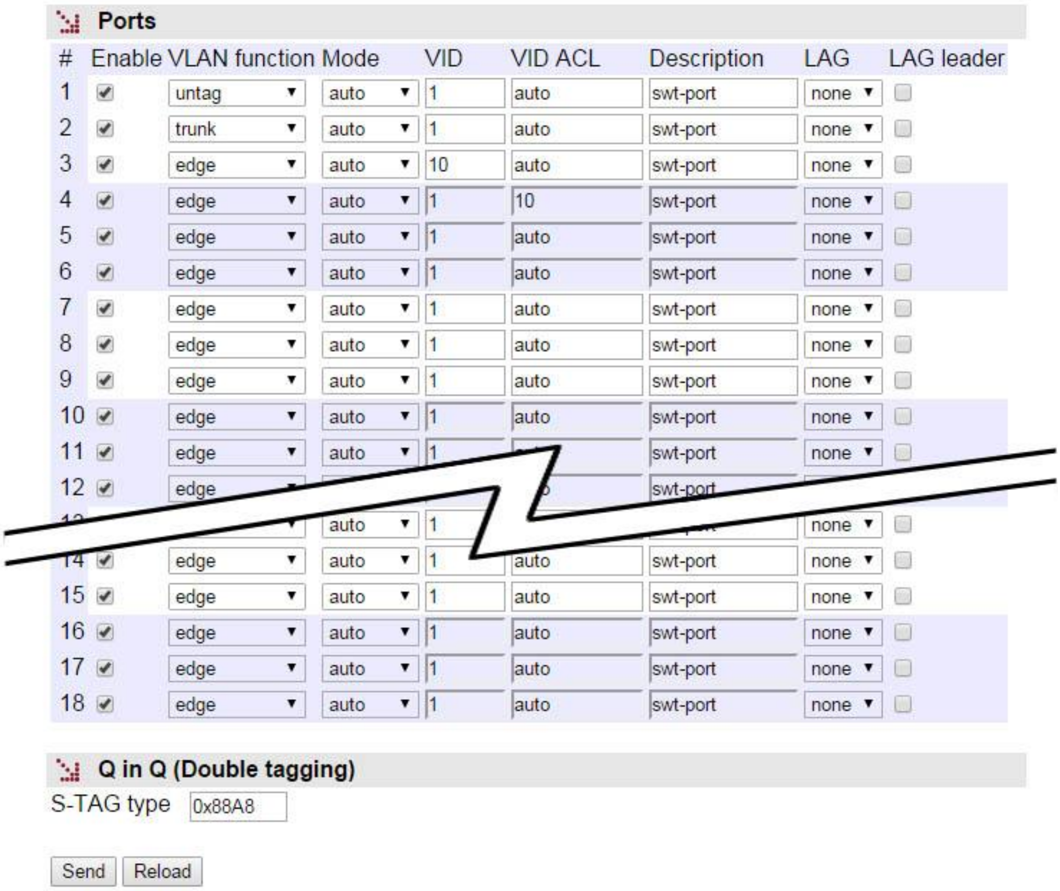
The ***LAN*** menu has two submenus: *Ports and VLAN,* which function is described below.

5.3.1 PORTS

The ***Ports*** menu permits the configuration of the operating parameters of the ports of the equipment, and the assigning of each port to the VLANs defined in the equipment (see section 5.3.2).

> By default, all ports are assigned to **vlan1**.
>
> Web management will be accessible in any of the VLAN logical interfaces where a valid IP address is configured, unless restrictions are applied using filters.

FIGURE 28 ***Ports*** menu configuration page



Ports

#	Enable	VLAN function	Mode	VID	VID ACL	Description	LAG	LAG leader
1	☑	untag ▼	auto ▼	1	auto	swt-port	none ▼	□
2	☑	trunk ▼	auto ▼	1	auto	swt-port	none ▼	□
3	☑	edge ▼	auto ▼	10	auto	swt-port	none ▼	□
4	☑	edge ▼	auto ▼	1	10	swt-port	none ▼	□
5	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
6	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
7	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
8	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
9	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
10	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
11	☑	edge ▼	auto ▼	1		swt-port	none ▼	□
12	☑	edge				swt-port		
			auto ▼	1			none ▼	□
	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
15	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
16	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
17	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□
18	☑	edge ▼	auto ▼	1	auto	swt-port	none ▼	□

Q in Q (Double tagging)

S-TAG type 0x88A8

The page related to the ***Ports*** menu has two well differentiated sections, which are described below.

Ports:

- **#.** It identifies the port number, and it coincides with the equipment connector number. The last four ports are always associated with the SFP ports (SFP1 to SFP4).
- **Enable.** This permits a port to be enabled or disabled, by ticking or not ticking the respective *Enable* box.
- **VLAN function.** It specifies the port behaviour when processing the tag 802.1q, where the options are *edge*, *trunk*, *untag, native, QinQ Core or QinQ Access*.

  Edge: The 802.1 frames will be transmitted with the same 802.1q configuration they had when they are received by the switch, that is, if the received frame included a **tag**, it will be transmitted **with a tag**, and if the received frame **did not include a tag**, it will be transmitted without a **tag**.

  Trunk: All the frames will in all cases be **transmitted with a tag**. It is the specific mode for connection with other switching devices, so as preserve the VLAN information between switches.

  Tag: The 802.1 frames will be transmitted **with a tag,** regardless of the fact that they have a tag or not when they are received by the equipment.

  Untag: The 802.1 frames will be transmitted **without a tag,** regardless of the fact that they have a tag or not when they are received by the equipment.

  Native: The native mode is equivalent to **Trunk** mode, except that the frames belonging to the VLAN that matches the configured **VID** are transmitted without tag. This mode of operation is equivalent to Native VLAN of Cisco, with the consideration that the native VLAN is port-to-port defined by means of the **VID** parameter.

  QinQ Core. All frames are **always** transmitted **with double tag (Double tagged)**. It is the specific mode for the connection to a third-party network from which a privative tag has been obtained.

  QinQ Access. All frames are **always** transmitted with **tag**. It is the specific mode for the interface that accepts the traffic that will be transmitted to a third-party network using double tagging.

- **Mode.** This specifies the type of operation for the port in terms of data rate and operation mode.
  Auto (autonegotiation): Recommended and default value.
  10fdx: 10 Mbit/s Full-duplex.
  100fdx: 100 Mbit/s Full-duplex.
  10hdx: 10 Mbit/s Half-duplex.
  100hdx: 100 Mbit/s Half-duplex.

> If an operation mode other than **Auto** is configured, both ends of the link must be identically configured.

> For **100Base-Fx ports,** only values **100 Mbit/s Full-duplex (100fdx)** and **100 Mbit/s Half-duplex (100hdx)** have sense, so any value other than 100hdx is processed as 100fdx.

> The **SFP** interfaces **do not support changing data rate**, that is to say, **they can operate at the data rate set by the manufacturer**, so that the field value does not affect to the operation of the SFP interfaces.

- **VID (VLAN id by default)**. VLAN numeric identifier in which the port is included. It is also the VLAN identifier to be assigned to the frames received in the port that is untagged, or when the tag includes only the priority (priority tagged). The VLAN definition is selected from the ***VLANs*** menu, see section 5.3.2.

> For the interfaces operating in QinQ Access mode, the value of this parameter determines the VLAN identifier to be included in the most outer tag on the interfaces with double tag, the so-called S-Tag.

- **VID ACL (Access control list).** Access VLANs allowed for each port. This parameter behaves like a filter with regard to packets accepted on the Port level, and only packets with a VLAN identifier included in the list will be processed for transmission and reception purposes. All the packets have a VLAN identifier, either because it was included when they were received (tagged frames) or because it was assigned by the input port at the time of reception, with the **VID** parameter being assigned to the port in the latter case. The special value **any** signifies that the filter is not active. The default value is auto, and it implies that only those packets belonging to the VLAN assigned to the port will be accepted, that is, the filter is not active.

  A group of discreet vlans is configured with the identifier of each one, separated by a comma, without spaces. If a range is to be included, the initial and final vlan identifiers are separated by a dash. Example: in equipment with the **vlan1** to **vlan3** and **vlan5** defined, the group of numerical identifiers will be **1-3,5**.

> For the interfaces operating in QinQ Core mode, the VLAN identifiers that are included in this parameter determine which QinQ Access interfaces are to be served through each interface, those whose VID parameter is part of the ACL.

- **Description.** A mnemonic descriptive field available to users.

- **LAG.** Link group identifier. It sets whether the interface is part of a group of interfaces operating as aggregate interface or not. The value of the parameter, if it is other than **none**, indicates in which of the 8 possible groups the interface will be integrated.

> A group of LAG interfaces is to be considered as a single interface, so that the links of the same group are not to be considered a loop by the STP, allowing a bandwidth increase between equipment while keeping some level of automatic redundancy. All the interfaces within a group must be interconnected to the same end devices.

- **LAG leader.** For proper operation of the aggregate interfaces, all interfaces belonging to the same group must match in their configuration parameters. It is necessary to choose a **Leader** within the group to determine which set of parameters will be used for all the interfaces included in the group. In case for multiple selection, the last that is found is taken as Leader, ignoring the rest.

> If interfaces are configured as members of a group but none of the interfaces is selected as Leader of it, the group will not be effective.

Q in Q (Double tagging):

- **S-TAG type.** This parameter allows the user to set up the ‘ethertype’ field to be used in the service tag or provider, and which allows to identify that a frame includes double tagging. The default value is 0X88A8 according to the standards.

5.3.2 VLAN

A Virtual Local Area Network (VLAN) corresponds to an independent Ethernet spread domain. The equipment can create many of these independent domains and can assign each user ports to one of them. Domains can spread across many switches covering different floors of a building, different buildings, and remote geographical zones.

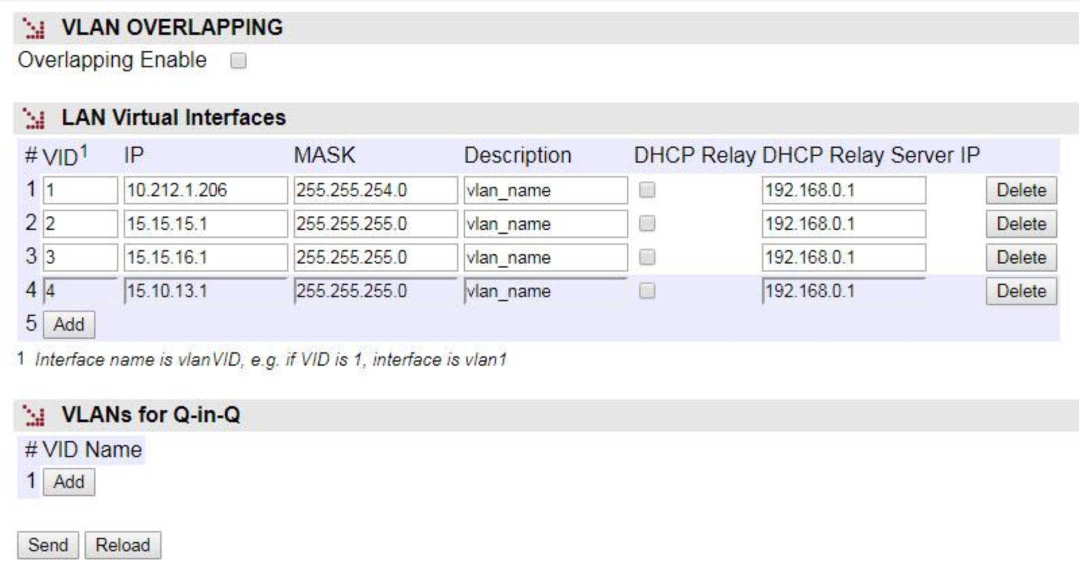
Each VLAN is distinguished from the rest by a specific identifier, usually called a **VID**, which spread in the standard tag specified in the IEEE 802.1q. The tag allows several VLANs to share resources, including switching devices such as the SW3-L3, or links between switching units, with the guarantee that the traffic from each VLAN will reach the correct destination.

The fact that in relation to the equipment, the definition of the VLAN and assigning of the ports to each one is done based on configuration parameters offers great flexibility, as it is possible to alter the topology of the VLANs without having to make changes to the infrastructure.

> The SW3-L3 only processes frames with VLAN identifiers that are expressly defined, regardless of the fact that there are local interfaces assigned to the VLAN defined or not.

In the SW3-L3, the VLAN are also simultaneously the logical interfaces in which routing is performed, and that is why the IP address and the corresponding mask is included as part of the configuration of the VLAN.

FIGURE 29 ***VLANs*** menu configuration page



VLAN OVERLAPPING

Overlapping Enable □

LAN Virtual Interfaces

#	VID[1]	IP	MASK	Description	DHCP Relay	DHCP Relay Server IP	
1	1	10.212.1.206	255.255.254.0	vlan_name	□	192.168.0.1	Delete
2	2	15.15.15.1	255.255.255.0	vlan_name	□	192.168.0.1	Delete
3	3	15.15.16.1	255.255.255.0	vlan_name	□	192.168.0.1	Delete
4	4	15.10.13.1	255.255.255.0	vlan_name	□	192.168.0.1	Delete
5	Add						

[1] *Interface name is vlanVID, e.g. if VID is 1, interface is vlan1*

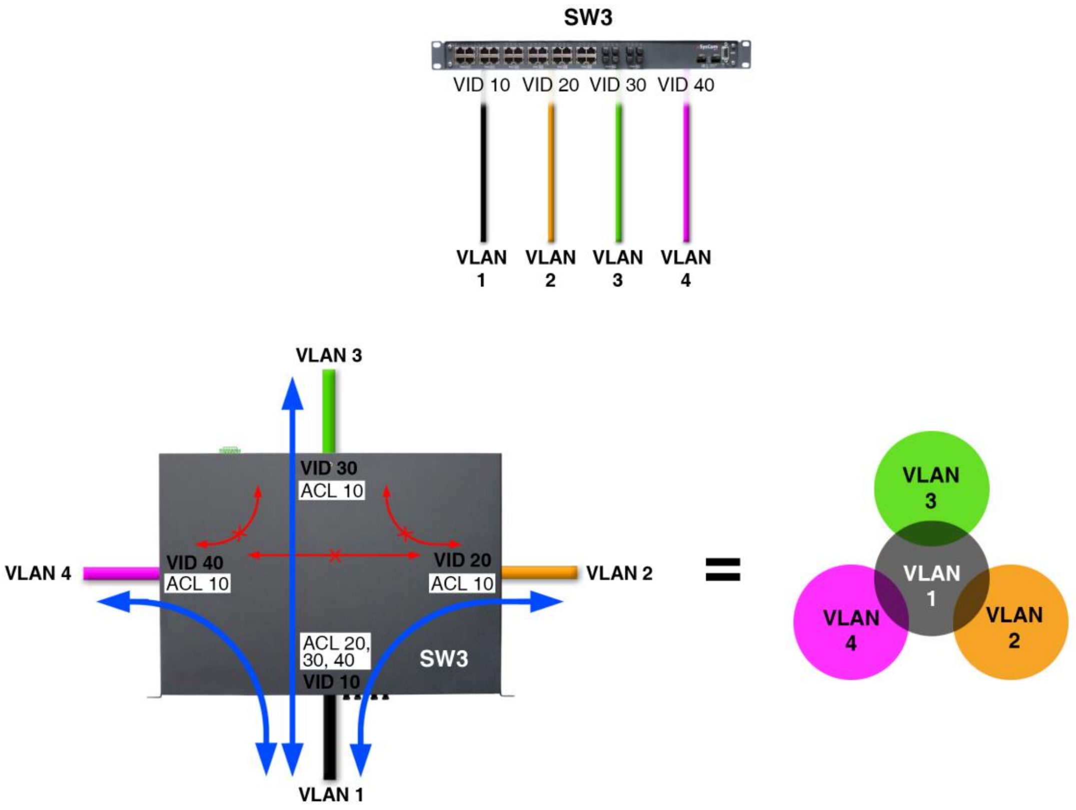
VLANs for Q-in-Q

#	VID	Name
1	Add	

There is a global parameter that affects all the VLANs, which determines the level 2 switching operation, called Overlapping.

- **Overlapping Enable.** It sets the switch internal operation mode as regards the management of the MAC addresses of the different VLANs. The operation mode is ***IVL*** (*Independent VLAN Learning*) by default. The equipment operates in ***SVL*** mode (*Shared VLAN Learning*) with the option selected.
  The ***SVL*** (**Overlapping Enabled**) mode is necessary when using topologies with several VLANs when there is an interface with access to more than one of the configured VLANs, that is, that **the VLANs share some user interface**, and that the **clients operate with UNTAGGED frames**. In these cases, the traffic exclusion is done through the **access control lists** determined for each one of the interfaces (see the ***VID ACL*** parameter in section 5.3.1).
  FIGURE 30 shows an example for using the **Overlapping Enable** parameter.

FIGURE 30 Example for using the **Overlapping Enable** parameter



4 VLANs with common ports and UNTAGGED clients = OVERLAPPING ENABLE ACTIVATED

The IP address for each of the virtual logical interfaces and its mask can be obtained automatically from the DHCP client, which is known as dynamic or NON-static configuration.

Users can activate this service through the *Checkbox* control with the ***Static IP*** label.

When the control **is NOT marked**, the equipment uses the data provided by the **DHCP** client.

When the control **is marked**, the equipment uses the data provided by the **user.**

The individual configuration parameters for each VLAN are:

- **#.** Indicates the position in the table.
- **VID.** It sets the VLAN identifier to be linked to the logical interface. Valid values are **1** to **4095**.
- **IP and MASK.** Values for the IP address and interface mask when operating in static mode.
- **Description.** A mnemonic descriptive field available to users. No conditions the operation of equipment in any way.
- **DHCP Relay.** This parameter indicates whether the DHCP Relay function is enabled or disabled for the logical interface. If so, the requests of received dynamic addresses will be retransmitted to the server with the IP address set in the field below.
- **DHCP Relay Server IP.** Remote DHCP server to which is transmitted the requests of received dynamic addresses.

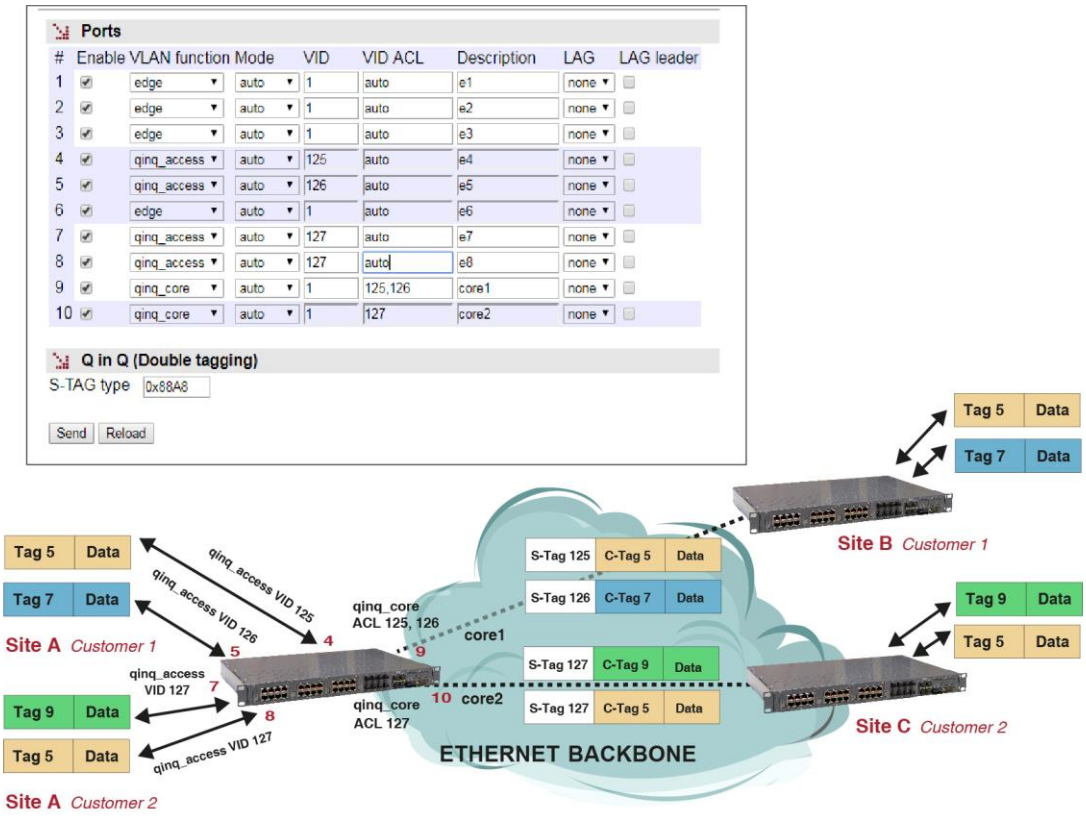
VLANs for Q-in-Q:

In this section must be indicated which of the VLANs will be the ones used in interfaces QinQ Access, that is, which of the VLANs accepted by the equipment will be sent on another network through the use of the double tagging. FIGURE 31 shows an example.

- **#.** Indicates the position in the table.
- **VID.** Indicates that the VLAN VID will be sent with double tagging.
- **Name.** A mnemonic descriptive field available to users.

> The VID identifiers that are configured for the Q-in-Q function will be used in the S-Tag, and will therefore be those indicated by the ethernet backbone provider (usually a third party).
>
> The system does not support that the same VID identifier is in use simultaneously as a local VLAN and as a reserved VLAN for Q-in-Q. In the case of simultaneity, the use as a local VLAN is a priority and would not be considered for the operation of Q-in-Q.

FIGURE 31 Example for using the **VLAN for Q-in-Q** parameter



Ports

#	Enable	VLAN function	Mode	VID	VID ACL	Description	LAG	LAG leader
1	☑	edge	auto	1	auto	e1	none	□
2	☑	edge	auto	1	auto	e2	none	□
3	☑	edge	auto	1	auto	e3	none	□
4	☑	qinq_access	auto	125	auto	e4	none	□
5	☑	qinq_access	auto	126	auto	e5	none	□
6	☑	edge	auto	1	auto	e6	none	□
7	☑	qinq_access	auto	127	auto	e7	none	□
8	☑	qinq_access	auto	127	auto	e8	none	□
9	☑	qinq_core	auto	1	125,126	core1	none	□
10	☑	qinq_core	auto	1	127	core2	none	□

Q in Q (Double tagging)

S-TAG type: 0x88A8

5.4 BANDWIDTH LIMIT CONFIGURATION

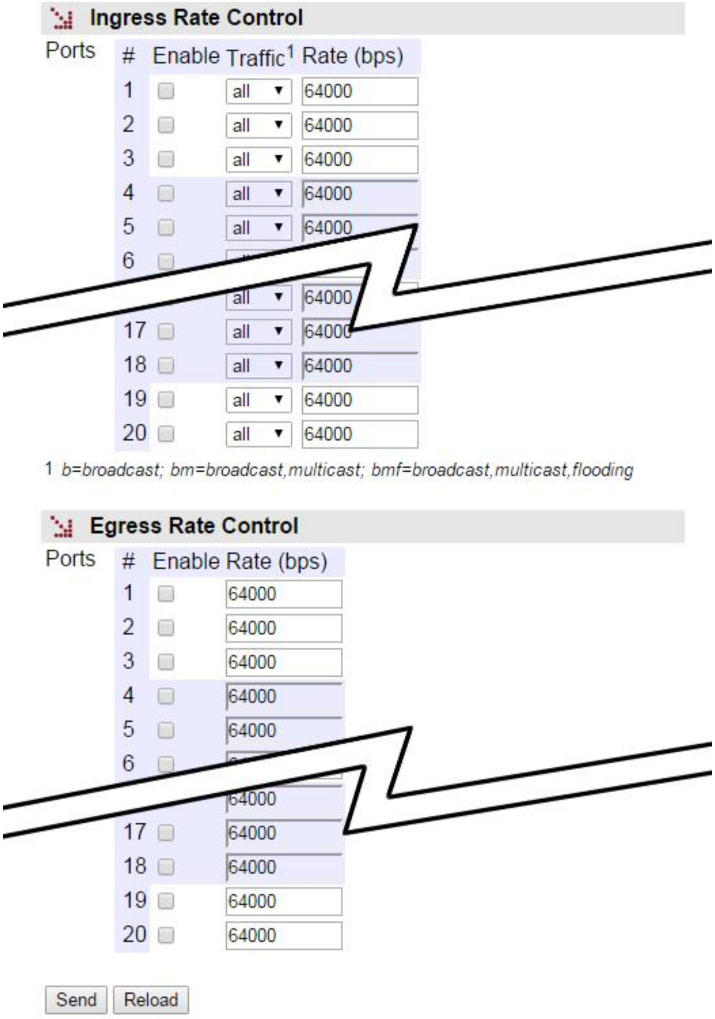
The ***Rate Control*** menu permits bandwidth limits to be selected in each one of the ports, both incoming and outgoing.

The data volume limit may be selected in general for all types of traffic, as well as for certain combinations that take into account the type of Ethernet addresses used: *unicast known*, *unicast unknown*, *multicast* and *broadcast*.

The menu parameters are divided into two quite different blocks, which are:

- Incoming bandwidth control to the port (***Ingress Rate Control***).
- Outgoing bandwidth control from the port (***Egress Rate Control***).

FIGURE 32 ***Rate Control*** menu configuration page



Ingress Rate Control

Ports

#	Enable	Traffic[1]	Rate (bps)
1	□	all ▾	64000
2	□	all ▾	64000
3	□	all ▾	64000
4	□	all ▾	64000
5	□	all ▾	64000
6	□		
		all ▾	64000
17	□	all ▾	64000
18	□	all ▾	64000
19	□	all ▾	64000
20	□	all ▾	64000

[1] b=broadcast; bm=broadcast,multicast; bmf=broadcast,multicast,flooding

Egress Rate Control

Ports

#	Enable	Rate (bps)
1	□	64000
2	□	64000
3	□	64000
4	□	64000
5	□	64000
6	□	
		64000
17	□	64000
18	□	64000
19	□	64000
20	□	64000

The configuration parameters of each block are indicated below.

Ingress Rate Control:

- **#.** It identifies the port number, and it coincides with the equipment connector number. The last four ports are always associated with the SFP ports (SFP1 to SFP4).
- **Enable.** This permits each port to be enabled or disabled individually, by ticking or not ticking the respective *Enable* box.

- **Traffic.** It specifies the type of traffic: ***all***, *broadcast* (***b***), *broadcast* and *multicast* (***bm***) or *broadcast*, *multicast* and *flooding* (***bmf***).
  Broadcast refers to the diffusion messages, that is, the information transmission mode where an emitting node sends information to all the receivers simultaneously.
  Multicast refers to the multi-diffusion messages, which are directed towards to the members of a multi-diffusion group.
  Flooding refers to the situation of unknown unicast address transmission of at the time to be analyzed, which means that they spread by all VLAN interfaces (*flood*).
- **Rate (bps).** It sets the maximum incoming bandwidth to the port: **64000** bps (64 kbps) to **250000000** bps (250 Mbps). The maximum data rate only affects the Gigabit Ethernet ports.

Egress Rate Control:

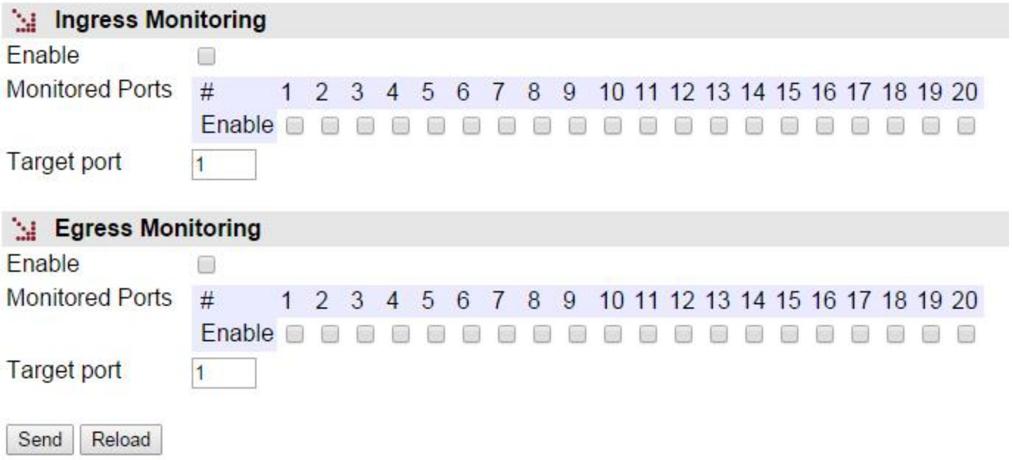
- **#.** It identifies the port number, and it coincides with the equipment connector number. The last four ports are always associated with the SFP ports (SFP1 to SFP4).
- **Enable.** This permits each port to be enabled or disabled individually, by ticking or not ticking the respective *Enable* box.
- **Rate (bps).** It sets the maximum outgoing bandwidth from the port: **64000** bps (64 kbps) to **250000000** bps (250 Mbps). The maximum data rate only affects the Gigabit Ethernet ports.

5.5 PORTS MONITORING CONFIGURATION

This menu performs ***Port mirroring*** functions in the ports in order to monitor their behaviour.

The **incoming and/or outgoing** traffic from a specific port (Monitored port) is replicated in a target port to be monitored through a protocol analyzer, for example.

FIGURE 33 ***Monitor*** menu configuration page



Ingress Monitoring

Enable □

Monitored Ports

#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Enable	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Target port: 1

Egress Monitoring

Enable □

Monitored Ports

#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Enable	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Target port: 1

The menu parameters are divided into two quite different blocks, which are:

- Incoming traffic monitoring (***Ingress Monitoring***).
- Outgoing traffic monitoring (***Egress Monitoring***).

The configuration parameters for each block are indicated below.

Ingress Monitoring:

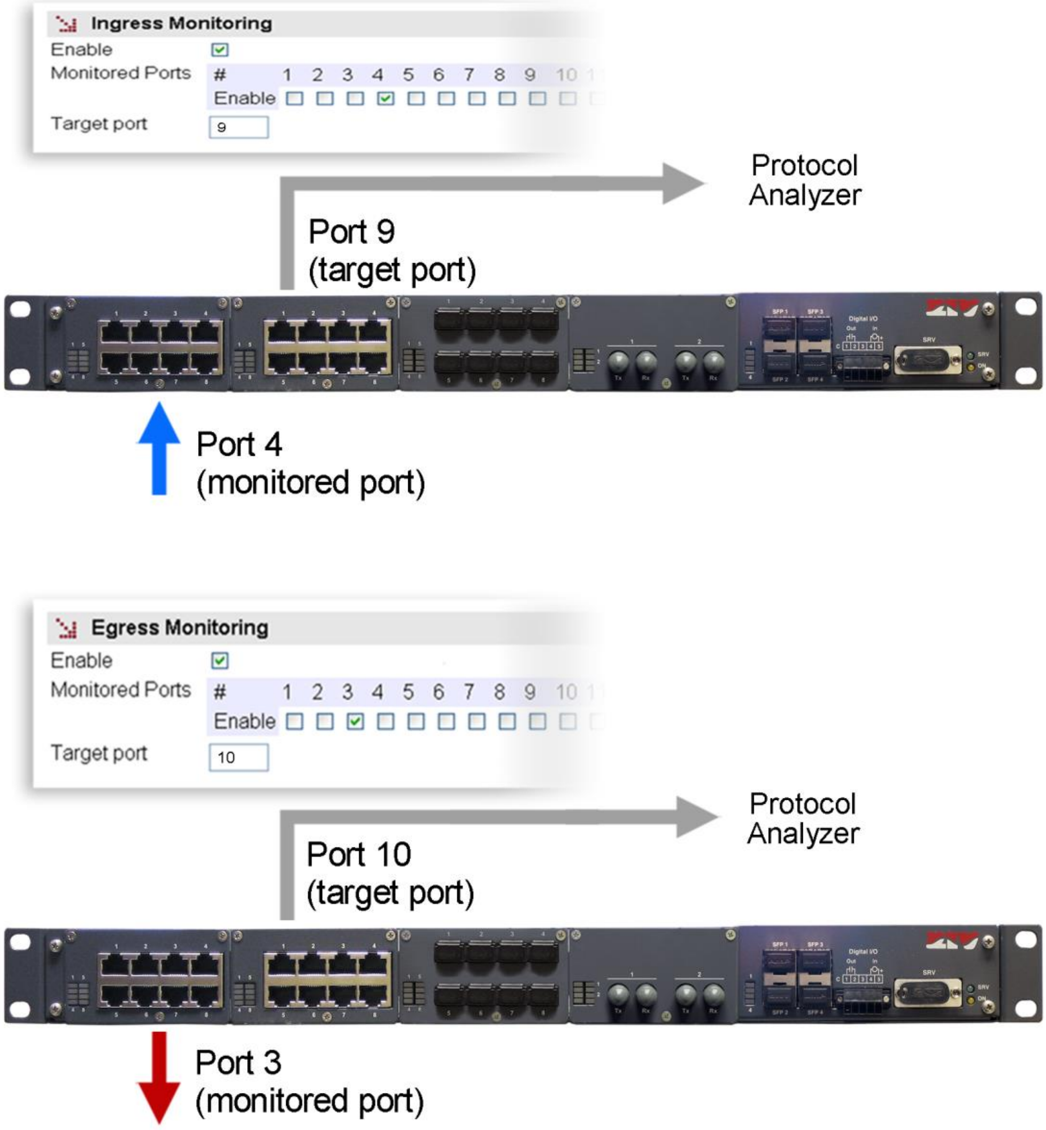
- **Enable.** It permits enabling and disabling monitoring of the incoming traffic by ticking or not ticking the corresponding box.
- **Monitored Ports.** It sets the port or ports to be monitored. The incoming traffic in each one of the selected ports will be replicated in the target port.
- **Target port.** It sets the port where the replicated packets will be sent to be monitored.

Egress Monitoring:

- **Enable.** It permits enabling and disabling monitoring of the outgoing traffic by ticking or not ticking the corresponding box.
- **Monitored Ports.** It sets the port or ports to be monitored. The outgoing traffic in each one of the selected ports will be replicated in the target port.

- **Target port.** It sets the port where the replicated packets will be sent to be monitored.

FIGURE 34 Example of ***Monitor*** menu configuration



Ingress Monitoring

Enable ☑

Monitored Ports

#	1	2	3	4	5	6	7	8	9	10
Enable	□	□	□	☑	□	□	□	□	□	□

Target port 9

Egress Monitoring

Enable ☑

Monitored Ports

#	1	2	3	4	5	6	7	8	9	10
Enable	□	□	☑	□	□	□	□	□	□	□

Target port 10

5.6 LLDP CONFIGURATION

LLDP is a standard protocol of the link layer used to announce identity and capabilities to neighbouring devices in local area networks.

Both the information transmitted and the information received is accessible through the SNMP protocol, through the MIBs defined in the LLDP standard itself, and is usually used to determine the topology of the networks.

The standard sets information fields that must be included in a mandatory way. Other fields are optional and the user can select the information of each of them.

> Accessing information through SNMP necessarily implies that the SNMP agent is enabled.

The device controls the execution of the LLDP protocol through a *CheckBox* parameter, and offer additional, specific parameters for each of the ports, which are the following:

- **Admin Status.** It sets the operation mode of the LLDP agent of the interface. Valid values are *TxRx*, *TxOnly*, *RxOnly* and *disabled*. The default value is *TxRx*.

- **Tx Interval.** It sets the time between the transmission of messages, in normal operation. The units are seconds, and 30 is the default value and recommended. Valid values are 1 to 3600.

- **Hold.** The value of this parameter is used as a multiplier on *Tx Interval* and determines the value of *txTTL* that is included in the LLDP messages sent by the agent. 4 is the default value and recommended. Valid values are 1 to 100.

- **Reinit.** It sets the period of time between the setting of *Admin Status* as *disabled* and the reinitialization attempt. The units are seconds, and 2 is the default value and recommended. Valid values are 1 to 10.

- **Credit Max.** It sets the maximum number of consecutive LLDP messages that can be transmitted at any time. 5 is the default value and recommended. Valid values are 1 to 10.

- **Tx Interval Fast.** It sets the period of sending LLDP messages in the period of high-speed transmission, which is activated automatically when a neighbouring device is detected. 1 is the default value and recommended. Valid values are 1 to 3600.

- **Mess num Fast.** It sets the number of LLDP messages that will be sent during a high-speed transmission. 4 is the default value and recommended. Valid values are 1 to 8.

- **Tx Notif. Enable.** Indicates to the LLDP agent whether SNMP (traps) notifications must be sent when changes occur in the remote information received in the interface.

> In order for SNMP notifications to be effectively sent, they must be explicitly allowed to be sent in the SNMP menu.

- **PortDesc.** Indicates to the LLDP agent whether or not to include the optional field with the descriptive information of the interface in the LLDP messages sent. The value of the field is the text of the *Description* parameter of the *Port* menu (see 5.3.1).

- **SysName.** Indicates to the LLDP agent whether or not to include the optional field with the name of the device in the LLDP messages sent. The value of the field is the text of the *Hostname* parameter of the main menu (see 5.1.1).

- **SysDesc.** Indicates to the LLDP agent whether or not to include the optional field with the description of the device in the LLDP messages sent. The value of the parameter is obtained automatically from the running firmware, so it is not subject to changes by the user.

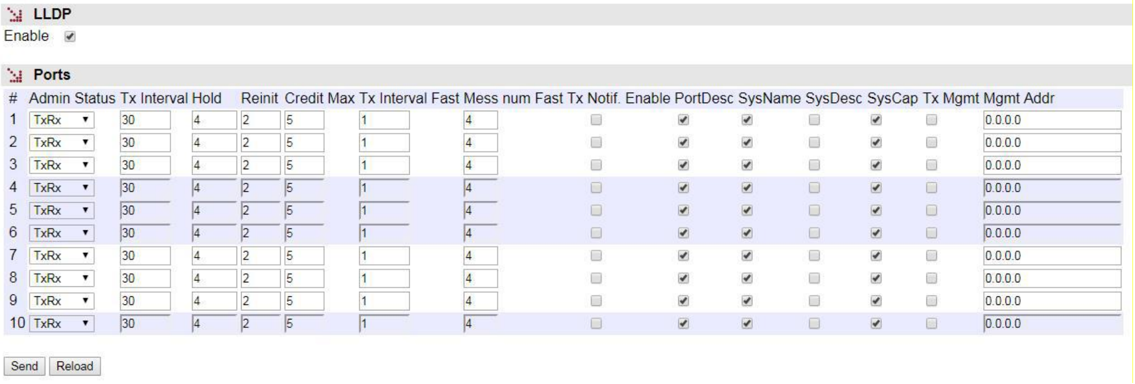
- **SysCap.** Indicates to the LLDP agent whether or not to include the optional field with the device capabilities in the LLDP messages sent. The coding of the field is set in the standard and it is made up of flags. The value is automatically inserted.

- **Tx Mgmt.** Indicates to the LLDP agent whether or not to include the optional field with the management address of the device in the LLDP messages sent. The value to be sent is set by the *Mgmt Address* parameter.

- **Mgmt Address.** It allows the user to set the value of the optional field that reports the management address of the device.

The protocol has its own statistics that show the data specific to the execution of the protocol in each interface as part of the information received.

FIGURE 35 Example of configuration of ***LLDP*** menu



LLDP

Enable ☑

Ports

#	Admin Status	Tx Interval	Hold	Reinit	Credit Max	Tx Interval Fast	Mess num Fast	Tx Notif. Enable	PortDesc	SysName	SysDesc	SysCap	Tx Mgmt	Mgmt Addr
1	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0
2	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0
3	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0
4	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0
5	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0
6	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0
7	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0
8	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0
9	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0
10	TxRx ▾	30	4	2	5	1	4	☐	☑	☑	☐	☑	☐	0.0.0.0

5.7 QoS CONFIGURATION

The Quality of Service (QoS) permits the traffic classification and service policy and selects the conditions in which it will be treated by the equipment.

The equipment provides QoS at level 2 (switching). Level 2 QoS is performed on switched traffic, adjusted to the processing of parameters and behaviour of IEEE 802.1p, with four internal priority levels. This priority is taken into account for selecting the processing and transmission order in each switch output interface.

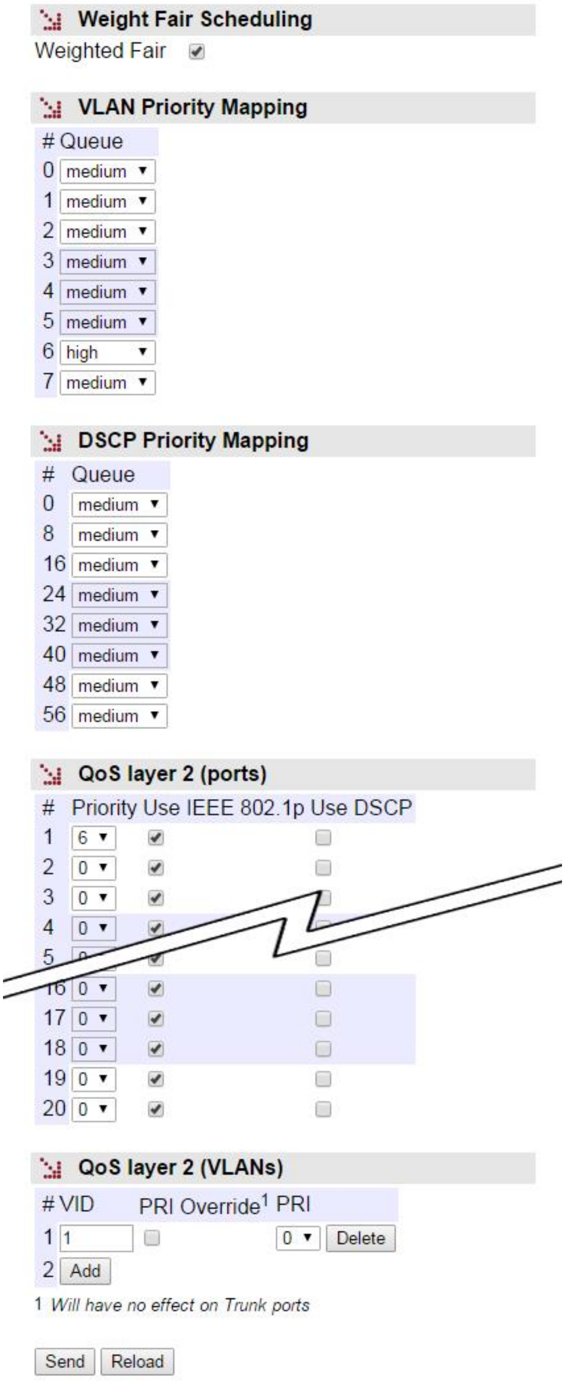
Two potential service policies are admitted in processing the queues for each priority: ***Priority*** or ***Weight Fair Scheduling*** **(WFQ)**. The ***Priority*** policy only serves a queue with a lower priority when the higher priority queues are empty. The **WFQ** policy guarantees a weighted service for all the priority, but pre-eminently to queues with a high priority.

The service policy is unique for level 2 service. The parameters are the VLAN and the priority 802.1p (included in the tag or assigned depending on the input port) or the DSCP field of level 3.

The priority supported by standard 802.1p admits values of between 0 and 7. The untagged frames received are given a priority within that range, depending on the interface through which they were received, pursuant to the section entitled **QoS Layer 2 (ports)**. Tagged frames may include either the VLAN identifier as the priority (tagged) or only the priority (priority tagged, VLAN = 0). If the VLAN identifier is included, they are processed in accordance with the rules of the section **QoS Layer 2 (VLANs)**. If, on the contrary, they only include the priority, they are processed in accordance with the section entitled **QoS Layer 2 (ports).**

In any case, except for the DSCP assignment that is direct to the internal queues, the assigned priority is used for the final classification in accordance with the section **VLAN Priority Mapping.**

FIGURE 36 ***QoS*** menu configuration page



Weight Fair Scheduling

Weighted Fair ☑

VLAN Priority Mapping

#	Queue
0	medium
1	medium
2	medium
3	medium
4	medium
5	medium
6	high
7	medium

DSCP Priority Mapping

#	Queue
0	medium
8	medium
16	medium
24	medium
32	medium
40	medium
48	medium
56	medium

QoS layer 2 (ports)

#	Priority	Use IEEE 802.1p	Use DSCP
1	6	☑	☐
2	0	☑	☐
3	0	☑	☐
4	0	☑	☐
5	0	☑	☐
16	0	☑	☐
17	0	☑	☐
18	0	☑	☐
19	0	☑	☐
20	0	☑	☐

QoS layer 2 (VLANs)

#	VID	PRI Override[1]	PRI	
1	1	☐	0	Delete
2	Add			

1 *Will have no effect on Trunk ports*

Send Reload

The sections and their configuration parameters are as follows:

Weight Fair Scheduling:

- **Weighted Fair.** This sets the level 2 priority service policy. When the NO option is enabled, the policy is ***Priority***. When the Yes option is enabled, the policy is ***WFQ***.

VLAN Priority Mapping:

- **#.** This identifies the value of the priority contained in the tag 802.1 of the frame (it covers the whole range of values permitted by the standard), or that which is assigned by default based on input port when the frame does not include the tag 802.1.
- **Queue.** This sets the queue priority in which the traffic coinciding with the priority value indicated by the # field will be inserted. Valid values identify the four internal priorities: **High**, **Medium, Low** or **Mgmt.**

> ! Although it is available, it is recommended to reserve the **Mgmt** priority for exclusive use as priority 7, avoiding the use of such priority for user traffic.

DSCP Priority Mapping:

- **#.** Identifies the DSCP values, located in the IPv4 header, that the equipment is able to distinguish.
- **Queue.** This sets the queue priority in which the traffic coinciding with the DSCP value indicated by the # field will be inserted. Valid values identify the three internal priorities: **High**, **Medium** or **Low.**

QoS layer 2 (ports):

- **#.** The physical interface identifier.
- **Priority.** Value of the priority assigned to frames 802.1 received through the interface indicated by #. This priority is assigned when the frames received do not include an 802.1p tag. The assigning of internal priorities is done based on the values selected in the section entitled **VLAN Priority Mapping**.

- **Use IEEE 802.1p.** The enabled option indicates that the priority field present in the frames must be used when they include tag 802.1p. The assigning of internal priorities is done based on the values selected in the section entitled **VLAN Priority Mapping.**

- **Use DSCP.** The enabled option indicates that the DSCP field of the frames received must be processed, to assign the internal frame priority of the frame, based on the values selected in the section entitled **DSCP Priority Mapping.**

> The options **Use IEEE 802.1p** and **Use DSCP** may be activated simultaneously. The hierarchy for the final priority assigned to the frame is the following: **DSCP**, **IEEE 802.1p** and **Priority** (user); so that:
>
> - The priority selected as default value in the input port will be associated with a frame without tag 802.1.
>
> - Regardless of whether the priority was already included in the original frame or assigned by the mechanism described in the previous paragraph, if header is IPv4, the choice of the process queue will take into account the value of the DSCP field. If the traffic is not IPv4, the choice of the process queue will be based on the priority 802.1.

QoS layer 2 (VLANs):

This section includes a table that supports adding and removing sets of parameters.

- **#.** Indicator of position in the table.

- **VID.** VLAN identifier value included in the tag 802.1.

- **PRI Override.** This sets whether the priority of the frames belonging to the VLAN that matches the VID field should be modified (option enabled) or must remain the priority received (option NOT enabled).

- **PRI.** If the **PRI Override** option is enabled, it modifies the priority assigned to the frames belonging to the VLAN that matches the VID field.

5.8 ROUTING CONFIGURATION

The equipment operates as a router for the IPv4 protocol. The router services are always active. The data for the routing function may have two sources; static data of a permanent nature established by the user and dynamic data, obtained by the equipment itself through executing the standard routing protocols: RIP, OSPF and BGP.

The IP address of the different devices is configured in section 5.3.2. If it is desired that the routing functionality may not work in any of the configured devices (vlan), simply assign to it the IP address equal to IP 0.0.0.0. If routing should be partially active instead of not being active, the filtering rules must be configured, see section 5.9.

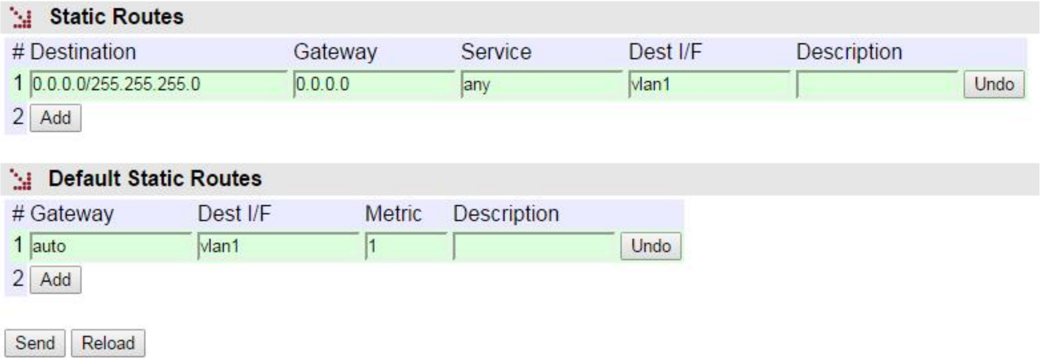
The ***Routing*** menu contains five submenus: ***Static Routes, DNS servers***, ***RIP, OSPF*** and ***BGP***, which are described in the following sections.

5.8.1 Static routes

Through the *Static routes* submenu in the *Routing* menu, the user can provide the system with the static and permanent data for the routing service.

Two types of data are configured in this submenu; explicit static routes in the section *Static Routes*, and the address acting as a route by default in the case that the service has no specific data for reaching a destination, in the section *Default Static Routes*.

FIGURE 37 *Static routes* submenu in the *Routing* menu



Static Routes

#	Destination	Gateway	Service	Dest I/F	Description	
1	0.0.0.0/255.255.255.0	0.0.0.0	any	vlan1		Undo
2	Add					

Default Static Routes

#	Gateway	Dest I/F	Metric	Description	
1	auto	vlan1	1		Undo
2	Add				

The parameters for configuring a static route are:

- **Destination.** This allows the IP address to be specified, and the remote or destination network subnet mask. The field requires the values to be entered in the IP address format. Example: 192.168.0.0/255.255.255.0 or 192.168.0.0/24.

- **Gateway.** This allows the IP address of the router to which the traffic destined for the remote network of the previous field must be sent.

- **Service.** This allows an additional filter to be set in the remote IP address for determining the selection of the next hop. The condition is selected based on a specific service (tcp/udp/icmp). After the service the port number (1÷65535), must be indicated, separated by two points. The default value is **any**, that is to say, the route applies for all types of traffic (only the IP destination is taken into account). Example: tcp:5000, which means that all the packets with tcp traffic on port 5000 will be sent to the indicated router.

- **Dest I/F (Destination interface).** This allows the interface through which the routed traffic coinciding with this route will be sent. The interfaces are identified by the associated device, e.g. vlan1.

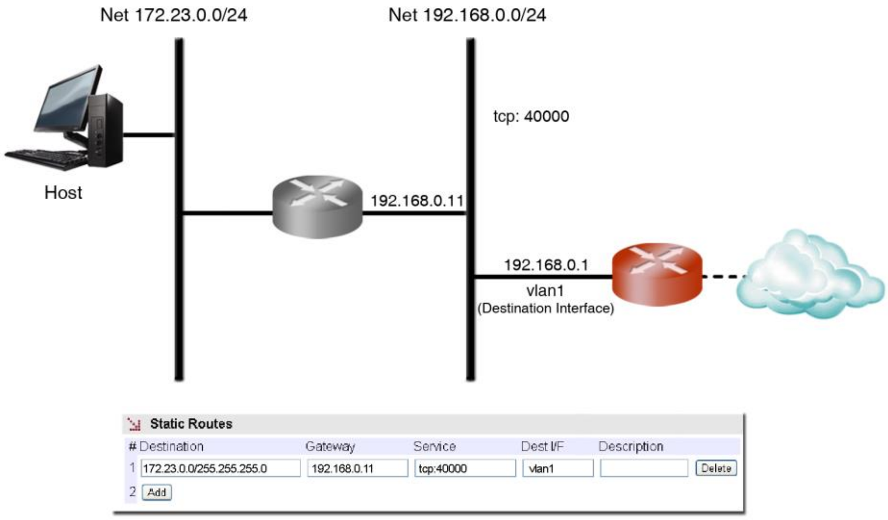
- **Description.** This permits a description of up to 15 alphanumerical characters to be specified.

Example:

The figure shows an example of assigning a static route between two different network segments. All the TCP packets of port 40000 can reach the network segment 172.23.0.0/24 through router 192.168.0.11.

FIGURE 38

Example of how a static route is configured



#	Destination	Gateway	Service	Dest I/F	Description
1	172.23.0.0/255.255.255.0	192.168.0.11	tcp:40000	vlan1	

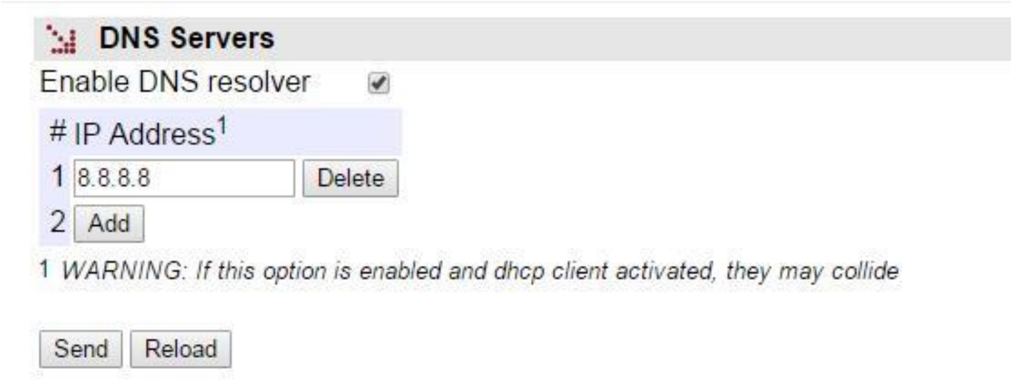
The default parameters for configuring a static route are:

- **Gateway.** This allows the IP address of the next router to be specified for routing traffic whose destination does not coincide with any known route.
- **Dest I/F (Destination interface).** This permits the specification of the interface through which traffic routed to the router indicated in the previous field will be sent. The interfaces are identified by the associated device, e.g. vlan1.
- **Metric.** This permits a value to be set originating from among the default different routes that could be created. A higher metric means a lower priority.
- **Description.** This permits a description of up to 15 alphanumerical characters to be specified.

5.8.2 DNS servers

The equipment supports configuring DNS servers in the *DNS Servers* submenu by configuring their IP addresses.

FIGURE 39 *DNS Servers* submenu in the *Routing* menu



DNS Servers

Enable DNS resolver ☑

#	IP Address[1]	
1	8.8.8.8	Delete
2	Add	

[1] WARNING: If this option is enabled and dhcp client activated, they may collide

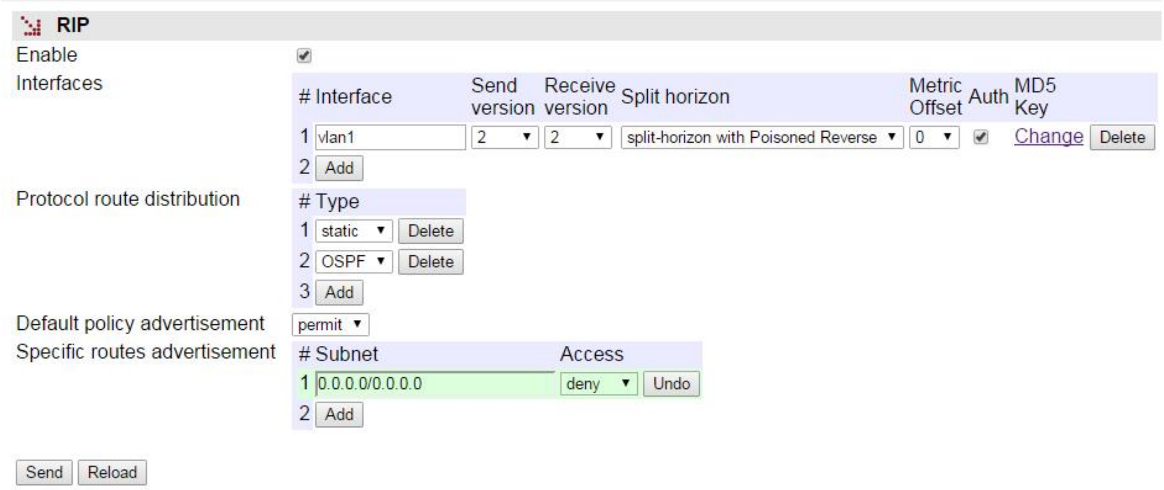
As indicated in the warning of the figure, it must be taken into account that the simultaneous configuration of the DNS servers together with interfaces operating in DHCP mode may imply an incorrect final configuration, given that it is quite typical that the DHCP setup should also include the DNS servers.

5.8.3 RIP Protocol

The equipment has the standard RIPv1 [1] and RIPv2 [2] routing protocol.

The RIP protocol can be enabled or disabled by the user, through the *Checkbox Enable* control. If the user enables the protocol, the interfaces in which it is required to be operative must also be established.

FIGURE 40 *RIP Protocol* submenu in the *Routing* menu



RIP

Enable ☑

Interfaces

#	Interface	Send version	Receive version	Split horizon	Metric Offset	Auth	MD5 Key	
1	vlan1	2	2	split-horizon with Poisoned Reverse	0	☑	Change	Delete
2	Add							

Protocol route distribution

#	Type	
1	static	Delete
2	OSPF	Delete
3	Add	

Default policy advertisement: permit

Specific routes advertisement

#	Subnet	Access	
1	0.0.0.0/0.0.0.0	deny	Undo
2	Add		

Send Reload

The configuration parameters for each interface are:

- **Interface.** This identifies the real or virtual device in which the protocol execution must be enabled.
- **Send version.** This selects the protocol version to be use by the equipment to transmit the routing data on the specified interface. The options are: ***none*** (no information transmitted), ***1*** (version 1), ***2*** (version 2) and ***1-2*** (information transmitted with both versions).
- **Receive version.** This selects the protocol version accepted by the equipment in the messages received in the specified interface. The options are: ***none*** (no RIP message accepted), ***1*** (only messages with version 1 will be processed), ***2*** (only messages with version 2 will be processed) and ***1-2*** (messages with either version are accepted).

- **Split-horizon.** This sets the criteria to be used in processing the routing data, in order to prevent the “counting to infinity” problem. The options are: ***no split-horizon***, ***split-horizon*** and ***split-horizon with poisoned reverse*** (See section 3.4.3 of [2, bibliography reference]).

- **Metric offset.** This field allows the user to set a weight that is added to the metric of the routes advertised by each of the interfaces. Valid values are from 0 to 15. Value 0 is not altering the metrics, and 15 is the maximum value that is accepted as valid metric in RIP. Value 16 is interpreted as infinity.

- **Auth.** This field enables authentication for RIP messages sent on the interface and, in turn, implies the requirement that the received messages are also authenticated. Authentication using MD5 is always performed.

- **MD5 Key.** This text field sets the key that is used to calculate the MD5 hash that is used for the authentication of the RIP packets. Its maximum length is 16 characters.

The common configuration parameters for all interfaces are:

- **Protocol Route Distribution.** It indicates whether the protocol must include not only the routing information obtained through the protocol messages and IP data of the local interfaces, but also the routing data specified in the static routes section or other dynamic routing protocols (OSPF and BGP options). Local network addresses of the device are always spread.

- **Default policy advertisement and Specific routes advertisement.** These two parameters allow filtering options to be selected on the routing information. The first selects the general filter criteria (permit or reject) and affects all the routes. The second permits the desired exceptions to the general criteria to be indicated, and therefore each specific input also includes the permit or reject option.

General criteria options combined with possible exceptions allow the filter to behave in two ways:

- **Send all with exceptions.** The general *permit* criteria option, which is the default value, with the exclusions selected in the respective section, which in this case, would have the *reject* option enabled.

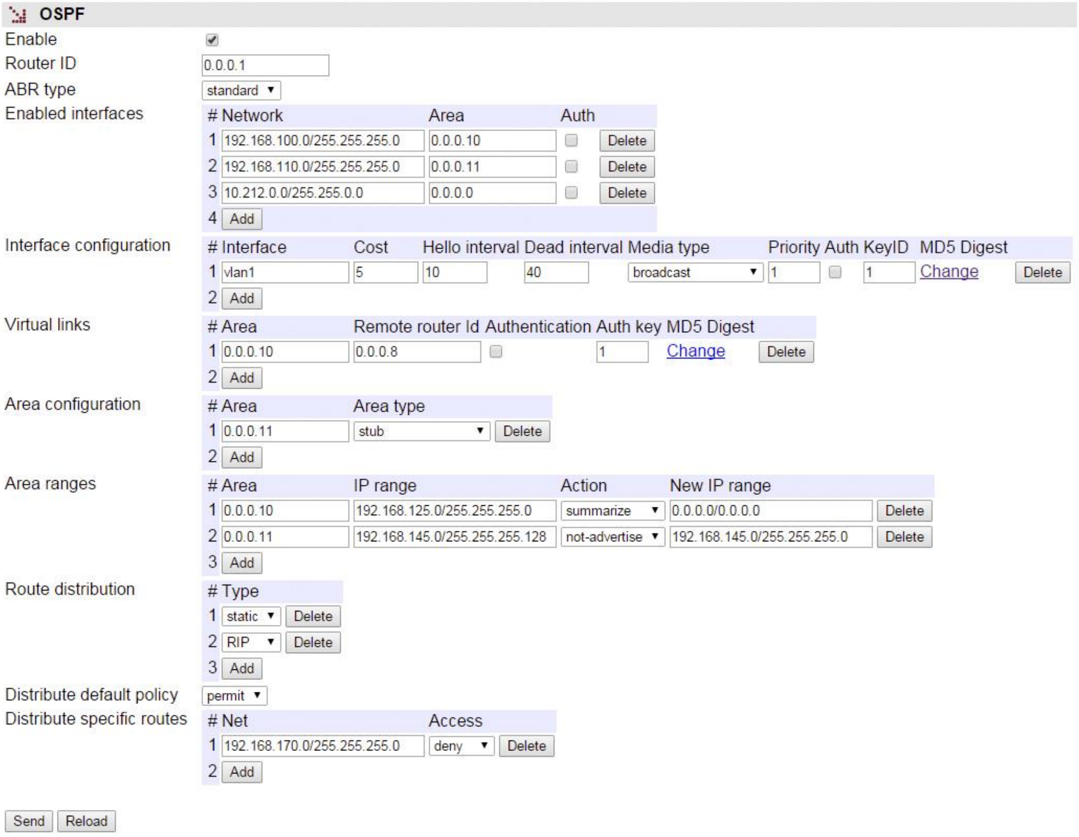
- **Only exceptions sent.** The general *reject* criteria option, with the exceptions selected in the respective section, which in this case would have the *permit* option enabled.

5.8.4 OSPF Protocol

The equipment has the standard OSPFv2 routing protocol.

The OSPF protocol can be enabled or disabled by the user, through the *Checkbox Enable* control.

FIGURE 41 *OPSF Protocol* submenu in the *Routing* menu



OSPF

Enable ☑

Router ID: 0.0.0.1

ABR type: standard ▾

Enabled interfaces

#	Network	Area	Auth	
1	192.168.100.0/255.255.255.0	0.0.0.10	□	Delete
2	192.168.110.0/255.255.255.0	0.0.0.11	□	Delete
3	10.212.0.0/255.255.0.0	0.0.0.0	□	Delete
4	Add			

Interface configuration

#	Interface	Cost	Hello interval	Dead interval	Media type	Priority	Auth	KeyID	MD5 Digest	
1	vlan1	5	10	40	broadcast ▾	1	□	1	Change	Delete
2	Add									

Virtual links

#	Area	Remote router Id	Authentication	Auth key	MD5 Digest	
1	0.0.0.10	0.0.0.8	□	1	Change	Delete
2	Add					

Area configuration

#	Area	Area type	
1	0.0.0.11	stub ▾	Delete
2	Add		

Area ranges

#	Area	IP range	Action	New IP range	
1	0.0.0.10	192.168.125.0/255.255.255.0	summarize ▾	0.0.0.0/0.0.0.0	Delete
2	0.0.0.11	192.168.145.0/255.255.255.128	not-advertise ▾	192.168.145.0/255.255.255.0	Delete
3	Add				

Route distribution

#	Type	
1	static ▾	Delete
2	RIP ▾	Delete
3	Add	

Distribute default policy: permit ▾

Distribute specific routes

#	Net	Access	
1	192.168.170.0/255.255.255.0	deny ▾	Delete
2	Add		

The group of parameters necessary to execute the protocol and its conditions are described below:

- **Router ID.** Identifies the equipment. Although the format coincides with that normally used for an IP address, it is really a digit to distinguish the routers executing the OSPF protocol from each other. Normally, it coincides with one of the IP addresses assigned to the router.

- **ABR Type.** This field allows to change the behaviour of the router. In default conditions, it is according to the standard, but it admits as alternative options *cisco* and *ibm* values, which are equivalent. When the value is different from *standard*, the router can consider the messages received from other ABR through areas other than the backbone, when in normal conditions would not. Behaviour change is consistent with the implementation described in Cisco routers and IBM. It must be taken into account that areas with full adjacency through virtual links are considered with full capacity for transit. In this way, they can be used to route the traffic of the backbone, and this configuration do not affect them.

- **Enabled interfaces.** This has three values, the first being an IP address or range of IP addresses, which means that the interface or interfaces whose IP addresses are included in the referred range will execute the OSPF protocol, and their area will be that indicated by the **Area** parameter (second parameter); despite the fact that it is usually represented as an IP address, it is the element identifying the Area to which the interfaces included by the first value are connected. All the routers with interfaces operating in the same area share that identification element. The area with the identifier 0.0.0.0 is valid and behaves as a backbone, since all the areas must be connected to it. The third parameter determines whether messages for the defined area should provide and require authentication, using MD5 for it. The value for the calculation of the hash must be configured in the following section of interface configuration given that, with different interfaces of the same area, it is possible to use different keys.

- **Interface configuration.** The interfaces on which the protocol runs allow the modification of various parameters associated with them. The parameters are:

  - **Interface.** Identification of the interface to be configured.

  - **Cost.** Cost associated with the link for the interface. The cost is the value used in the field associated with the metric of the router-LSA messages and it will be used to calculate the SPF algorithm (Shortest Path First). The default value is 5.

  - **Hello interval.** It sets the value, in seconds, of the timer that controls the transmission of the *Hello* messages. The default value is 10 s.

  - **Dead interval.** It sets the value, in seconds, of the timer that monitors the inactivity and waiting processes of the remote routers. The default value is 40 s.

  - **Media type.** Identifies the media type associated with the interface. Valid values are: ***broadcast***, ***non-broadcast***, ***point-to-multipoint*** and ***point-to-point***.

 - **Priority.** It sets the priority value of the router. The router with the highest priority has more options to be chosen as *Designed Router*. The 0 value means that it will never be chosen. The default value is 1.

 - **Authentication.** This parameter controls the use of the MD5 authentication, on the interface, for the protocol messages.

 - **KeyID.** Parameter that identifies the secret key used to create the **MD5 Digest** (next parameter). The field is part of the protocol and should be consistent in all routers operating in the same link. Valid values are 1 to 255.

 - **MD5 Digest.** Key used to generate the MD5 hash that is used as authentication. Its value is linked to the **KeyID** parameter. The maximum lenght is 16 characters.

- **Virtual links.** It offers the possibility of creating virtual links in order that routers that do not have interfaces in the backbone (area 0.0.0.0) can have connectivity. The **Area** parameter indicates in which of the equipment access areas the virtual connection will be created. The equipment identifier in which the virtual connection will be carried out is configured in **Remote router Id**. By means of an option it is possible to enable the use of MD5 authentication for the said connection. The **Auth Key** parameter is a numeric value that must be shared by the remote end (according to protocol standard). The last parameter, **MD5 Digest,** sets the alphanumeric key to generate the MD5 hash. The maximum length is 16 characters.

- **Area configuration.** This parameter sets a behaviour that be alternative to the standard, as detailed in the protocol specification. The types are *stub* and *stub_no_summary* (also known as Not So Stuby Area or NSSA). The area identifier must be specified in **Area** as well as the desired topology. When configuring areas with any of the mentioned types, it is necessary to communicate the route by default in the areas. In this way, it is necessary to include the *default* option in the route distribution block (Protocol Route Distribution).

- **Area ranges.** This parameter sets rules for the intra-area route processing when the routes are announced in other areas (protocol type 3 messages). The parameters are:

   - **Area.** Identifies the area in which the address range of the following parameter must be detected.

  - **IP Range.** Address range, by means of mask, that will involve the execution of the configured action.

  - **Action.** There are three options: *summarize*, *not-advertise* and *substitute*. ***Summarize****:* if in the configured area there is any address included in the selected range, the IP range as address in a message of type 3 will be announced to the rest of the areas (in practice, all the networks of the range are agglomerated in an unique announced address).

    Not-advertise: in the same detection conditions, instead of grouping the addresses, the router will not announce the addresses to the other areas. ***Substitute***: it is equivalent to *summarize*, but instead of the detection range, the selected route will be announced in the following field.

  - **New IP Range.** Value to be announced if the **Action** is *substitute* and an address exists in the **Area** included in the detection range of **IP Range**.

- **Protocol Route distribution.** It indicates whether the protocol must include not only the routing information obtained through the protocol messages and IP data of the local interfaces, but also the routing data specified in the static routes section or other dynamic routing protocols (RIP and BGP options). Local network addresses of the device are always spread.

- **Distribute default policy** and **Distribute specific routes.** These two parameters select filtering options of the routing information obtained by means other than OSPF protocol. The first selects the general filter criteria (permit or reject) and affects all the routes. The second permits the desired exceptions to the general criteria to be indicated, and therefore each specific input also includes the permit or reject option.

General criteria options combined with possible exceptions allow the filter to behave in two ways:

- **Send all with exceptions.** The general *permit* criteria option, which is the default value, with the exclusions selected in the respective section, which in this case, would have the *reject* option enabled.

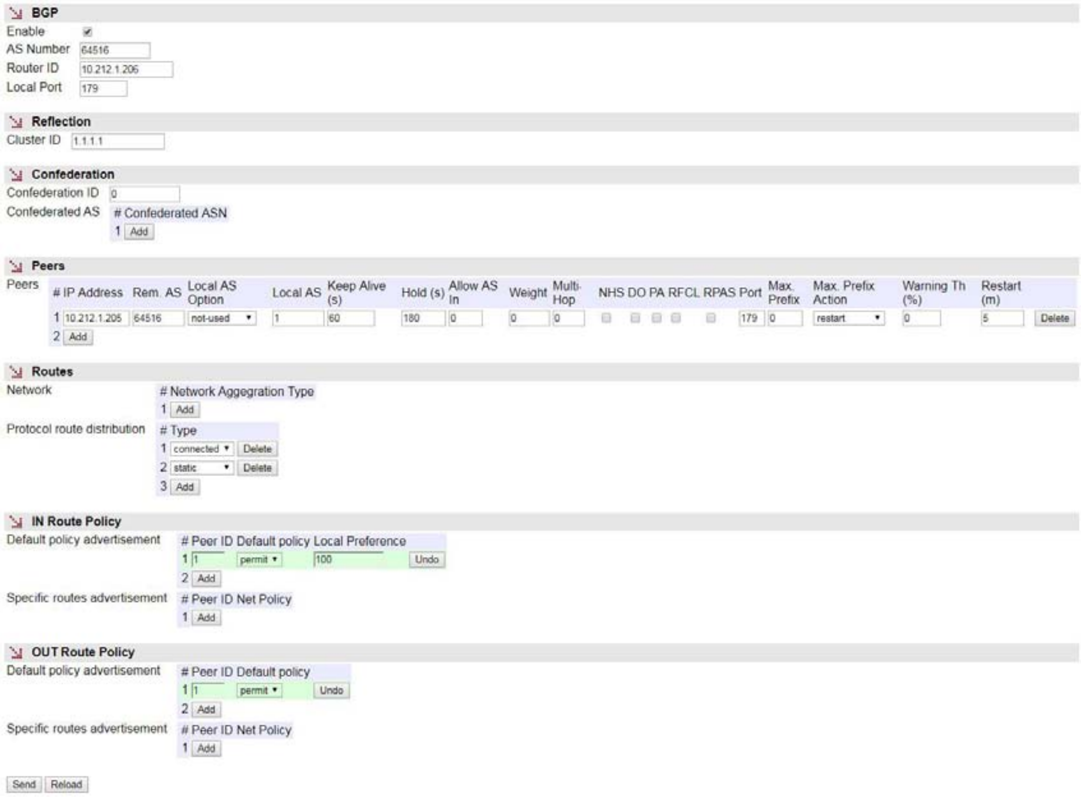
- **Only exceptions sent.** The general *reject* criteria option, with the exceptions selected in the respective section, which in this case would have the *permit* option enabled.

5.8.5 BGP Protocol

The equipment has the standard BGPv4 routing protocol.

The BGP protocol can be enabled or disabled by the user, through the Checkbox *Enable* control.

FIGURE 42 *BGP Protocol* submenu in the *Routing* menu



BGP

Enable ☑

AS Number: 64516

Router ID: 10.212.1.206

Local Port: 179

Reflection

Cluster ID: 1.1.1.1

Confederation

Confederation ID: 0

Confederated AS

#	Confederated ASN
1	Add

Peers

Peers

#	IP Address	Rem. AS	Local AS Option	Local AS	Keep Alive (s)	Hold (s)	Allow AS In	Weight	Multi-Hop	NHS	DO	PA	RFCL	RPAS	Port	Max. Prefix	Max. Prefix Action	Warning Th (%)	Restart (m)	
1	10.212.1.205	64516	not-used ▾	1	60	180	0	0	0	□	□	□	□	□	179	0	restart ▾	0	5	Delete
2	Add																			

Routes

Network

#	Network Aggregation Type
1	Add

Protocol route distribution

#	Type	
1	connected ▾	Delete
2	static ▾	Delete
3	Add	

IN Route Policy

Default policy advertisement

#	Peer ID	Default policy	Local Preference	
1	1	permit ▾	100	Undo
2	Add			

Specific routes advertisement

#	Peer ID	Net Policy
1	Add	

OUT Route Policy

Default policy advertisement

#	Peer ID	Default policy	
1	1	permit ▾	Undo
2	Add		

Specific routes advertisement

#	Peer ID	Net Policy
1	Add	

The group of parameters necessary to execute the protocol and its conditions are described below:

BGP:

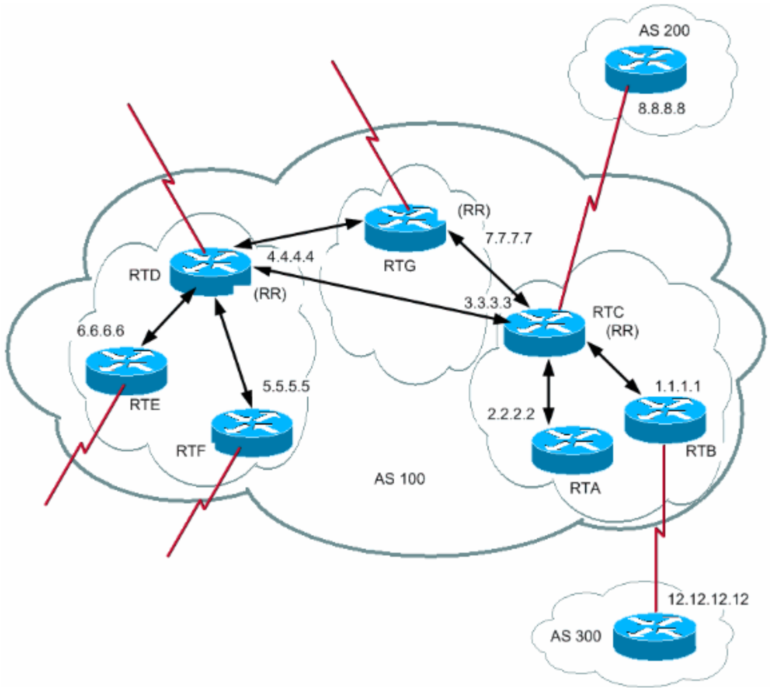
- **AS Number.** Identifies the AS of the router, usually referred to as ASN.
- **Router ID.** Identifies the equipment. Although the format coincides with that normally used for an IP address, it is really a digit to distinguish the routers executing the BGP protocol from each other. If it is not configured, that is, the default value remains 0.0.0.0, the highest IP address configured on the equipment is automatically assigned as a value.
- **Local Port.** Configuration of the local TCP port to be used for the BGP protocol. By default, it is the standard 179 port.

Reflection:

The BGP protocol requires a full-mesh type connection, that is to say, each of the routers of the same AS must establish a connection with each and every one of the routers with the same AS. In scenarios where the number of routers is large, the requirement is very demanding and involves a very high number of connections and therefore configuration. Therefore, there are provided mechanisms to avoid compliance of the same.

One of the simplification mechanisms is the use of the equipment as Route-Reflector. Client equipment are only connected to the router that acts as a Reflector. FIGURE 43 shows an example of three routers operating as Route-Reflectors, being RTC, RTD and RTG. In this scenario, RTD router has RTE and RTF as client routers, and RTC router has RTA and RTB. In turn, routers acting as Route-Reflectors are connected together in a full mesh.

FIGURE 43 Example of three routers operating as Route-Reflectors, being RTC, RTD y RTG



When it is desired that the equipment operates in a topology with Reflection, it is necessary to provide an identifier for the instance in the following parameter:

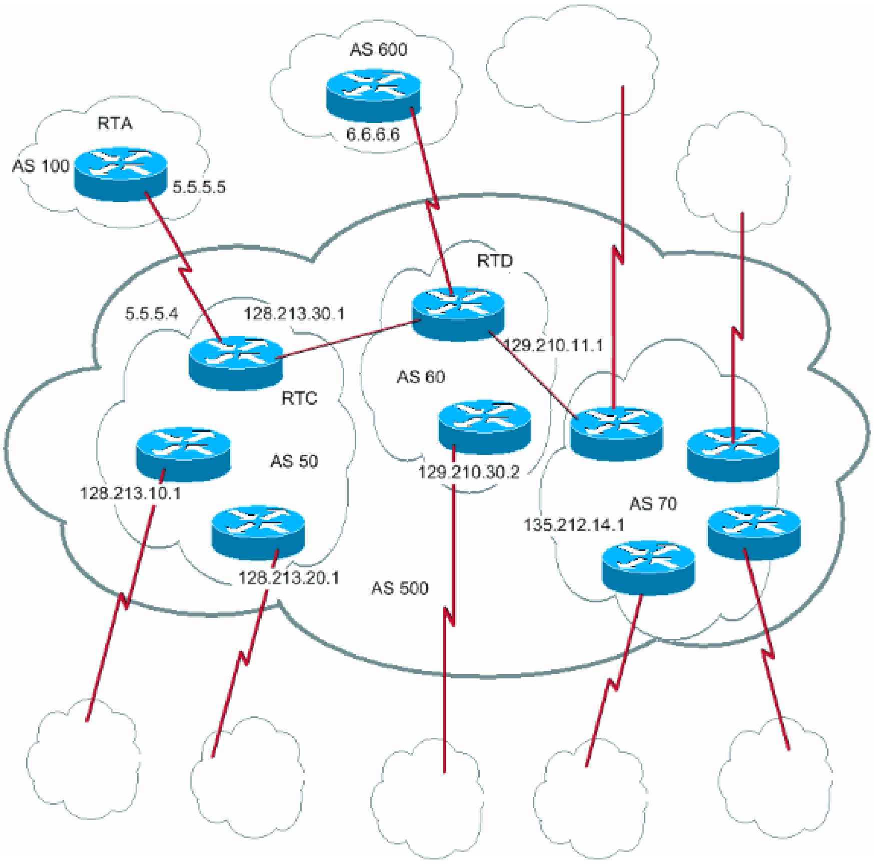
- **Cluster ID.** Identifier indicating that the equipment is included in a cluster, either as Route-Reflector or Client Router. A value 0 indicates that the equipment has not activated the Reflection mode.

> The equipment that behaves as a Route-Reflector is identified by having even devices with the same ASN and by having active the ***RFLC*** option activated, in the block in which the parameters are defined individually for each of the neighbouring devices configured.

Confederation:

Another mechanism that can reduce the requirement of full-mesh type connection between routers is the use of Confederations. Confederation allows subdivide an AS into subgroups with its own ASN, as shown in FIGURE 44, where the AS 500 is divided into the AS 50, AS 60 and AS 70.

FIGURE 44 Example of Confederations where the AS 500 is divided into the AS 50, AS 60 and AS 70



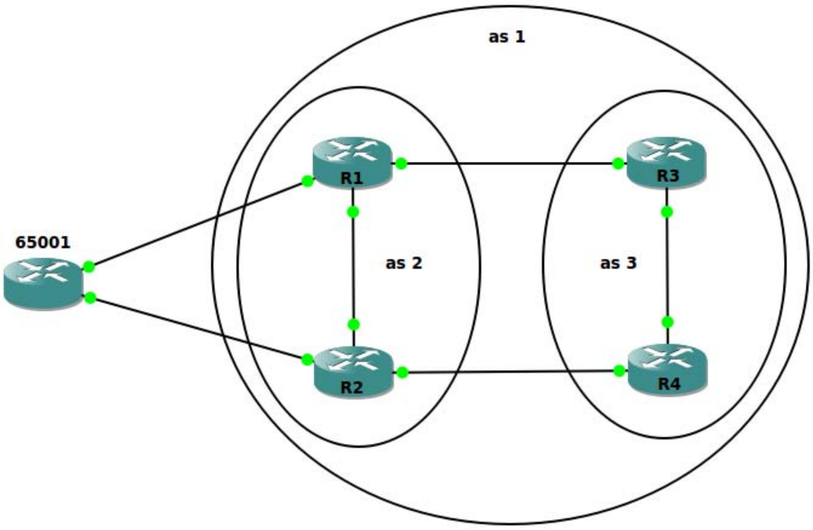
For the effective configuration of devices in Confederated mode the necessary parameters are:

- **Confederation ID.** Identifier that identifies the Confederation as a whole group.
- **Confederation AS.** ASN identifiers that form part of the Global Confederation identified by means of the previous parameter.

> In order for the Confederation be effective, the *Confederation ID* must be different from 0 and, at the same time, there must be at least one ASN configured in the *Confederation AS* table.

FIGURE 45 shows a much simpler example to identify the values that should be set up in each of the parameters.

FIGURE 45 Example of configuration of the Confederation parameters



For the R1 and R2 routers, values are:

AS Number: 2

Confederation ID: 1

Confederation AS: 3

For the R3 and R4 routers, values are:

AS Number: 3

Confederation ID: 1

Confederation AS: 2

> ! Note that the identifier of the Confederation (*Confederation ID*)
>
> coincides with the ASN of the complete set, while the ASN of the subgroup in which the router belongs is defined in the *AS Number* general parameter located in the configuration global zone.

Peers:

The neighbouring routers are configured in this block, as well as the specific parameter set for each one of them:

- **IP Address.** IP address of the neighbouring router.
- **Remote AS.** ASN identifier of the neighbouring router.
- **Local AS Option.** This sets the use of an alternative specific AS for the neighbouring router. It admits four possible values: ***not-used***, ***alternative***, ***no-prepend*** and ***replace-as***. The behaviour for each of the cases is as follows:
    - ***not-used***: The value of the *Local AS* parameter is not used in any way.
    - ***alternative***: The *Local AS* configured is put before the AS (AS PATH) sequence for the routes **received** from the neighbouring router, and is added to the sequence of AS for routes sent to the neighbouring router.
    - ***no-prepend***: The *Local AS* configured is only put before the AS sequence for the routes **sent** to the neighbouring router, but is NOT put before the AS sequence for the routes received.
    - ***replace-as***: In the routes **sent** to this neighbouring device, *the Local AS* configured is only put before the *AS* sequence.
- **Local AS.** Alternative specific AS for this neighbouring router.
- **Keep Alive.** This sets the period of time for sending the Keepalive messages. The units are seconds, and the default value is 60.
- **Hold.** This sets the maximum period of time without receiving Keepalive messages before declaring that the connection is unavailable. The units are seconds, and the default value is 180. The recommendation is that the Hold value be at least three times the Keepalive time.

- **Allow As In.** When the value is different from 0 the AS sequences will be accepted and with the own AS included the maximum number of times set in the parameter, being 10 the maximum.

- **Weight.** This sets a default weight for the routes received from this neighbouring router. A value of 0 indicates that the parameter is not in use.

- **Multi-Hop.** When a value greater than 0 is configured this establishes the maximum number of allowable hops for the established links with eBGP (exterior BGP) neighbouring devices that are not directly connected to the local networks of the router. The default value 0 implies that the TTL field of the BGP packets is 1 single hop. The maximum number is 255.

- **NHS.** When this option is active, the device indicates to the even equipment all non-local routes with its own IP address as the next hop.

- **DO.** This sets that the default route is sent to the neighbouring router when the route is known locally.

- **PA.** When it is *active* the opening messages are not sent to the neighbouring router but will behave in passive way, awaiting that the neighbouring router activates the connection.

- **RFCL.** Indicates to the router that the remote equipment is a client of the Route-Reflector server. This option is taken into account once the *Cluster* ID parameter is set.

- **RPAS.** This option indicates to the router that the private AS must be removed in output updates to the neighbouring router.

- **Port.** Configuration of the TCP port to be used to establish a connection to the neighbouring router. By default, it is the standard 179 port.

If there is a maximum number of prefixes that are accepted from the neighbouring router, there are several parameters that control the operation of the router. The router's response regarding the threshold overruns can be of two types: sending a warning or restarting the connection. In the last case, it is possible to establish a percentage of the limit that will act as a threshold when sending a warning, but it is optional.

- **Max Prefix.** Maximum number of prefixes that will be accepted from this neighbouring router.

- **Max Prefix Action.** It admits two values: ***warning-only*** and ***restart***. Sets the action to be adopted when the limit set in *Max. Prefix* is exceeded.

- **Warning Th.** Percentage regarding the maximum number of prefixes configured which, if exceeded, involves the sending of a warning. If the value is 0, the threshold option is not active. It makes sense to activate when the configured action is *restart*.

- **Restart.** If the action is *restart*, it sets the time since the limit is exceeded until the restart occurs. The units are minutes.

Routes:

In this section the networks that are advertised by the router, and the conditions with which these advertisements will be made are set:

- **Network.** Address of IP network. Admits the A.B.C.D/M format where M is the size of the mask, or the A.B.C.D/N.O.P.Q format.

- **Aggregation Type.** Controls how the network information of the previous parameter is advertised. It admits five values: ***no-aggregate***, ***aggregate***, ***as-set***, ***summary-only*** and ***as-set_sumary-only***. For all modes involving aggregation, only the route configured in update messages will be included when there is at least a real route that is included in the aggregated network. The behaviour of each of the options is as follows:

    - ***no-aggregate***: The network is advertised as it has configured.

    - ***aggregate***: Indicates that the network is advertised as aggregated type.

    - ***as-set***: Indicates that the network is advertised as aggregated type and that the AS group is created.

    - ***summary-only***: Indicates that the network is advertised as aggregated type and that the routes included in the aggregated network will be filtered so that will not be advertised.

    - ***as-set_sumary-only***: Indicates that the network is advertised as aggregated type and that the routes included in the aggregated network will be filtered so that will not be advertised, and that the AS group is created.

- **Protocol Route distribution**. This indicates the information the protocol must include, in addition to what is acquired through the protocol own messages. The origin of the information can be local addressing (*connected* option), static routes (*static* option) or other dynamic routing protocols (RIP and OSPF options).

The parameters that follow are used to control the filters that are applied to the input (IN) and output (OUT) routes for each of the neighbouring routers. The set of parameters necessary for the implementation of the protocol and its conditions are listed below:

In/Out Route Policy:

- **Peer ID.** Identifier of the neighbouring router. It corresponds to the index the system has automatically assigned at the time to its configuration. It may be modified if the ratio or order of neighbouring routers change.

- **Default policy.** This selects the general criteria, accept (***permit***) or reject (***deny***), and affects all the input/output routes that are not going to have more specific policies for the router identified with the previous parameter (Peer ID).

- **Local Preference.** It sets the value of the Local Preference parameter for the routes obtained from the even equipment identified as *Peer ID*. The default value is 100. Valid values are 0 to 4294967295.

In/Out Specific Route Advertisement:

- **Peer ID.** Identifier of the neighbouring router. It has the same criteria as for the establishment of general policies.

- **Net.** Network address to which it applies the filtering policy.

- **Policy.** Sets the action executed by the router for the network address selected, accept (***permit***) or reject (***deny***).

General criteria options combined with possible exceptions allow the input and output filters to behave in two ways for each of the remote routers:

- **Send all with exceptions.** Option of the *permit* general criteria, which is the default value, with the exclusions selected in the corresponding section, which in this case would have the *deny* option enabled.

- **Only exceptions sent.** Option of the *deny* general criteria, with the exceptions selected in the corresponding section, which in this case would have the *permit* option enabled.

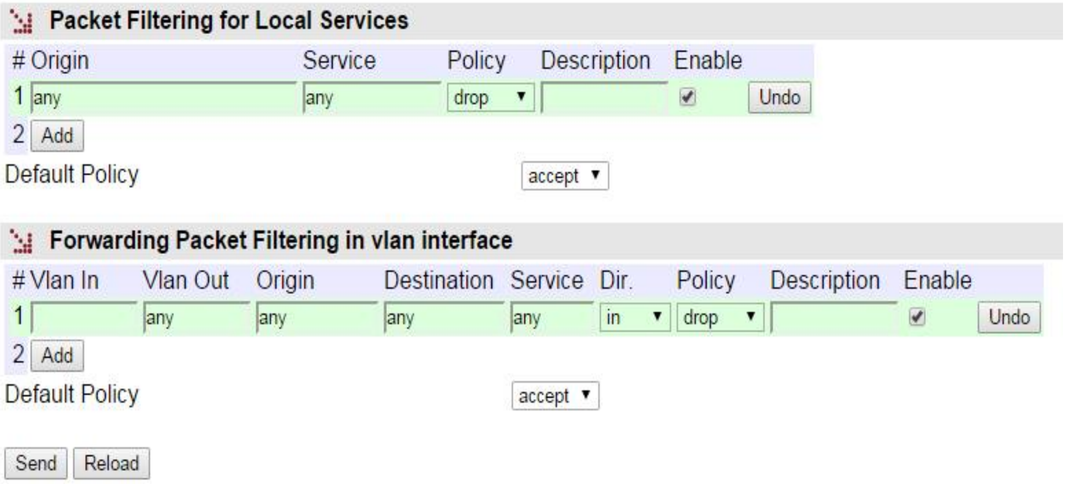
5.9 FILTERING CONFIGURATION

The *Filtering* menu permits IPv4 traffic filtering functionalities, defining which traffic is allowed and which traffic is rejected and the application of additional conditions to the traffic processed through the routing function.

The menu parameters are divided into two quite different blocks, which are:

- Filtering of packets for local services (for example: http, Telnet, etc.).
- Filtering of packets through the incoming/outgoing service for virtual interfaces associated with each VLAN that is defined.

FIGURE 46 *Filtering* menu



Packet Filtering for Local Services

#	Origin	Service	Policy	Description	Enable	
1	any	any	drop ▼		☑	Undo
2	Add					

Default Policy: accept ▼

Forwarding Packet Filtering in vlan interface

#	Vlan In	Vlan Out	Origin	Destination	Service	Dir.	Policy	Description	Enable	
1		any	any	any	any	in ▼	drop ▼		☑	Undo
2	Add									

Default Policy: accept ▼

Send Reload

The configuration parameters in each block are:

- **Origin.** This allows the IP source of the traffic to be specified, i.e., from a specific IP address or any IP address (**any**). The default value is **any.** The specification of a particular IP address requires the values to be entered in the IP address format. Example: Subnet (192.168.50.0/255.255.255.0 or 192.168.50.0/24) or Host (192.168.50.5/255.255.255.255 or 192.168.50.5/32 ó 192.168.50.5). Only present in the sections in which this makes sense.

- **Destination.** This allows the IP source of the traffic to be specified, i.e., to a specific IP address or from any IP address (**any**). The default value is **any.** The specification of a particular IP address requires the values to be entered in the IP address format. Example: Subnet (192.168.50.0/255.255.255.0 or 192.168.50.0/24) or Host (192.168.50.5/255.255.255.255 or 192.168.50.5/32 or 192.168.50.5).

- **Service.** This allows any type of traffic to be specified (**any**) or a specific traffic (**tcp/udp/icmp)**. The default value is **any.** If a specific traffic is indicated, the port number can be indicated together with the service, if required (1÷65535) or a range. Example: tcp or tcp:23 or udp:5001-5005.

- **Dir.** This allows the traffic way to be specified, i.e., whether it is incoming (**in**) or outgoing (**out**).
  in: incoming by Vlan In and outgoing by Vlan Out.
  out: incoming by Vlan Out and outgoing by Vlan In.

- **Policy.** This allows the filtering policy to be specified (**accept**, **drop** or **reject**). When the filtering policy is **accept**, only packets complying with the selected rule are accepted. When the filtering policy is **drop**, on the other hand, packets complying with the selected rule are dropped. The **reject** filtering policy also rules out packets complying with the selected rule, but unlike drop, when the packet is ruled out, the appropriate ICMP message is sent to the source address of the packet.

- **Description.** This permits a description of up to 15 alphanumerical characters to be specified.

- **Default Policy.** This allows the behaviour of the equipment filtering to be determined as regards not being included in any specific rule of the respective section.

- **Vlan In y Vlan Out.** Identifiers for the virtual interfaces. In this case allows the identification of traffic, generically, taking into account the input device or the one calculated as output, so that allows rules with generic character as it is independent from IP addressing.

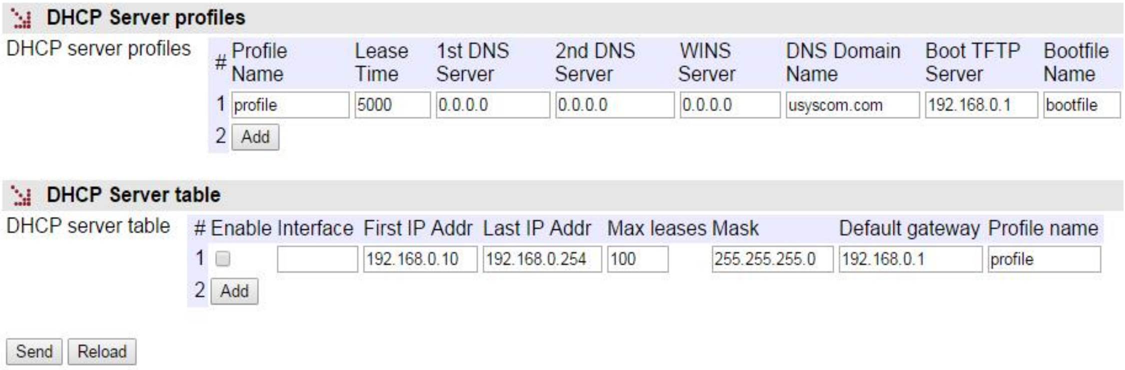
5.10 DHCP SERVER CONFIGURATION

The SW3-L3 has a built-in DHCP server which allows IP addresses to be assigned automatically to the equipment requesting this.

If the operation of DHCP assignment is carried out in a centralized way, rather than enabling a local DHCP server for the interface, requests are retransmitted according to the configuration set in the remote servers (DHCP relay, see section 5.3.2).

The local server supports multiple instances, so that it is possible to operate on several of the equipment virtual VLAN interfaces, each one with its own server.

FIGURE 47 *DHCP Server* menu



DHCP Server profiles

DHCP server profiles

#	Profile Name	Lease Time	1st DNS Server	2nd DNS Server	WINS Server	DNS Domain Name	Boot TFTP Server	Bootfile Name
1	profile	5000	0.0.0.0	0.0.0.0	0.0.0.0	usyscom.com	192.168.0.1	bootfile
2	Add							

DHCP Server table

DHCP server table

#	Enable	Interface	First IP Addr	Last IP Addr	Max leases	Mask	Default gateway	Profile name
1	□		192.168.0.10	192.168.0.254	100	255.255.255.0	192.168.0.1	profile
2	Add							

5.10.1 DHCP Server Profiles

Creating profiles allows the creation of sets of parameters that are common to different instances of the DHCP server, operating on different interfaces.

The parameters for configuring a profile are:

- **Profile Name.** Identifies a profile, defined as a set of parameters, in order to be easily shared by more than one instance of the server, avoiding the need for repetitive configuration.

- **Lease time.** This allows the time in seconds to be specified for an IP address to be assigned following a request from a DHCP client. After the indicated time, if the DHCP has not requested a renewal, the IP address will be considered available for dealing with new requests.

- **1st DNS server.** This allows the specification of the primary DNS server IP address which the DHCP server will provide to the DHCP client. If left blank (0.0.0.0) no information on DNS servers will be sent to the client.

- **2nd DNS server.** This allows the IP address of a secondary DNS server to be specified to the DHCP client. If left blank (0.0.0.0) this means that no information will be sent to the client in this respect.

- **WINS server.** This allows the IP address of the WINS server to be selected, which will be notified to the DHCP client. WINS is a name resolution system owned by Microsoft for equipment executing the Windows operating system.

- **DNS Domain Name.** This selects the DNS domain to be used by the client for creating its full DNS name.

- **Boot TFTP Server.** This selects the IP address of the TFTP server that stores the remote boot file, thereby allowing the client to execute a request to download the file.

- **Bootfile Name.** This selects the name of the remote boot file which the client will request from the TFTP server configured in the preceding point.

5.10.2 DHCP Server Table

The configuration parameters for each interface are:

- **Enable.** Enable the DHCP server. It should be marked if you want to use a DHCP server. DHCP Server will only run in interfaces with IP static address and no DHCP Relay agent enabled.

- **Interface.** This selects the interface where the client requests will be dealt with, based on the parameters defined below.

- **First IP Addr.** Allows the **first** IP address of the IP addresses pool managed by the DHCP Server in this interface to be specified.

- **Last IP Addr.** Allows the **last** IP address of the IP addresses pool managed by the DHCP Server in this interface to be specified.

- **Max leases.** Allows the maximum number of IP addresses simultaneously assigned in use to be specified.

- **Mask.** This selects the net mask that will communicate with the DHCP clients.
- **Default Gateway.** This selects the default router address (Default Gateway) that will communicate with the DHCP clients.
- **Profile name.** This selects which of the profiles defined in the above section must be applied to the requests served on this interface.

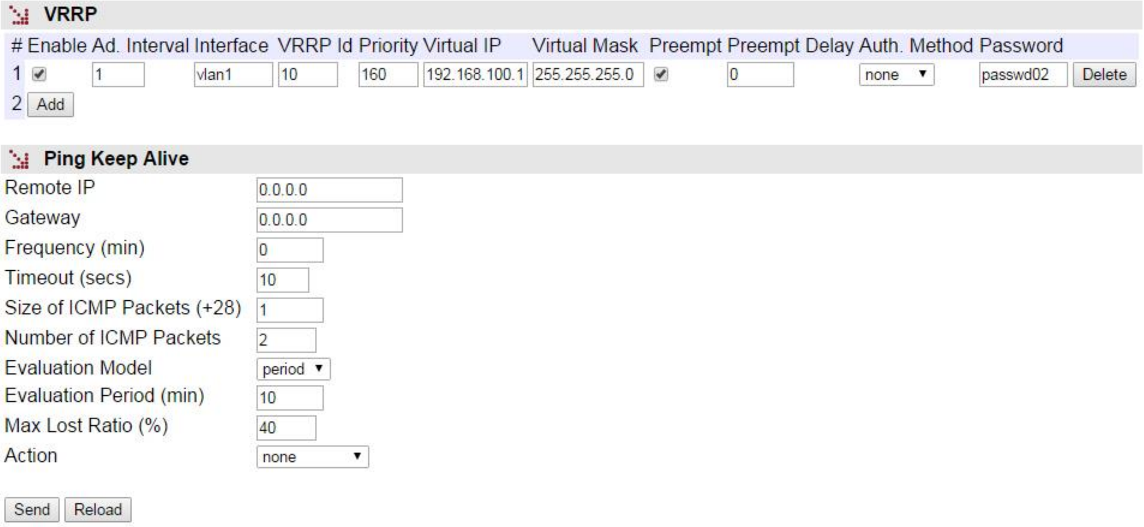
5.11 VRRP CONFIGURATION

In some environments the networks connect to each other through one router. This single router is therefore a potential failure point, which could disconnect a whole network from the rest.

The VRRP protocol permits several routers to be presented to clients with a common single virtual IP address, controlling the routers included in the virtual router, which is always the one that effectively provides the service, thereby providing redundancy to clients in a transparent manner. A master is selected from among all the routers, whereas the other routers act as backups in the case of the master one failing.

The master router regularly sends VRRP advertisement packets to the backup routers. If the backup routers do not receive the VRRP advertisement packets for a time that is three times the selected period, they assume that the master router has fallen and commence a process for selecting a new master.

FIGURE 48 VRRP menu



VRRP

#	Enable	Ad. Interval	Interface	VRRP Id	Priority	Virtual IP	Virtual Mask	Preempt	Preempt Delay	Auth. Method	Password	
1	☑	1	vlan1	10	160	192.168.100.1	255.255.255.0	☑	0	none ▾	passwd02	Delete
2	Add											

Ping Keep Alive

Remote IP	0.0.0.0
Gateway	0.0.0.0
Frequency (min)	0
Timeout (secs)	10
Size of ICMP Packets (+28)	1
Number of ICMP Packets	2
Evaluation Model	period ▾
Evaluation Period (min)	10
Max Lost Ratio (%)	40
Action	none ▾

The equipment supports the simultaneous execution of multiple instances of VRRP protocol. Each one is configured into an individual register, whose parameters are described below:

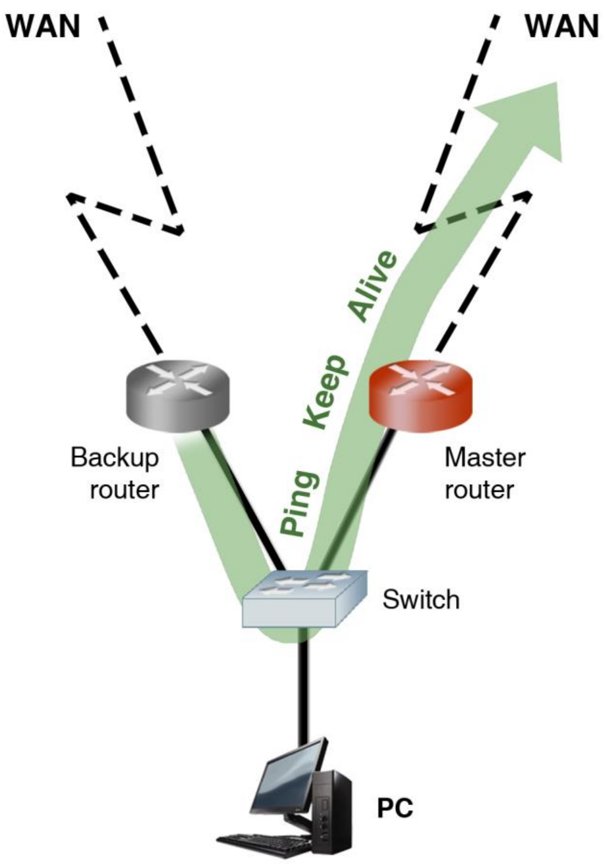
VRRP:

- **Enable VRRP.** Enables the execution of the protocol instance.
- **Advertisement Interval.** This selects the time in seconds to be used for either transmitting the VRRP advertisement packets when acting as a master or the basic time for supervising the master when it acts as a backup router. The default value is 1 second.
- **Interface.** It sets the logical interface (vlan) which runs the VRRP protocol.
- **VRRP Id.** The master router uses the address MAC 00:00:5E:00:01:XX, as set in the standard protocol, where XX is the Virtual Router IDentifier (VRID). The VRID allows a distinction to be made between the different virtual VRRP routers operating in the network. The parameter selects the VRID value. If, for example, VRID 3 is specified, the MAC virtual address will be 00:00:5E:00:01:03.
- **Priority.** This parameter sets the priority the router will present during the process for selecting the master router. Valid values are **1** to **254**. The master router is identified by using the priority 255, once the selection process has ended.
- **Virtual IP.** This sets the virtual IP address to be used by the client to access the routing service. It is common to all routers included in the virtual router.
- **Virtual Mask.** This sets the net mask associated with the IP address of the previous parameter.
- **Preempt.** This option means that if a backup router has a priority greater than the one granted to the master router selected, the equipment will force the change and declare it as the new master router as soon as it is included in the virtual router. A delay can be programmed for this action through the Preempt Delay parameter.
- **Preempt Delay.** This allows the time in seconds to be specified for the backup router with the higher priority to be converted into the master router.
- **Authentication Method.** This allows the authentication method for the physical routers included in the virtual VRRP router to be selected. The options are **PASS** (Password) and **AH** (Authentication Header), but it is also possible to operate without authentication, by selecting the option **none.**

- **Password.** This sets the password to be used in the event of selecting the authentication use.

Ping Keep Alive:

This option is configured between a backup router and the master router, and allows that a physical backup router to be chosen as router master when the supervision function fails.



- **Remote IP.** This sets the address of the external equipment (final destination) to be supervised. If the field value is 0.0.0.0 this means the function is disabled.
- **Gateway.** The IP address of the physical master router.
- **Frequency (minutes).** This sets the frequency with which the supervision messages will be transmitted.
- **Timeout (secs).** This allows the maximum response time to the ICMP (ping) packets sent by the *Ping Keep Alive* function to be specified. Valid values are **5** to **60**.

- **Size of ICMP packets.** This allows the size of the ICMP packet to be specified. The configuration consists of indicating the extra bytes to be added to the smallest ICMP packet, which is, by default, 28 bytes.
- **Number of ICMP packets.** This allows the number of ICMP packets that are sent in each verification to be specified.
- **Evaluation Model.** This sets the model for the evaluation of the accessibility test. The options are: **single** and **period**. The **single** model specifies that, if some execution of the test fails, the behaviour of the equipment is the one defined in the **Action** parameter. The **period** model specifies, by means of the two following parameters, a test evaluation period and an admitted failure percentage within it.
- **Evaluation Period (min).** When the Evaluation Model parameter is configured as **period,** this sets a period between **1** and **6000.** All the responses to the *Ping Keep Alive* packets sent in this period make the universe of samples that will be considered to decide about the execution of *Action* according to the fulfilment of the criteria selected by means of the following parameter.
- **Max Lost Ratio (%).** This allows the maximum admitted percentage of failure in the Evaluation period to be specified for the results of the Ping Keep Alive messages.
- **Action.** This selects the desired behaviour of the equipment when the supervision function fails. The available actions are: **None** (no action taken) or **vrrp2master** (forcing priority to 255).

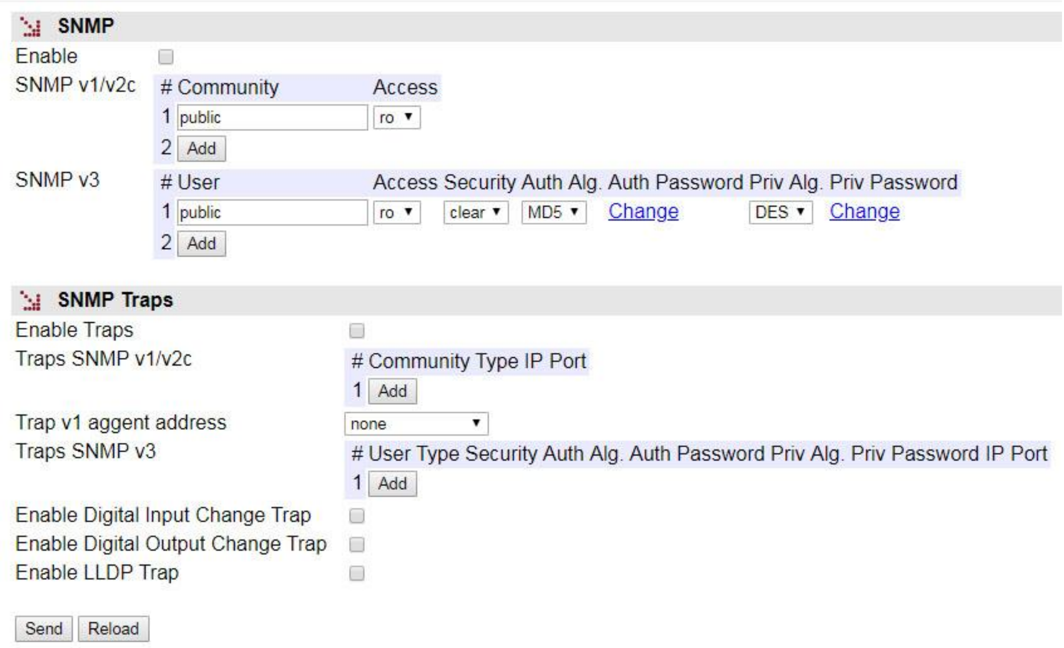
5.12 SNMP CONFIGURATION

The equipment has an SNMP agent with the capacity to generate spontaneous messages to control devices, based on that protocol.

The agent admits the emitting of messages based on the SNMPv1 [3], SNMPv2c [4] and SNMPv3 protocol, and the selection of the type of message, *trap* and *inform*.

> Changes made to the SNMP agent configuration will **only** be active after **RESETTING** the equipment. The ***Apply*** command is not sufficient, and so the changes must previously be saved using the ***Save*** command before requesting the reboot.

FIGURE 49 ***SNMP*** menu configuration page



SNMP

Enable □

SNMP v1/v2c

#	Community	Access
1	public	ro ▾
2	Add	

SNMP v3

#	User	Access	Security	Auth Alg.	Auth Password	Priv Alg.	Priv Password
1	public	ro ▾	clear ▾	MD5 ▾	Change	DES ▾	Change
2	Add						

SNMP Traps

Enable Traps □

Traps SNMP v1/v2c

#	Community	Type	IP	Port
1	Add			

Trap v1 aggent address: none ▾

Traps SNMP v3

#	User	Type	Security	Auth Alg.	Auth Password	Priv Alg.	Priv Password	IP	Port
1	Add								

Enable Digital Input Change Trap □

Enable Digital Output Change Trap □

Enable LLDP Trap □

The configuration parameters are:

SNMP:

- **Enable.** Enables/disables the execution of the SNMP agent. The agent is operative when the option is selected.

- **Community.** Parameter associated with SNMPv1/v2c. Tabulate information that allows several operating profiles to be defined, including the rights of access (Access) associated with each one, read only rights (*ro*) or reading/writing rights (*rw*). The profiles are called *communities*.

- **User.** Parameter associated with SNMPv3. Tabulate information that allows the users, including the privileges and the operation mode associated with each user, to be defined. That is to say, the rights of access (Access), read only rights (*ro*) or reading/writing rights (*rw*), and the way in which the data transference (Security) will be carried out, without encryption (*clear*), authentication (*auth*) or authentication and encryption (*priv*).

  In case of authentication transmission (*auth*), it is necessary to select the type of algorithm (*Auth Alg*.), MD5 or SHA, and set the authentication password (*Auth Password*). The password set the word to be used to generate the authentication information. The authentication word must be known by the receiver in order to be able to verify the authenticity of the identity of the transmitter.

In case of encrypted transmission (*priv*), in addition to select the type of authentication algorithm (*Auth Alg*.) and authentication password (*Auth Password*), it is necessary to select the cipher algorithm (*Priv Alg*.), DES o AES, and select the cipher password (*Priv Password).*

The password is not shown for security reasons and so when it is changed (**Change** option), it must be entered twice.

> Once the **Password** is introduced from the **Change** option, execute the **send** command of said option, and then, if you want the password to be applied and saved in the equipment, **DO NOT forget** to execute the **apply** and **save** commands from the main menu tree.

SNMP Traps:

- **Enable Traps.** Enables/disables the generation and transmission of spontaneous messages by the SNMP agent. The agent will send messages of the different events when the option is selected.

- **Traps SNMPv1/v2c.** Tabulate information allowing several destination devices for the *traps* to be defined.
  For each of the spontaneous SNMP message addressees, a profile must be provided, which must be included in the spontaneous message, the SNMP protocol version with which it will be coded, the IP address of the addressee and the UDP port to which the messages will be sent. The default value set in the standard is port 162. It can be changed to adapt to the operating data of each addressee.
  The transmission of the messages in a confirmed (*inform*) way is only accepted for the v2c and v3 versions of the protocol.

- **Trap v1 agent address.** This sets the IP address the agent will communicate as being its own when sending spontaneous messages. This parameter is only used to create the traps when using SNMPv1.

- **Traps SNMPv3.** Tabulate information allowing several destination devices for the notifications to be defined.
  The receivers are identified by means of their IP address and the UDP port to which the notifications are to be sent. The standard UDP port for the SNMP notifications is the 162, being the default value.
  The *Type* control is used to set whether the transmission of the notifications is carried out in an unconfirmed (*trap*) or confirmed (*inform*) way.

- **Enable Digital Input Change Trap.** Enables/disables the transmission of SNMP spontaneous messages indicating the status changes of the digital input.
  The digital input corresponds to pins 4 and 5 of the I/O connector.

- **Enable Digital Output Change Trap.** Enables/disables the transmission of SNMP spontaneous messages indicating the status changes of the digital output.
  The digital output corresponds to pins 1 and 2 of the I/O connector.

> If the digital output is configured as Alarm, the SNMP messages associated with its changes are not sent although the configuration indicates that should be done.

- **Enable LLDP Trap.** Indicates the SNMP agent whether the notifications created by the LLDP agent are allowed or not.

5.13 STP PROTOCOL CONFIGURATION

The Spanning Tree Protocol, in both its original version (STP) and the improved version (RSTP) has the objective of identifying potential loops in level 2 networks, so that the different devices can communicate with each other and set whether the different interfaces in each will be active for switching client traffic, or on the contrary, whether they will be used as backups in case of potential topological changes. The final result is that the active interfaces of each device end up forming a tree structure with no loops from the root device.

> If the device is to be included in a level 2 network interconnected to other switching devices and there is a possibility of loops being created (depending on the connection topology), it is ESSENTIAL to activate the Spanning Tree Protocol.

The specific device configuration parameters are:

- **Enable.** A simple checkbox parameter to set whether the STP must be executed or not.

- **Version.** This sets which of the possible protocol versions will be executed. STP or RSTP (Rapid STP).

- **Bridge Priority.** This sets the priority of the device communicating with the root device.

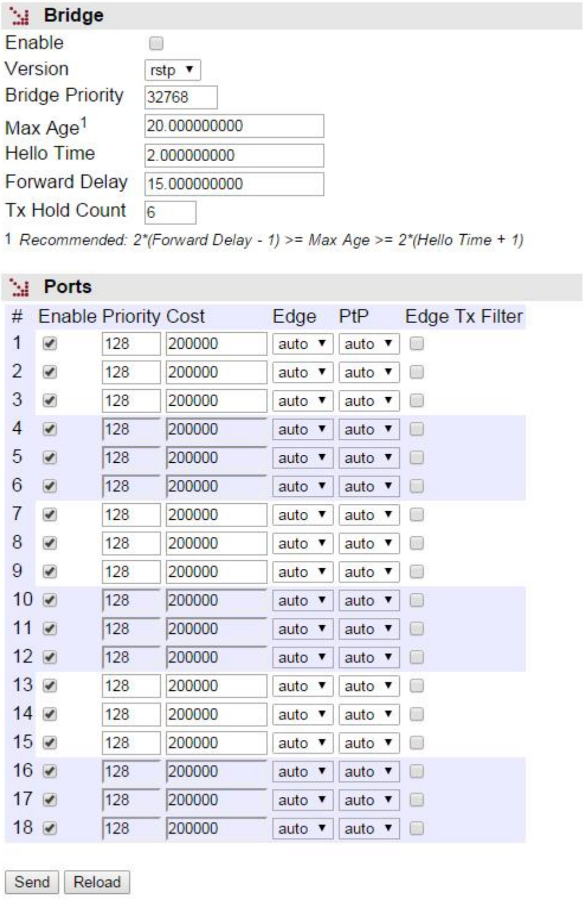
- **Max Age.** The maximum time during which the device considers the last BPDU message received as valid. In the case of the stipulated time expiring, the device assumes there has been a topological change and initiates the topological change communication process. The default value is 20 seconds, and valid values are 6 to 40 seconds.

- **Hello Time.** This parameter sets the time between sending BPDU messages (the STP protocol messages). The default and maximum value is 2 seconds.

- **Forward Delay.** This parameter is the maximum period of time for an interface to be in the listening and learning states. The default value for this period is 15 seconds, and valid values are 4 to 30 seconds.

- **Tx Hold Count.** This sets the maximum number of BPDU packets that can be transmitted in one second. The default value is 6 and valid values are 1 to 10.

FIGURE 50 **STP** menu configuration page



Bridge

Enable	□
Version	rstp ▾
Bridge Priority	32768
Max Age[1]	20.000000000
Hello Time	2.000000000
Forward Delay	15.000000000
Tx Hold Count	6

[1] Recommended: 2*(Forward Delay - 1) >= Max Age >= 2*(Hello Time + 1)

Ports

#	Enable	Priority	Cost	Edge	PtP	Edge Tx Filter
1	☑	128	200000	auto ▾	auto ▾	□
2	☑	128	200000	auto ▾	auto ▾	□
3	☑	128	200000	auto ▾	auto ▾	□
4	☑	128	200000	auto ▾	auto ▾	□
5	☑	128	200000	auto ▾	auto ▾	□
6	☑	128	200000	auto ▾	auto ▾	□
7	☑	128	200000	auto ▾	auto ▾	□
8	☑	128	200000	auto ▾	auto ▾	□
9	☑	128	200000	auto ▾	auto ▾	□
10	☑	128	200000	auto ▾	auto ▾	□
11	☑	128	200000	auto ▾	auto ▾	□
12	☑	128	200000	auto ▾	auto ▾	□
13	☑	128	200000	auto ▾	auto ▾	□
14	☑	128	200000	auto ▾	auto ▾	□
15	☑	128	200000	auto ▾	auto ▾	□
16	☑	128	200000	auto ▾	auto ▾	□
17	☑	128	200000	auto ▾	auto ▾	□
18	☑	128	200000	auto ▾	auto ▾	□

The configuration parameters for each port are:

- **Enable.** It sets whether the STP protocol configured in the interface is executed or not. Only makes sense if the Enable *CheckBox* corresponding to general execution is active.

- **Priority.** This sets the port priority. If there are two or more ports with one cost, the priority allows the root port of the equipment to be selected.

- **Cost.** This sets the cost associated with the port. Selecting the root port of the equipment is directly related to the lower cost of the different ports in relation to the root equipment.

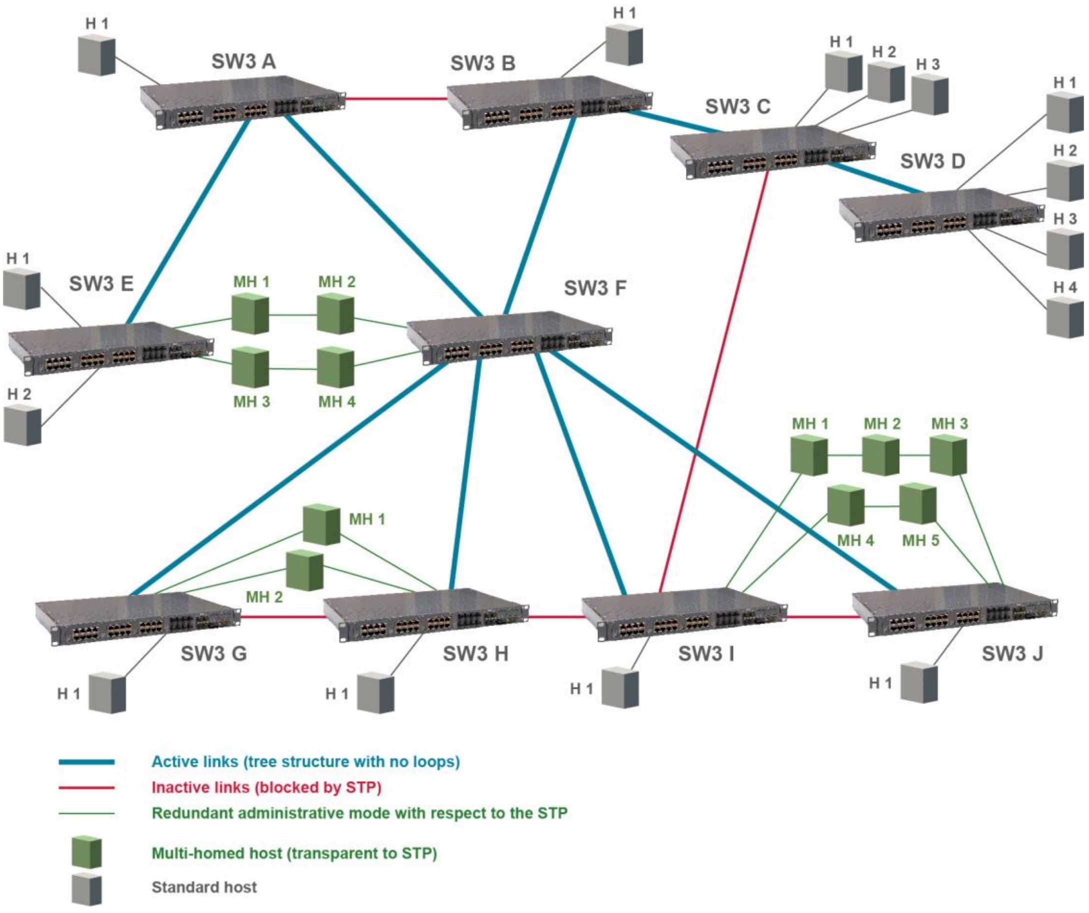
- **Edge.** This parameter sets the administrative mode of the interface with respect to the STP. Interfaces connected to client devices, i.e., devices that are not level 2 switching units and which therefore do not execute STP or give rise to the creation of loops may be booted directly to a traffic transmission situation (**on** mode). Interfaces that are directly connected to level 2 switching devices and are therefore prone to close loops must be booted in the accept user traffic mode (**off** mode).
  A third mode exists, **auto**, in which the equipment determines the presence or absence of level 2 switching devices connected to the interface. This is useful in cases in which the type of devices to be connected is not known.
  The last and fourth mode, **redundant**, is specifically designed for pairs of switches with multiple links due to chains of multi-homed client devices. The **redundant** mode allows the connection of client devices with more than one network interface in use connected to different switches and are transparent to STP, so that the interconnected switches can identify each other while giving access to the client devices. The **redundant** ports act as redundant links for access to client devices, but not as redundant links in terms of network topology. See an example of the **redundant** mode in FIGURE 51.
  Even when the **Edge** parameter is **on**, the switch maintains activated the detection of other switch connection to the interface, so operating state can become **off**.
  The operation mode of the interface, **on** or **off**, is shown in the STP statistics section.

- **PtP.** The PtP parameter sets whether the interface is directly connected to other level 2 switching equipment on an end-to-end link (**on** value) or not (**off** value) but the equipment is also capable of detecting that situation (**auto** value). If the equipment indicates that a link is PtP, this allows greater speed in protocol convergence, and the agreement process on changing the state of a link from *designated* to *non-discarding (*operative for user traffic) is speeded up.

- **Edge Tx Filter.** When the RSTP protocol is executed, this parameter allows the user to enable a filter that avoids the transmission of STP BPDU packets in the interfaces operating in **edge** mode. This parameter is only effective when the operating state of the interface is **edge**, and this situation is only possible when the **Edge** parameter is configured as **on** or **auto**.

> ! Switch interconnection **using interfaces with Edge at ON and Edge_Tx_filter active** lead to switches **being unable to detect** the connection as part of a loop.

FIGURE 51 Example of the **redundant** mode of the interface with respect to the STP


H 1
SW3 A
SW3 B
H 1
H 1
H 2
H 3
SW3 C
H 1
H 2
SW3 D
H 3
H 4
H 1
SW3 E
MH 1
MH 2
SW3 F
H 2
MH 3
MH 4
MH 1
MH 2
MH 3
MH 1
MH 4
MH 5
MH 2
SW3 G
SW3 H
SW3 I
SW3 J
H 1
H 1
H 1
H 1
Active links (tree structure with no loops)
Inactive links (blocked by STP)
Redundant administrative mode with respect to the STP
Multi-homed host (transparent to STP)
Standard host

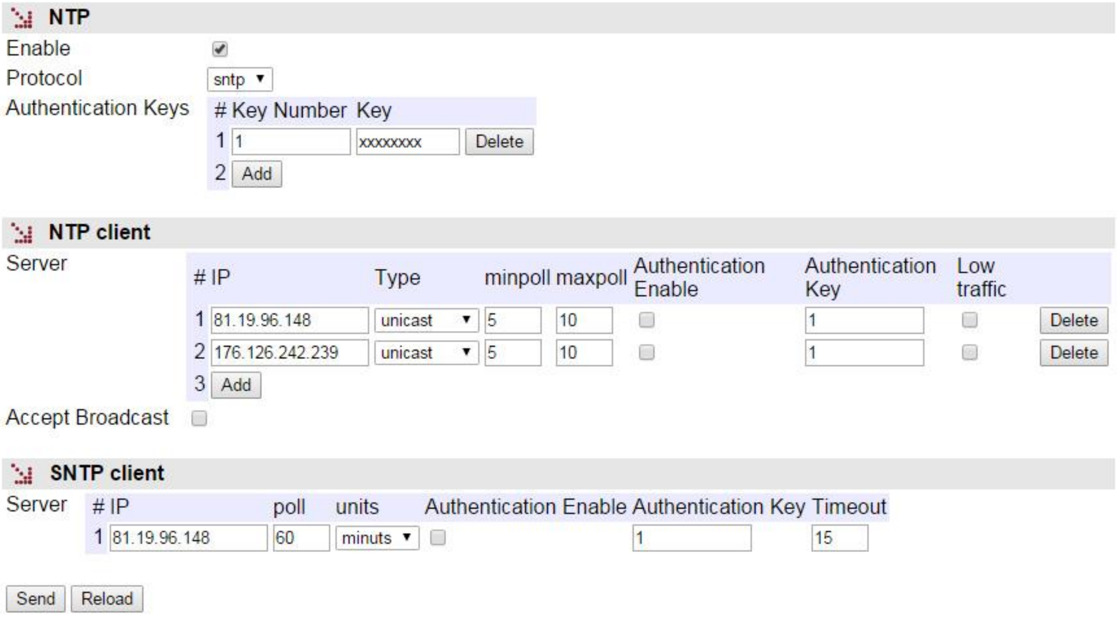
5.14 NTP/SNTP CONFIGURATION

The equipment has an NTP/SNTP client, meaning that it can synchronise time-related information by accessing NTP servers. The NTP [5] protocol is a standard that is widely used in TCP/IP-based networks. It admits the use of several NTP servers simultaneously, and the option of using authentication.

The SNTP variant means a faster synchronization but less accurate and, on the other hand, it is necessary to run it periodically.

The NTP/SNTP client will only act if the PTP synchronization option is disabled (see 5.15).

FIGURE 52 ***NTP/SNTP*** menu configuration page



NTP

Enable ☑

Protocol: sntp ▾

Authentication Keys

#	Key Number	Key	
1	1	xxxxxxxx	Delete
2	Add		

NTP client

Server

#	IP	Type	minpoll	maxpoll	Authentication Enable	Authentication Key	Low traffic	
1	81.19.96.148	unicast ▾	5	10	□	1	□	Delete
2	176.126.242.239	unicast ▾	5	10	□	1	□	Delete
3	Add							

Accept Broadcast □

SNTP client

Server

#	IP	poll	units	Authentication Enable	Authentication Key	Timeout
1	81.19.96.148	60	minuts ▾	□	1	15

The general usage parameters are:

- **Enable.** Enables/disables the execution of the NTP client. The client is operative when the option is selected.
- **Protocol.** This sets whether the NTP or SNTP client is used.

- **Authentication keys.** Tabulate information allowing the definition of different authentication codes to be used subsequently in communicating with the different NTP servers.

The NTP client supports the configuration of multiple NTP servers to carry out synchronization. Each has a set of customized parameters that determine the access procedure:

- **IP.** IP address of the NTP server.
- **Type.** This sets the type of messages to be sent to the NTP server. The messages can be individual (*unicast*) or collective (*manycast*).
- **Minpoll.** Minimum time between requests. The parameter is the exponent of the power of 2 that corresponds to the minimum period.
- **Maxpoll.** Maximum time between requests. The parameter is the exponent of the power of 2 that corresponds to the maximum period.
- **Authentication Enable.** This sets whether messages should be sent with authentication information.
- **Authentication Key.** If the previous option is enabled it determines which of the authentication keys defined in the previous block is used to authenticate the message.
- **Low Traffic.** Minimizes the use of the bandwidth that is used for the synchronization messages.

There is an additional parameter not dependent on the configuration of NTP servers that sets whether broadcast NTP-type messages will be accepted.

- **Accept broadcast.** Enables the acceptance of NTP messages that are received with broadcast address.

The SNTP client only supports the configuration of a server, and the necessary parameters are:

- **IP.** IP address of the NTP server.
- **Poll.** This sets the period of generation of synchronization messages. Valid values are 1 to 60.

- **Units.** Time unit for the period of generation of synchronization messages. It can be minutes or hours.

- **Authentication Enable.** This sets whether messages should be sent with authentication information.

- **Authentication Key.** If the previous option is enabled it determines which of the authentication keys defined in the previous block is used to authenticate the message.

- **Timeout.** Maximum waiting period for receiving response to transmitted synchronization messages. Valid values are 1 to 15 seconds.

5.15 PTP CONFIGURATION

The ***PTP*** menu is only useful when the SWT-L3 is equipped with PTP ports.

The equipment supports the IEEE 1588v2 (PTP) protocol according to Power Profile in 2-step mode, although it accepts 1-step and converts automatically to 2-step.

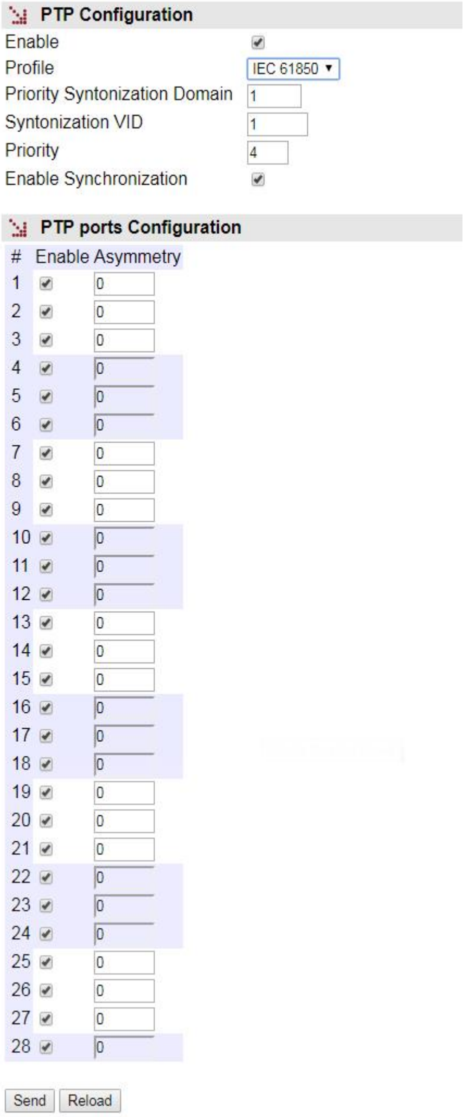
When the PTP protocol is in execution, the user can individually configure the execution of the protocol in each of the ports.

The equipment supports tuning, although it only does it with the PTP messages of a specific PTP domain and a specific VID, of the many that it can send; both the PTP domain and the VID are configurable parameters. The calculated tuning will be used to adjust all the corrections calculated by the equipment, regardless of the PTP domain and/or the VLAN to which they belong.

In the PTP messages, typical of the Peer-to-Peer mode, for the calculation of the line delay, the same PTP and VID domain will always be used as the one configured for tuning, as well as the established 802.1p priority.

As optional feature, the equipment can be synchronized at hour level from the PTP messages with which the tuning is performed, although the equipment never behaves as a PTP client.

FIGURE 53 ***PTP*** menu configuration page



PTP Configuration

Enable	☑
Profile	IEC 61850 ▾
Priority Syntonization Domain	1
Syntonization VID	1
Priority	4
Enable Synchronization	☑

PTP ports Configuration

#	Enable	Asymmetry
1	☑	0
2	☑	0
3	☑	0
4	☑	0
5	☑	0
6	☑	0
7	☑	0
8	☑	0
9	☑	0
10	☑	0
11	☑	0
12	☑	0
13	☑	0
14	☑	0
15	☑	0
16	☑	0
17	☑	0
18	☑	0
19	☑	0
20	☑	0
21	☑	0
22	☑	0
23	☑	0
24	☑	0
25	☑	0
26	☑	0
27	☑	0
28	☑	0

The configuration parameters are divided into two quite different blocks, which are:

PTP Configuration:

- **Enable.** Enables or disables the execution of the PTP protocol.
- **Profile.** It only supports the **IEC 61850** value, which selects the PTP operation according to the “Power Profile” (according to IEEE Std C37.118.1-2011 standard).
- **Priority Syntonization Domain.** It sets the PTP domain that the equipment will use for the identification of the PTP messages of the SYNC type that will be used for the tuning, and it will also be the PTP domain included in the PTP messages of the mechanism for the calculation of the Peer Delay created by the equipment.

- **Synchronization VID.** It sets the VLAN identifier that the equipment will use for the identification of the PTP messages of the SYNC type that will be used for the tuning, and it will also be the VID included in the PTP messages of the mechanism for the calculation of the Peer Delay created by the equipment.

- **Priority.** It sets the 802.1p priority to be included in the transmitted PTP messages, including the PTP messages of the mechanism for calculating the Peer Delay created by the equipment.

- **Enable Synchronization.** It sets that the equipment must be synchronized using the PTP protocol. Only messages belonging to the VLAN and PTP domain configured for tuning will be taken into account. It has priority over the NTP/SNTP client.

PTP ports Configuration:

- **Enabled.** It sets in each of the ports if the PTP protocol will be executed or not.

- **Asymmetry.** The equipment allows the user to configure an individualized time asymmetry value for each of the ports.

5.16 MULTICAST CONFIGURATION

Under normal conditions, multicast traffic propagates automatically on all interfaces belonging to each VLAN, with client devices that selectively enable the reception of specific multicast addresses in which they are interested.

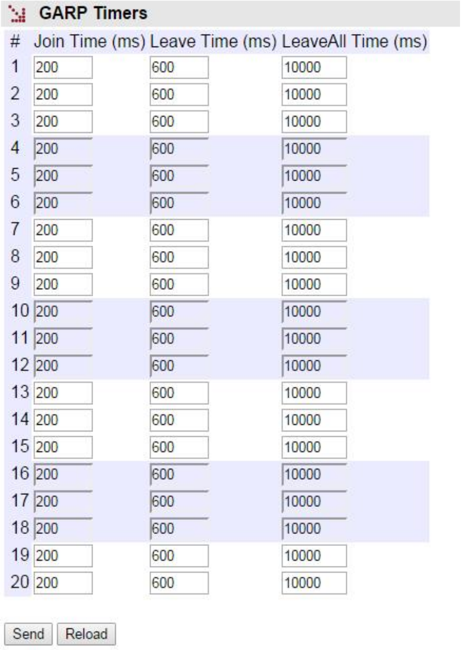
The switch has mechanisms to control the spread of multicast traffic, so not to spread on all ports. One mechanism is by explicit and manual configuration, that is, by configuring static entries with the multicast address of interest and the ports to which the corresponding traffic must be transmitted.

There are other mechanisms different from manual configuration. These use standard protocols to obtain the identification of the desired ports by each of the possible multicast flows. The protocols are GARP/GMRP and IGMP.

The GARP/GMRP is a layer 2 protocol, and operates by explicit register of the client devices in the network switches.

GARP is a base protocol on which GMRP operates. GARP requires the configuration of timers (see FIGURE 54).

FIGURE 54 ***GARP Timers*** menu configuration page



GARP Timers

#	Join Time (ms)	Leave Time (ms)	LeaveAll Time (ms)
1	200	600	10000
2	200	600	10000
3	200	600	10000
4	200	600	10000
5	200	600	10000
6	200	600	10000
7	200	600	10000
8	200	600	10000
9	200	600	10000
10	200	600	10000
11	200	600	10000
12	200	600	10000
13	200	600	10000
14	200	600	10000
15	200	600	10000
16	200	600	10000
17	200	600	10000
18	200	600	10000
19	200	600	10000
20	200	600	10000

The IGMP is layer 3 protocol, and message exchange of reception requests for multicast flows takes place between the client devices and the IGMP routers. In this case, the messages are spied by the switch to adapt the configuration of each port (IGMP Snooping). For the IGMP Snooping to be operative, the GARP/GMRP must be inactive.

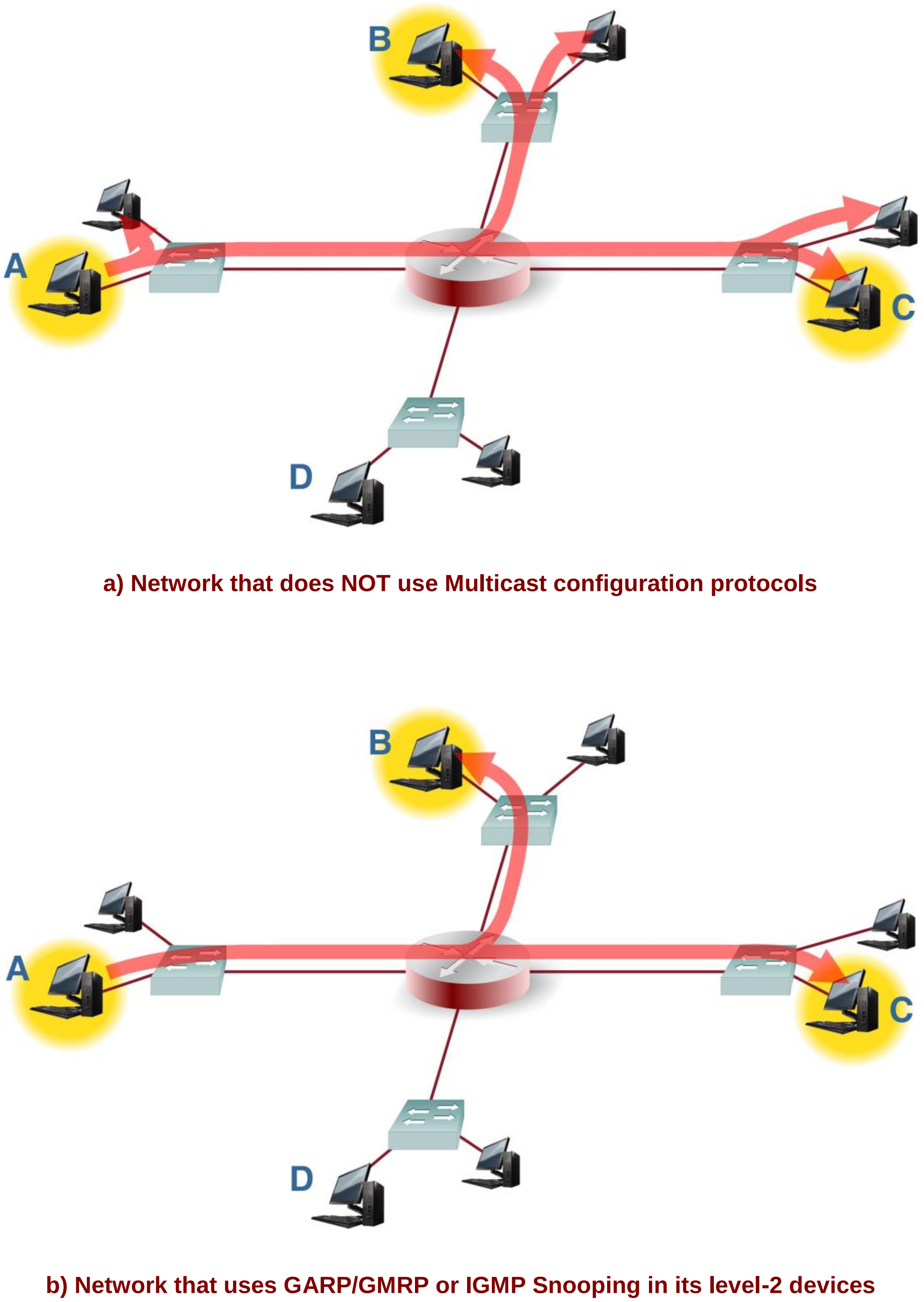
Activation of any of these mechanisms necessarily implies that the switch shall forward the multicast traffic only included in the manual configuration or requested by client devices. Any other multicast traffic will be discarded.

As an example, FIGURE 55 shows the advantages of using GARP/GMRP or IGMP Snooping.

FIGURE 55a) shows a network made up by four level-2 switches, which in turn are connected to a router. Host A is a multicast message emitter, and the Hosts B and C are multicast receivers belonging to the same group as the Host A. The router will route the multicast traffic only to the network sections where the Hosts B and C are found, while the level-2 switches will transmit traffic to all the hosts connected to their interfaces by flood.

FIGURE 55b) shows a network using the GARP/GMRP or IGMP Snooping mechanism in its level-2 devices. As shown in the figure, in this case only the hosts that belong to the diffusion group receive the multicast traffic.

FIGURE 55 Example of using the GARP/GMRP or IGMP Snooping



a) Network that does NOT use Multicast configuration protocols

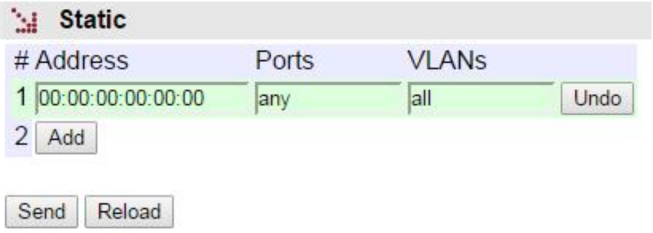
b) Network that uses GARP/GMRP or IGMP Snooping in its level-2 devices

5.16.1 Static

By means of this option, the user can manually configure the interfaces that will propagate each of the indicated multicast MAC addresses.

In networks with multiple switches, the configuration must be done in each of them.

FIGURE 56 ***Static*** configuration page of ***Multicast*** menu



Static

#	Address	Ports	VLANs	
1	00:00:00:00:00:00	any	all	Undo
2	Add			

The parameters for creating the list of multicast MACs are the following:

- **#.** Tabulate element identifier. Not relevant.
- **Address.** The multicast MAC address.
- **Ports.** Port(s) that will transmit traffic with multicast MAC address. A group of discreet ports is configured with the identifier of each one, separated by a comma, without spaces. If a range is to be included, the initial and final port identifiers are separated by a dash. The value **any** means the port is not relevant.
- **VLANs.** Numeric identifier of the VLANs defined on the equipment on which the MAC address will be transmitted (VID fields in the ***VLANs*** menu). A group of discreet vlans is configured with the identifier of each one, separated by a comma, without spaces. If a range is to be included, the initial and final vlan identifiers are separated by a dash. The value **all** means the vlan is not relevant. Example: in equipment with the **vlan1**, **vlan3** and **vlan4** defined, the group of numerical identifiers will be **1,3,4**.

> The presence of identifiers in the **Ports** parameter and **VLANs** section is not exclusive. If values for both parameters are specified, the configuration is applied at the indicated ports that also meet the requirement of belonging to VLANs configured.
>
> The **trunk** type ports are considered to belong to all vlans, so it should only be included when the **Ports** parameter has values different to **any**.

5.16.2 GMRP

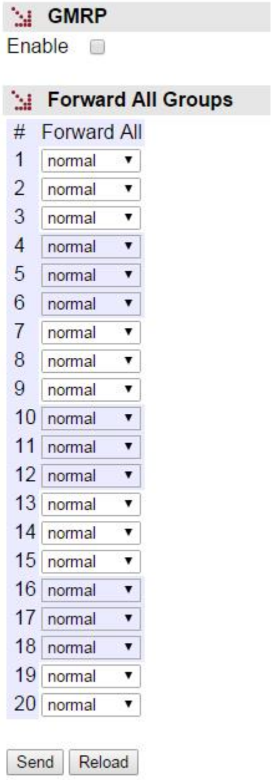
The GMRP protocol is designed in order for the switches fit the multicast data transmission based on requests issued by customers in each of the interfaces.

> However, the protocol is able to manually set the transmission of multicast addresses, so that client devices that are not running the protocol can operate properly. This option is performed by configuring the registers of the *Static* zone.

> Unlike purely manual operation, the execution of the protocol involves the automatic propagation of application manually set towards the rest of the switches in the network, so it is only necessary to configure the multicast address on the equipment on which the interface is involved.

Additionally, the GMRP protocol also applies this type of manual configuration in an abstract group address, called ***Forward All***, which means than an interface wants to receive all multicast traffic. This option is configured individually for each local interface of the equipment.

FIGURE 57 ***GMRP*** configuration page of ***Multicast*** menu



GMRP

Enable □

Forward All Groups

#	Forward All
1	normal
2	normal
3	normal
4	normal
5	normal
6	normal
7	normal
8	normal
9	normal
10	normal
11	normal
12	normal
13	normal
14	normal
15	normal
16	normal
17	normal
18	normal
19	normal
20	normal

The parameters are the following:

GMRP:

A single parameter to set the implementation of GMRP protocol:

- **Enable.** A simple *CheckBox* parameter, which controls the execution of the protocol.

Forward All Groups:

The equipment allows manual configuration of this special address individually for each interface.

- #**.** It sets the equipment physical port number.

- **Forward All.** Indicates the status of the special group address for the corresponding interface. Valid values are ***Normal***, ***Fixed*** and ***Forbidden***. The ***Normal*** option is the default option. It indicates that the spread or not of the multicast traffic is subjected to there being a client equipment that requested the register for the group address. The ***Fixed*** option means that the interface will propagate all multicast traffic, and GMRP messages concerning the group address is ignored. The ***Forbidden*** option assumes that requests won´t be accepted by the client devices for the group address, and that only the multicast traffic registered in the interface will be treated.

5.16.3 IGMP

The IGMP Snooping is an optimization to be used in level 2 devices, such as the SW3-L3. The IGMP protocol is level 3; therefore, the IGMP Snooping operation performed by the switch is conditioned by the presence of a Multicast router in the network.

The SW3-L3 includes a special feature if there is NO multicast router in the network, and if the IGMP Snooping operation has to be active. Said feature implies that the switch itself emulates the presence of a multicast router, by periodically consulting the clients about belonging to the different multicast diffusion groups.

The configuration parameters are the following:

IGMP:

There is a single parameter that determines whether the emulation as IGMP router is active or not:

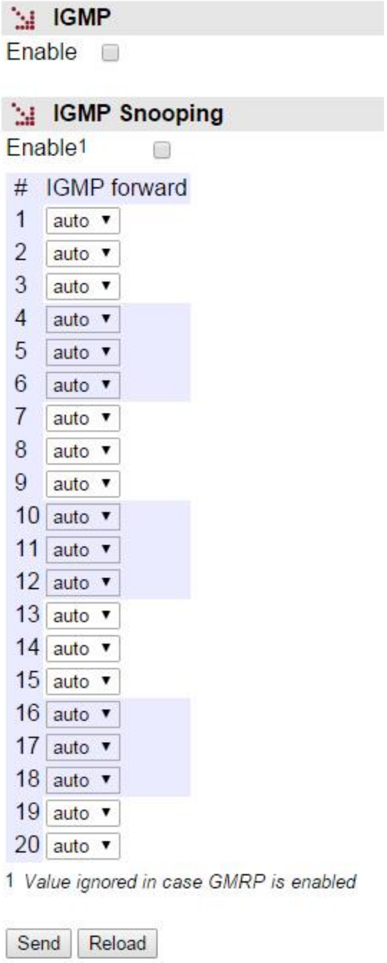
- **Enable.** A simple *CheckBox* parameter to set if the IGMP periodic consultation service is active or not.

IGMP Snooping:

It is a feature that permits the switch to analyze the multicast traffic between devices and routers in order to identify the ports where there are devices actively participating in multicast groups; the objective is to limit selective data transmission based on the obtained information.

- **Enable.** A simple *CheckBox* to set if the IGMP periodic consultation service is active or not.
- #**.** It sets the equipment physical port number.
- **IGMP forward.** It sets the treatment of the multicast messages in the corresponding port. Configured in **on**, the port transmits all the multicast messages, while it does not transmit anything when it is **off**. Configured in **auto**, the port will selectively transmit the multicast messages if there are client devices registered in the corresponding group.

FIGURE 58 *IGMP* configuration page of ***Multicast*** menu



IGMP

Enable □

IGMP Snooping

Enable1 □

#	IGMP forward
1	auto ▼
2	auto ▼
3	auto ▼
4	auto ▼
5	auto ▼
6	auto ▼
7	auto ▼
8	auto ▼
9	auto ▼
10	auto ▼
11	auto ▼
12	auto ▼
13	auto ▼
14	auto ▼
15	auto ▼
16	auto ▼
17	auto ▼
18	auto ▼
19	auto ▼
20	auto ▼

1 *Value ignored in case GMRP is enabled*

5.17 ACCESS CONFIGURATION

The equipment offer users several means of access: operating console, access via HTTP server (web) and telnet.

Local users predefined in the system are always present but some external resources can be used to validate users for different types of access, for which reason the user database is a centralised and independent resource with respect to the equipment itself. For this purpose, the equipment has a TACACS+ client and a RADIUS client.

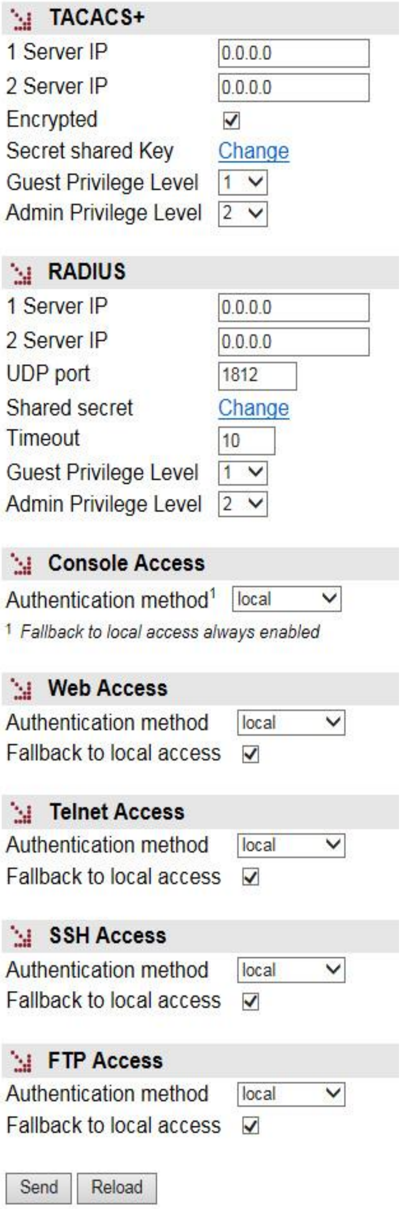
TACACS+:

TACACS+ (**Terminal Access Controller Access Control System**) is a remote authentication protocol used to manage access to servers and communication devices; it provides separate authentication, authorisation and registration services.

The general configuration parameters are the following:

- **1 Server IP.** This sets the IP address of the primary TACACS+ server.
- **2 Server IP.** This sets the IP address of the secondary TACACS+ server.
- **Encrypted.** This permits user to select whether the equipment communication with the TACACS+ servers must be made in the ciphered mode or not.
- **Secret Shared Key.** This sets the code to be used for ciphering the communication when the **encrypted** option is active.
- **Guest Privilege Level.** This sets the privilege level (0 to 15) in the request to the TACACS+ server to gain access as guest user (***guest***). The privilege level must be consistent with the one configured in the TACACS+ server queried.
- **Admin Privilege Level.** This sets the privilege level (0 to 15) in the request to the TACACS+ server to gain access as administrator user (***admin***). The privilege level must be consistent with the one configured in the TACACS+ server queried.

FIGURE 59 ***Access*** menu configuration page



TACACS+

1 Server IP	0.0.0.0
2 Server IP	0.0.0.0
Encrypted	☑
Secret shared Key	Change
Guest Privilege Level	1
Admin Privilege Level	2

RADIUS

1 Server IP	0.0.0.0
2 Server IP	0.0.0.0
UDP port	1812
Shared secret	Change
Timeout	10
Guest Privilege Level	1
Admin Privilege Level	2

Console Access

Authentication method[1]	local

[1] *Fallback to local access always enabled*

Web Access

Authentication method	local
Fallback to local access	☑

Telnet Access

Authentication method	local
Fallback to local access	☑

SSH Access

Authentication method	local
Fallback to local access	☑

FTP Access

Authentication method	local
Fallback to local access	☑

RADIUS:

The parameters for the RADIUS client are the following:

- **1 Server IP.** It sets the primary RADIUS server IP address.
- **2 Server IP.** It sets the secondary RADIUS server IP address.
- **UDP Port.** It sets the UDP port in which the RADIUS servers operate. The default value set the UDP port reserved for the said protocol.

- **Shared Secret.** It sets the shared secret key. Being a necessary data, the device uses *ziv12345* as the default value.

- **Timeout.** It sets the timeout for obtaining response from the server. This parameter is necessary due to the use of the connectionless UDP protocol.

- **Guest Privilege Level.** It sets the privilege level (0 to 15) of the guest profile (***guest***). If the privilege level received for the calling user in the affirmative answer of the RADIUS server is equal to or more than this parameter, and at the same time lower than the *Admin* level, the user will get guest access (read only).

- **Admin Privilege Level.** It sets the privilege level (0 to 15) of the administrator profile (***admin***). If the privilege level received for the calling user in the affirmative answer of the RADIUS server is equal to or more than this parameter, the user will get administrator access (read and write access).

The parameters associated with each access option (**console**, **web**, **telnet, SSH** and **FTP access**) are the following:

- **Authentication method.** This sets whether the user validation must be made locally or by consulting the configured tacacsplus or radius servers.

- **Fallback to local access.** When this option is enabled, if there is no accessibility to the configured TACACS+ or RADIUS servers, users are permitted to validate themselves with local user names. If the option is disabled, and the TACACS+ or RADIUS servers are not accessible, users will not be granted access. Access through the console has this option permanently enabled, for which reason it is not configurable.

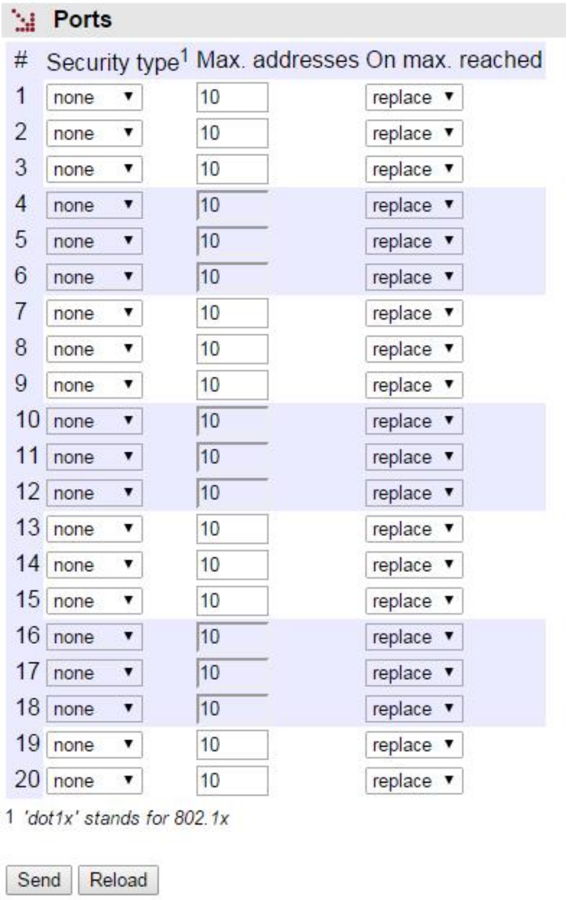
5.18 SECURITY CONFIGURATION

This menu allows traffic restrictions to be imposed, depending on the MAC addresses of the clients. The equipment admits two modes for verifying the admitted client MAC addresses: maclist or 802.1x.

When operating with lists, maclist, the equipment will only send traffic if the MAC address is included in the authorized address list. Activation of the restriction and the list is configured separately for each port.

For the 802.1x mode, the authentication of MAC addresses is done by consulting a RADIUS server. **RADIUS** (acronym for **Remote Authentication Dial-In User Server**) is a remote authentication protocol used to manage access to servers and communication devices; it provides separate authentication, authorization and registration services.

FIGURE 60 ***Security*** main menu configuration page



Ports

#	Security type[1]	Max. addresses	On max. reached
1	none	10	replace
2	none	10	replace
3	none	10	replace
4	none	10	replace
5	none	10	replace
6	none	10	replace
7	none	10	replace
8	none	10	replace
9	none	10	replace
10	none	10	replace
11	none	10	replace
12	none	10	replace
13	none	10	replace
14	none	10	replace
15	none	10	replace
16	none	10	replace
17	none	10	replace
18	none	10	replace
19	none	10	replace
20	none	10	replace

[1] *'dot1x' stands for 802.1x*

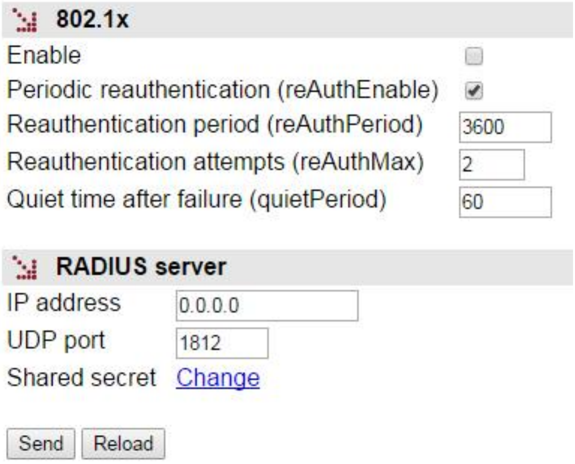
The general configuration parameters for the ports are the following:

- **#.** Physical interface identifier.
- **Security Type.** It sets if the filtering service by MAC address is active in the indicated port (**maclist** option), or the 802.1x authorization is used (**dot1x** option), or no filter is activated (**none** option).
- **Max. Addresses.** This sets the maximum number of MAC addresses permitted at one time in the indicated port.
- **On max. reached.** This sets the behaviour of the equipment in the event of reaching the maximum number of MAC addresses permitted, as set in the preceding parameter. The available options are **replace** or **restrict.**

5.18.1 802.1x

This submenu permits specifying the 802.1x user authentication through access to a RADIUS server.

FIGURE 61 ***802.1x*** submenu configuration page



802.1x

Enable	□
Periodic reauthentication (reAuthEnable)	☑
Reauthentication period (reAuthPeriod)	3600
Reauthentication attempts (reAuthMax)	2
Quiet time after failure (quietPeriod)	60

RADIUS server

IP address	0.0.0.0
UDP port	1812
Shared secret	Change

The general configuration parameters are the following:

- **Enable.** A simple *CheckBox* parameter to set if the RADIUS client, as well as the 802.1x authentication, is active or not.

- **Periodic reauthentication (reAuthEnable).** If the RADIUS server limits the session time, this option indicates to the equipment that periodic reauthentication has to be requested.

- **Reauthentication period (reAuthPeriod).** It sets the time between one reauthentication and the next. The parameter is expressed in seconds, and the accepted value range is between 1 and 86400 (1 day), where the default value is 3600 (1 hour).

- **Reauthentication attempts (reAuthMax).** It sets the maximum number of tries the equipment will send to request reauthentication. Valid values are 1 to 10.

- **Quiet time after failure (quietPeriod).** It sets the period of time in which the equipment will not request new tries once the maximum number of configured tries is exceeded. Valid values, in seconds, are 1 to 65535.

- **IP address.** It sets the RADIUS server IP address.

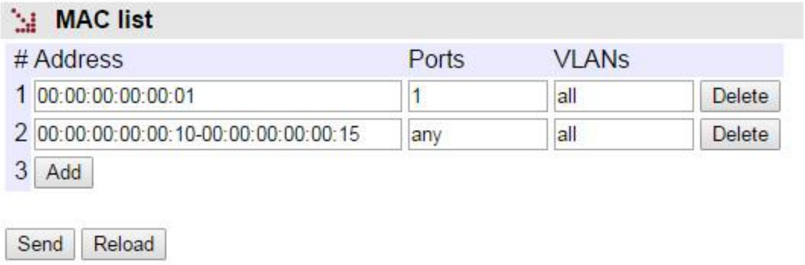
- **UDP port.** It sets the UDP port to which the RADIUS client will send requests to the server. The default value set in the standard is port 1812.

- **Shared secret.** It sets the password to be used to encode the communication with the RADIUS server.

5.18.2 MAC list

This submenu permits the authorized client MAC address list to be specified. The list may or may not be activated in each port through the **Security type** parameter.

FIGURE 62 ***MAC list*** submenu configuration page



MAC list

#	Address	Ports	VLANs	
1	00:00:00:00:00:01	1	all	Delete
2	00:00:00:00:00:10-00:00:00:00:00:15	any	all	Delete
3	Add			

The parameters for creating the MACS list are the following:

- **#.** Tabulate element identifier. Not relevant.

- **Address.** The client MAC address entered in the list. If a range is desired to be included, the initial address and final address are separated by a hyphen (see example in the figure).

- **Ports.** Port(s) in which the MAC address will be accepted. A group of discreet ports is configured with the identifier of each one, separated by a comma, without spaces. If a range is to be included, the initial port identifier and final port identifier are separated by a dash. The value **any** means the port is not relevant.

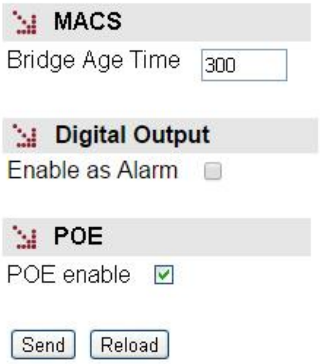
- **VLANs.** Numerical identifier of the VLAN defined in the equipment in which the MAC address will be accepted (VID fields in the ***VLANs*** menu). A group of discreet vlans is configured with the identifier of each one, separated by a comma, without spaces. If a range is to be included, the initial and final vlan identifiers are separated by a dash. The value **all** means the vlan is not relevant. Example: in equipment with a **vlan1**, **vlan3** and **vlan4** defined, the group of numerical identifiers will be **1,3,4**.

> The presence of identifiers in the **Ports** parameter and **VLANs** section is not exclusive. If values for both parameters are specified, the configuration is applied at the indicated ports that also meet the requirement of belonging to VLANs configured.

5.19 OTHERS CONFIGURATION

The ***Others*** menu brings other general equipment options.

FIGURE 63 ***Others*** menu configuration page



MACS

Bridge Age Time 300

Digital Output

Enable as Alarm □

POE

POE enable ☑

The sections and their configuration parameters are as follows:

MACS:

- **Bridge Age Time.** It sets the maximum time a learned MAC address of inactivity will remain in the switch MAC address table. Valid values, in seconds, are 15 to 3600. The default value is 300.

Digital Output:

- **Enable as Alarm.** A simple *CheckBox* parameter to indicate whether the digital output, pins 1 and 2 of I/O connector, will be used as alarm.

POE:

- **POE enable.** This option appears in the equipment with front ports and PoE power supply. By checking this box, the Power over Ethernet power supply is enabled (IEEE 802.3af). Said power supply offers the possibility of directly power supplying IP devices through the first eight electrical ports (1 to 4 of block 1 and 1 to 4 of block 2).

5.20 REBOOT

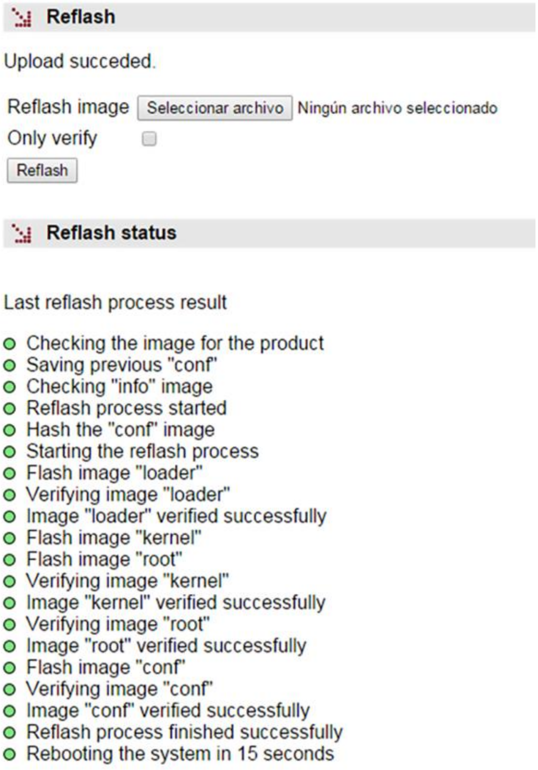
The equipment can be rebooted by executing the ***Reboot*** command, through the console or through the HTML pages. The command is available only for the administrator profile.

5.21 CODE REFLASH

The equipment admits the updating of applicative software by executing the ***Reflash*** command, which is only available in the HTML pages and for the administrator profile.

> The code reflash process does not alter the configuration data, unless this is expressly indicated. Nevertheless, once terminated, it entails a momentary loss of service due to the automatic rebooting of the unit.

FIGURE 64 ***Reflash*** configuration page



Reflash

Upload succeded.

Reflash image Ningún archivo seleccionado

Only verify □

Reflash status

Last reflash process result

- Checking the image for the product
- Saving previous "conf"
- Checking "info" image
- Reflash process started
- Hash the "conf" image
- Starting the reflash process
- Flash image "loader"
- Verifying image "loader"
- Image "loader" verified successfully
- Flash image "kernel"
- Flash image "root"
- Verifying image "kernel"
- Image "kernel" verified successfully
- Verifying image "root"
- Image "root" verified successfully
- Flash image "conf"
- Verifying image "conf"
- Image "conf" verified successfully
- Reflash process finished successfully
- Rebooting the system in 15 seconds

A binary image is necessary, which can be selected by pressing the button *Examine*.

After having selected the image, the update is executed by pressing ***Reflash***. The process usually takes about 5 minutes, during which time the results of the different steps are displayed in the HTML browser window, but depending on the browser, it is possible that only the result at the end of the process is shown.

The ***Only verify*** option allows users to check that the code saved is coincident with the binary image selected without affecting the installed image.

5.21.1 Backup

The equipment stores automatically an application software backup. The copy is not accessible or configurable by the user. The system itself is that, after a few minutes from the start up, checks if the application software running and the backup are identical and, if they are not, proceeds to update the backup.

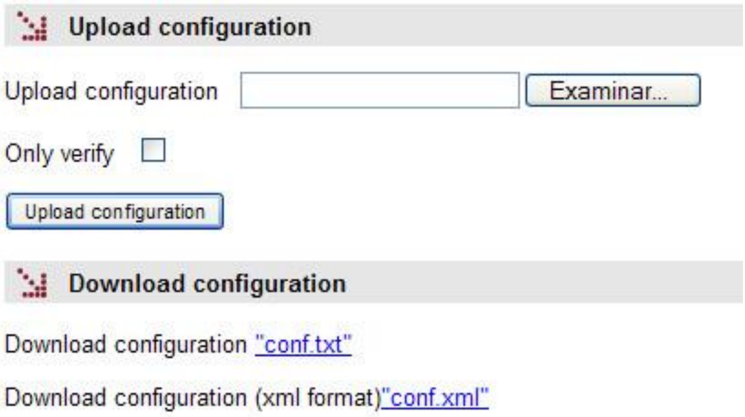
The action of verification and possible updating is done only when the software application running is NOT the one stored in the backup.

> During the copying process, the system does not allow the modification of configuration parameters nor operations *Reflash* o *Reboot* and hides the corresponding menu block.

5.22 CONFIGURATION FILE

The equipment configuration can be retrieved (***Download***) or uploaded (***Upload***) by means of a text or XML file.

FIGURE 65 Options for uploading (***Upload***) or downloading (***Download***) the configuration file



Upload configuration

Upload configuration [ ] Examinar...

Only verify □

Upload configuration

Download configuration

Download configuration "conf.txt"

Download configuration (xml format)"conf.xml"

5.22.1 Upload (from the PC to the equipment)

The user must select the file containing the configuration to be uploaded by pressing the button *Examine*.

In order to only verify the configuration without upload it, the ***Only verify*** box must be ticked.

Once the equipment has received the file, the system checks the file contents and verifies that the variables are valid and that the values assigned to them comply with the existing syntactic requirements. If errors are detected in the received file, irrespective of whether the ***Only verify*** option is selected or not, the system automatically rejects all the information received and indicates the error situation to the user.

If the received configuration is valid, it is indicated by the system to the user, and it is then possible to continue (*Continue* button). When continue is selected, the configuration is activated and stored.

> When applying the new configuration, the system issues a warning due to the possible loss of equipment access.

If the ***Only verify*** option has been selected, and verification has been successful, it is indicated by the system to the user. If desired, the configuration can be applied by means of the *Apply* and *Save* commands or both, and also remove from the memory the verified configuration by choosing the option *Cancel*.

The ***Customer default*** box assumes that the configuration file sent to the equipment will be stored as customer default configuration, which means that it will be the configuration of the equipment in case the reconfiguration button is pressed. If the ***Only Verify*** option is active simultaneously, once the file is verified, the user will have the option to store the configuration or discard it. Otherwise, if the verification is correct, the file will be stored automatically.

The default configuration can be queried by using the ***show*** command in CLI.

5.22.2 Download (from the equipment to the PC)

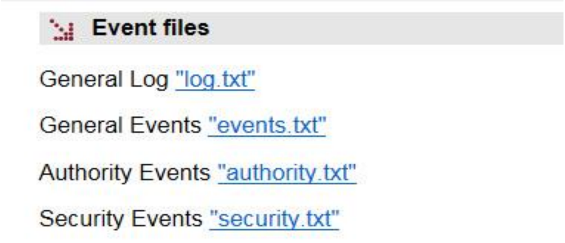
With this option the user obtains a local copy of the operating configuration in **.txt** format or **.xml** format.

The procedure for downloading this file depends on both the HTTP browser and the actions to perform with the received file (for example, where to store it).

5.23 EVENT FILES

With this option, the user can download different log files in txt format.

FIGURE 66 Event Files configuration page



Event files

General Log "log.txt"

General Events "events.txt"

Authority Events "authority.txt"

Security Events "security.txt"

The total event log (General Log “log.txt”), the most relevant event log (General Events “events.txt”), the authentication event log (Authority Events “authority.txt”) and the security event log (Security Events “security.txt”) are available. The latter is only accesible for Admin users.

As in the case of the downloading of the configuration of the equipment, the procedure for obtaining the file will depend on the HTTP browser used by the user, as well as the actions that must be performed with the received file (for example, where to store it, etc).

6 STATISTICS

The system provides statistics divided into eleven blocks, each of them corresponding to a specific functionality.

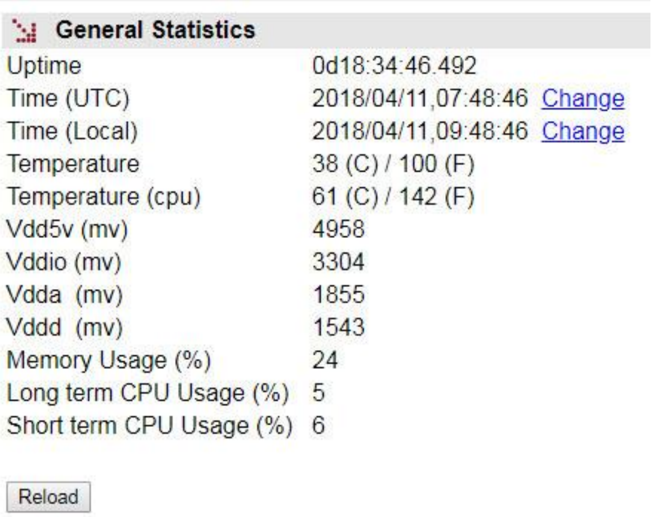
The first block shows general information related to the equipment, and is displayed automatically when the statistics object is selected.

The remaining statistics are grouped into data on the Ethernet interfaces (*Ports*), the MAC addresses identified by the switch (*MACS*), STP protocol, LLDP protocol, VLAN, Routing, DHCP Servers, VRRP, synchronization client (*NTP*), and PTP ports (as applicable), each of which can be accessed by selecting the respective tag located under the heading *Statistics*.

> Each statistical data table can be updated by pressing the *Reload* button without having to select the respective option again in the tree menu.

> The statistics can be **REBOOTED** by the user at will, from the console by running the ***clear*** command in the prompt, or using the menu option ***Clear Statistics***.

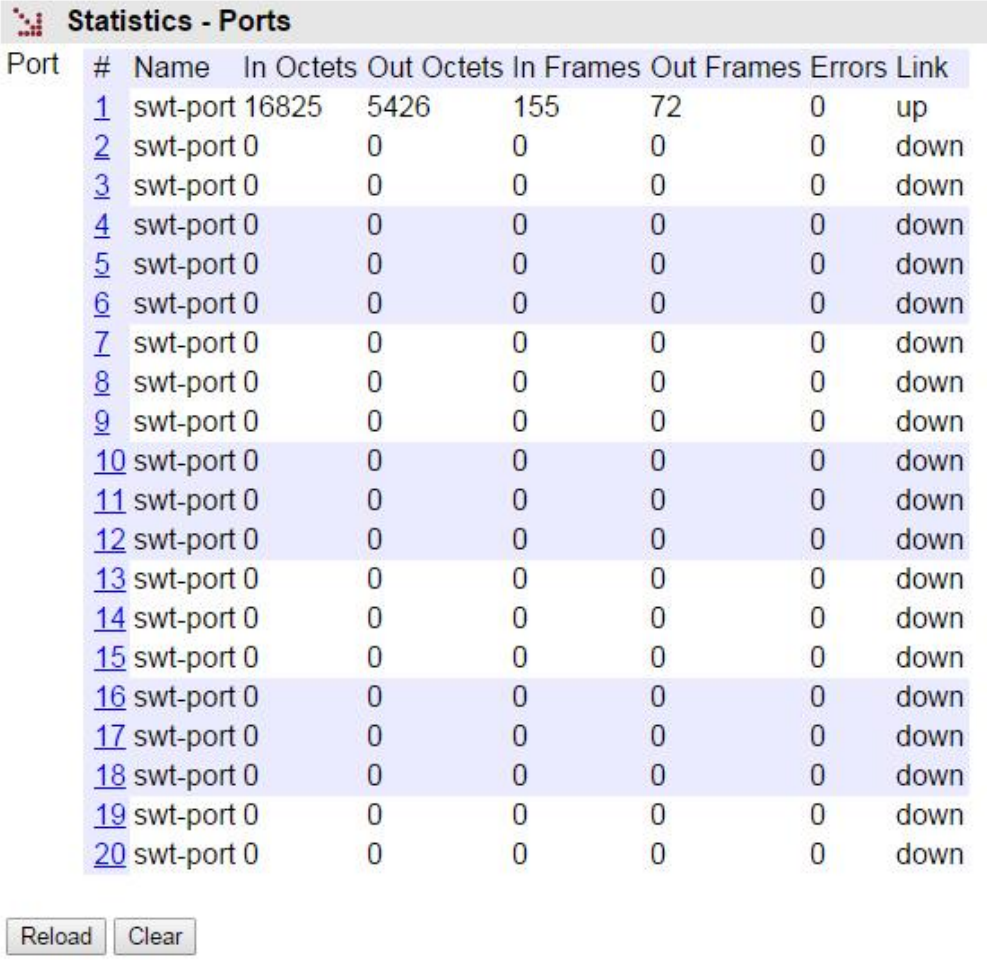
FIGURE 67 Example of statistics with general data



General Statistics

Uptime	0d18:34:46.492
Time (UTC)	2018/04/11,07:48:46 Change
Time (Local)	2018/04/11,09:48:46 Change
Temperature	38 (C) / 100 (F)
Temperature (cpu)	61 (C) / 142 (F)
Vdd5v (mv)	4958
Vddio (mv)	3304
Vdda (mv)	1855
Vddd (mv)	1543
Memory Usage (%)	24
Long term CPU Usage (%)	5
Short term CPU Usage (%)	6

FIGURE 68 Example of basic statistics of Ethernet ports

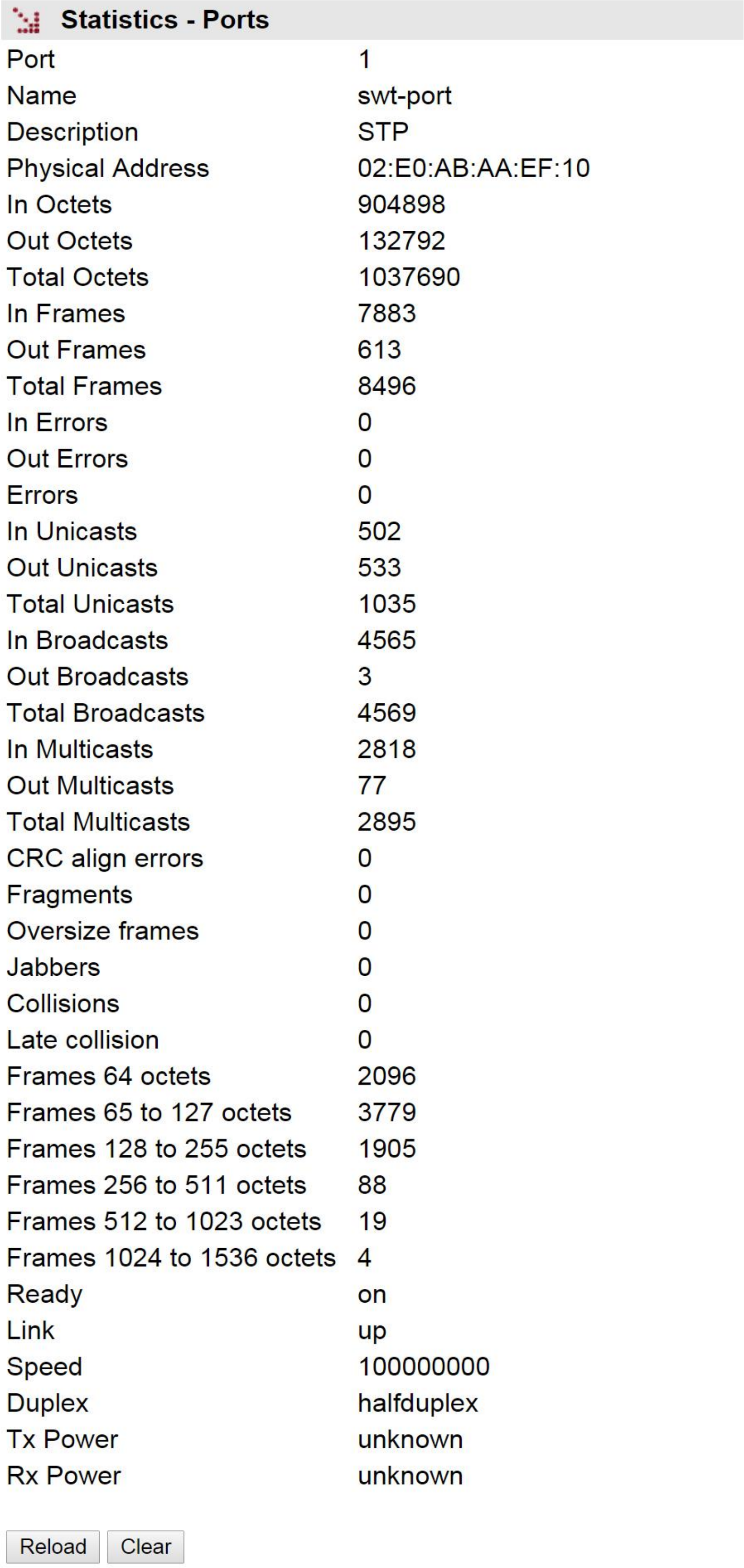


Statistics - Ports

Port

#	Name	In Octets	Out Octets	In Frames	Out Frames	Errors	Link
1	swt-port	16825	5426	155	72	0	up
2	swt-port	0	0	0	0	0	down
3	swt-port	0	0	0	0	0	down
4	swt-port	0	0	0	0	0	down
5	swt-port	0	0	0	0	0	down
6	swt-port	0	0	0	0	0	down
7	swt-port	0	0	0	0	0	down
8	swt-port	0	0	0	0	0	down
9	swt-port	0	0	0	0	0	down
10	swt-port	0	0	0	0	0	down
11	swt-port	0	0	0	0	0	down
12	swt-port	0	0	0	0	0	down
13	swt-port	0	0	0	0	0	down
14	swt-port	0	0	0	0	0	down
15	swt-port	0	0	0	0	0	down
16	swt-port	0	0	0	0	0	down
17	swt-port	0	0	0	0	0	down
18	swt-port	0	0	0	0	0	down
19	swt-port	0	0	0	0	0	down
20	swt-port	0	0	0	0	0	down

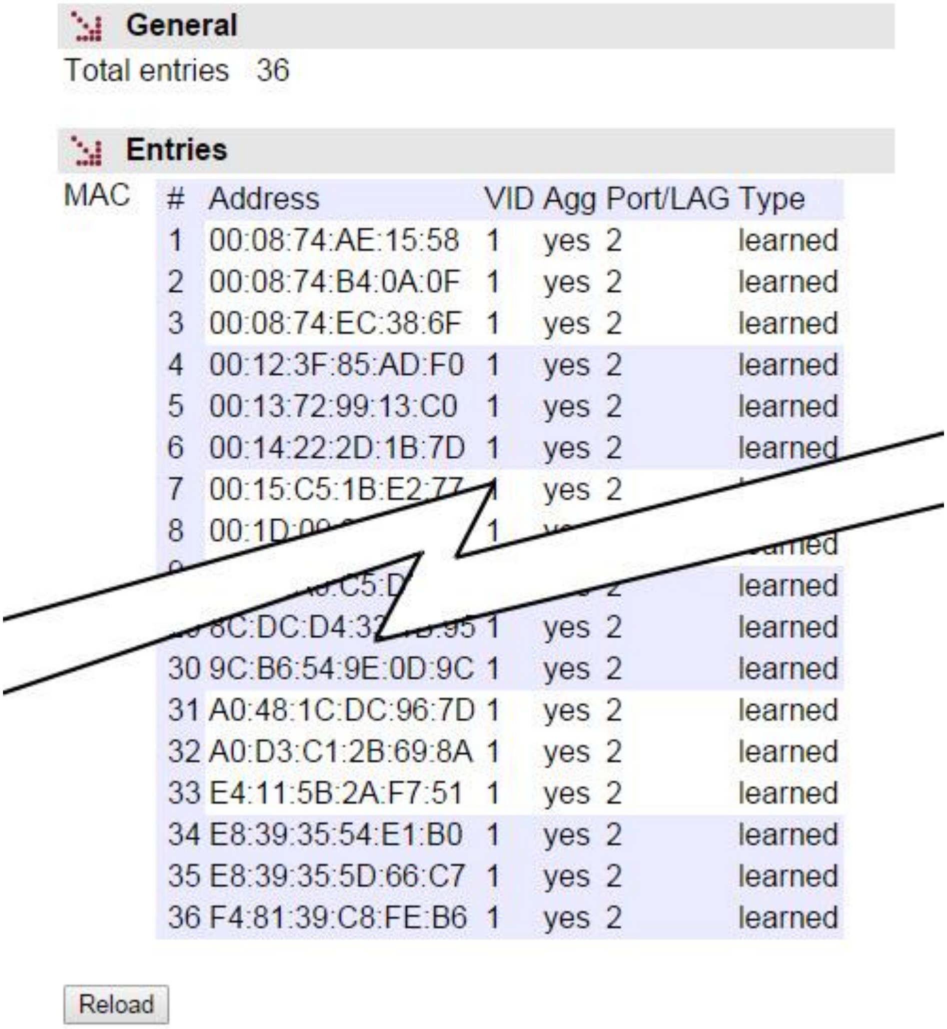
FIGURE 69 Example of statistics detail of a specific port (selection of # parameter)



Statistics - Ports

Port	1
Name	swt-port
Description	STP
Physical Address	02:E0:AB:AA:EF:10
In Octets	904898
Out Octets	132792
Total Octets	1037690
In Frames	7883
Out Frames	613
Total Frames	8496
In Errors	0
Out Errors	0
Errors	0
In Unicasts	502
Out Unicasts	533
Total Unicasts	1035
In Broadcasts	4565
Out Broadcasts	3
Total Broadcasts	4569
In Multicasts	2818
Out Multicasts	77
Total Multicasts	2895
CRC align errors	0
Fragments	0
Oversize frames	0
Jabbers	0
Collisions	0
Late collision	0
Frames 64 octets	2096
Frames 65 to 127 octets	3779
Frames 128 to 255 octets	1905
Frames 256 to 511 octets	88
Frames 512 to 1023 octets	19
Frames 1024 to 1536 octets	4
Ready	on
Link	up
Speed	100000000
Duplex	halfduplex
Tx Power	unknown
Rx Power	unknown

FIGURE 70 Example of statistics of the MAC addresses identified by the switch



General

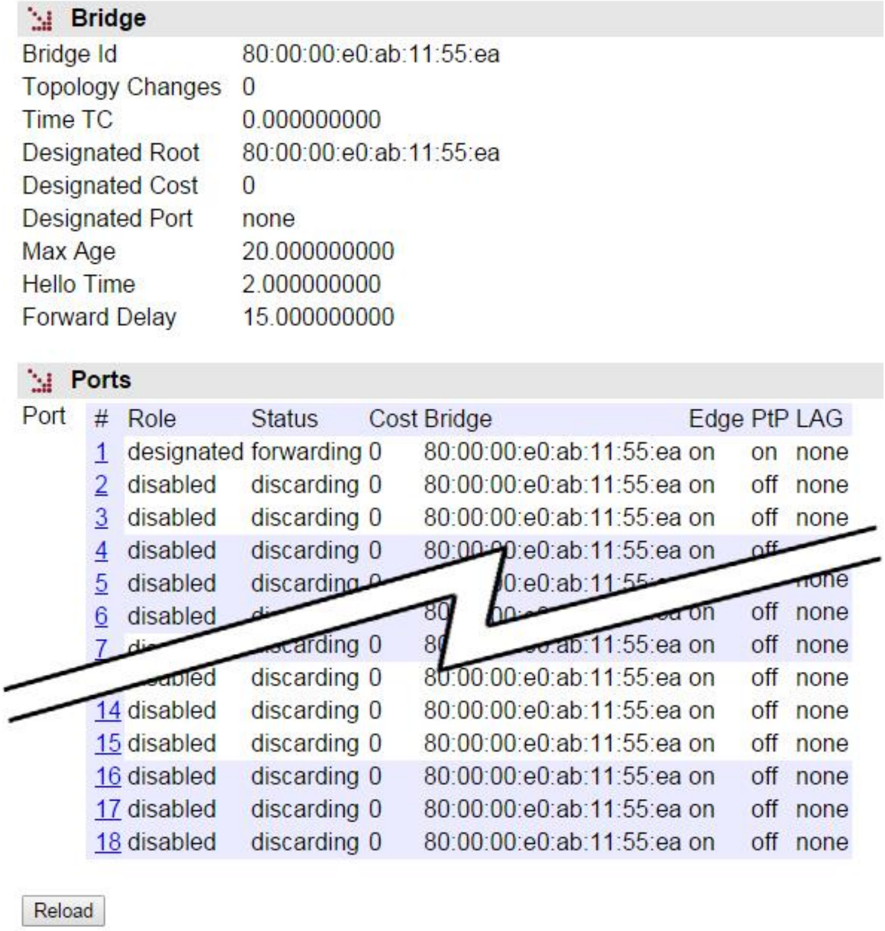
Total entries 36

Entries

MAC

#	Address	VID	Agg	Port/LAG	Type
1	00:08:74:AE:15:58	1	yes	2	learned
2	00:08:74:B4:0A:0F	1	yes	2	learned
3	00:08:74:EC:38:6F	1	yes	2	learned
4	00:12:3F:85:AD:F0	1	yes	2	learned
5	00:13:72:99:13:C0	1	yes	2	learned
6	00:14:22:2D:1B:7D	1	yes	2	learned
7	00:15:C5:1B:E2:77	1	yes	2	
8	00:1D:00	1			arned
	C5:D			2	learned
	8C:DC:D4:3 B:95	1	yes	2	learned
30	9C:B6:54:9E:0D:9C	1	yes	2	learned
31	A0:48:1C:DC:96:7D	1	yes	2	learned
32	A0:D3:C1:2B:69:8A	1	yes	2	learned
33	E4:11:5B:2A:F7:51	1	yes	2	learned
34	E8:39:35:54:E1:B0	1	yes	2	learned
35	E8:39:35:5D:66:C7	1	yes	2	learned
36	F4:81:39:C8:FE:B6	1	yes	2	learned

FIGURE 71 Example of statistics of the STP protocol



Bridge

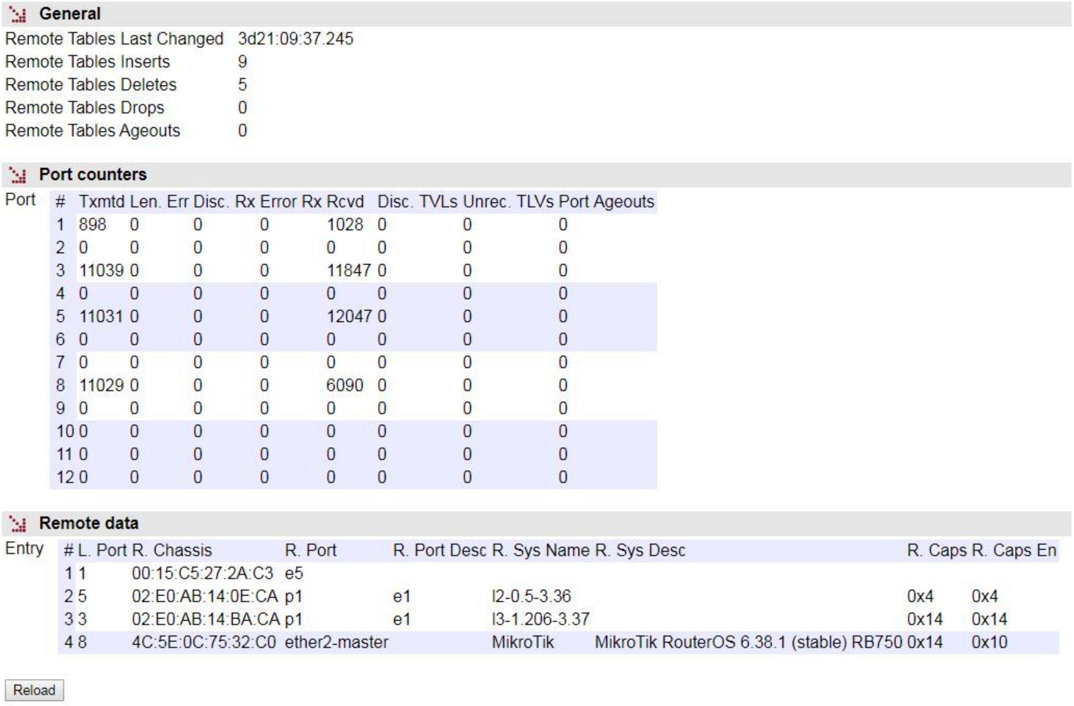
Bridge Id	80:00:00:e0:ab:11:55:ea
Topology Changes	0
Time TC	0.000000000
Designated Root	80:00:00:e0:ab:11:55:ea
Designated Cost	0
Designated Port	none
Max Age	20.000000000
Hello Time	2.000000000
Forward Delay	15.000000000

Ports

Port

#	Role	Status	Cost	Bridge	Edge	PtP	LAG
1	designated	forwarding	0	80:00:00:e0:ab:11:55:ea	on	on	none
2	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
3	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
4	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	
5	disabled	discarding	0	0:e0:ab:11:55			none
6	disabled	di		80 00:	on	off	none
7	di	carding	0	8 :ab:11:55:ea	on	off	none
	abled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
14	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
15	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
16	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
17	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
18	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none

FIGURE 72 Example of statistics of the LLDP protocol



General

Remote Tables Last Changed	3d21:09:37.245
Remote Tables Inserts	9
Remote Tables Deletes	5
Remote Tables Drops	0
Remote Tables Ageouts	0

Port counters

Port

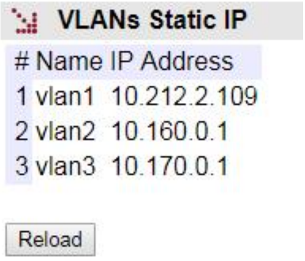
#	Txmtd	Len. Err Disc.	Rx Error	Rx Rcvd	Disc. TVLs	Unrec. TLVs	Port Ageouts
1	898	0	0	1028	0	0	0
2	0	0	0	0	0	0	0
3	11039	0	0	0	11847	0	0
4	0	0	0	0	0	0	0
5	11031	0	0	0	12047	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	11029	0	0	0	6090	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0

Remote data

Entry

#	L. Port	R. Chassis	R. Port	R. Port Desc	R. Sys Name	R. Sys Desc	R. Caps	R. Caps En
1	1	00:15:C5:27:2A:C3	e5					
2	5	02:E0:AB:14:0E:CA	p1	e1	l2-0.5-3.36		0x4	0x4
3	3	02:E0:AB:14:BA:CA	p1	e1	l3-1.206-3.37		0x14	0x14
4	8	4C:5E:0C:75:32:C0	ether2-master		MikroTik	MikroTik RouterOS 6.38.1 (stable) RB750	0x14	0x10

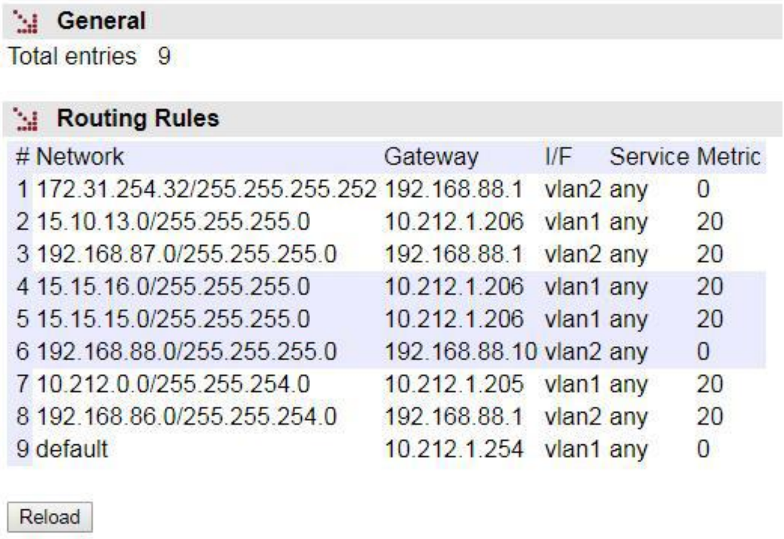
FIGURE 73 Example of statistics of IP addressing data (VLAN)



VLANs Static IP

#	Name	IP Address
1	vlan1	10.212.2.109
2	vlan2	10.160.0.1
3	vlan3	10.170.0.1

FIGURE 74 Example of statistics of routing information



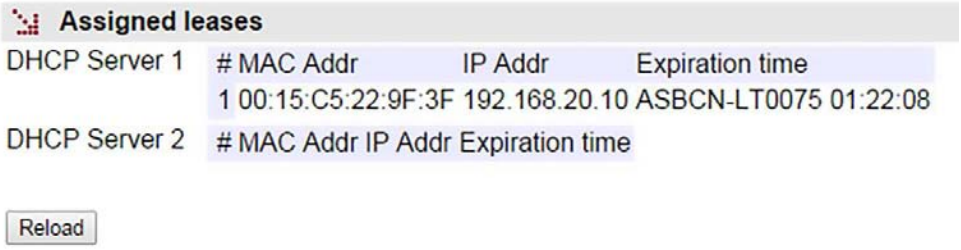
General

Total entries 9

Routing Rules

#	Network	Gateway	I/F	Service	Metric
1	172.31.254.32/255.255.255.252	192.168.88.1	vlan2	any	0
2	15.10.13.0/255.255.255.0	10.212.1.206	vlan1	any	20
3	192.168.87.0/255.255.255.0	192.168.88.1	vlan2	any	20
4	15.15.16.0/255.255.255.0	10.212.1.206	vlan1	any	20
5	15.15.15.0/255.255.255.0	10.212.1.206	vlan1	any	20
6	192.168.88.0/255.255.255.0	192.168.88.10	vlan2	any	0
7	10.212.0.0/255.255.254.0	10.212.1.205	vlan1	any	20
8	192.168.86.0/255.255.254.0	192.168.88.1	vlan2	any	20
9	default	10.212.1.254	vlan1	any	0

FIGURE 75 Example of statistics of DHCP Servers



Assigned leases

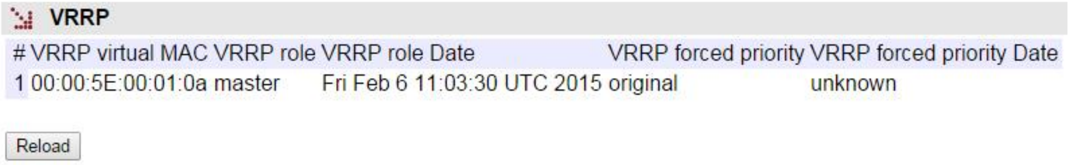
DHCP Server 1

#	MAC Addr	IP Addr	Expiration time
1	00:15:C5:22:9F:3F	192.168.20.10	ASBCN-LT0075 01:22:08

DHCP Server 2

#	MAC Addr	IP Addr	Expiration time

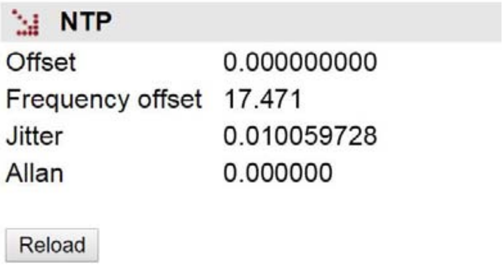
FIGURE 76 Example of statistics of the VRRP protocol



VRRP

#	VRRP virtual MAC	VRRP role	VRRP role Date	VRRP forced priority	VRRP forced priority Date
1	00:00:5E:00:01:0a	master	Fri Feb 6 11:03:30 UTC 2015	original	unknown

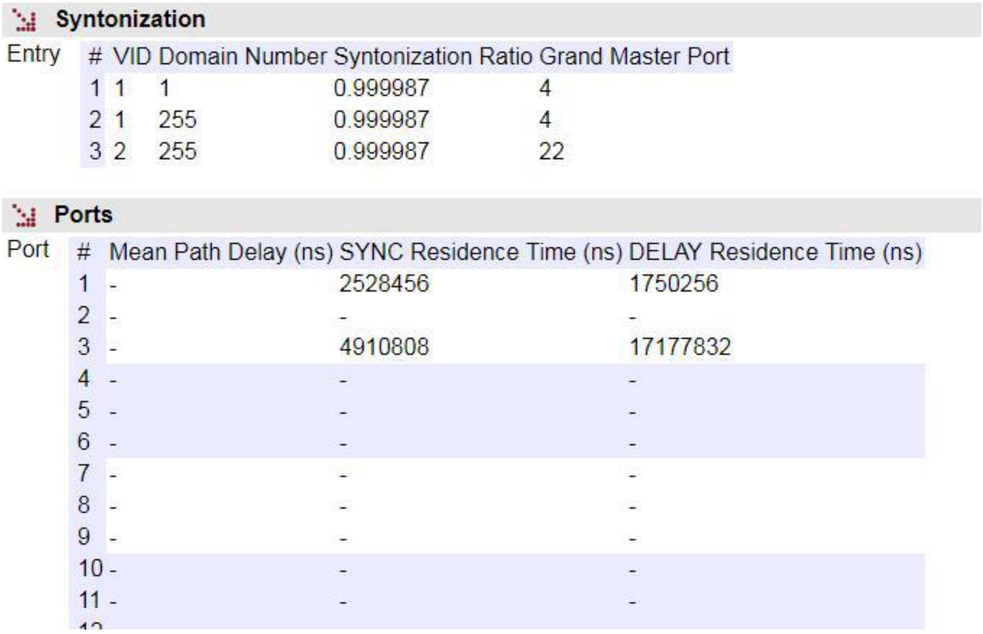
FIGURE 77 Example of statistics of the NTP client



NTP

Offset	0.000000000
Frequency offset	17.471
Jitter	0.010059728
Allan	0.000000

FIGURE 78 Example of statistics of the PTP protocol (*for SW3-L3 equipped with PTP ports*)



Syntonization

Entry

#	VID	Domain Number	Syntonization Ratio	Grand Master Port
1	1	1	0.999987	4
2	1	255	0.999987	4
3	2	255	0.999987	22

Ports

Port

#	Mean Path Delay (ns)	SYNC Residence Time (ns)	DELAY Residence Time (ns)
1	-	2528456	1750256
2	-	-	-
3	-	4910808	17177832
4	-	-	-
5	-	-	-
6	-	-	-
7	-	-	-
8	-	-	-
9	-	-	-
10	-	-	-
11	-	-	-

.

APPENDIX A

BIBLIOGRAPHY AND ABBREVIATIONS

APPENDIX A

BIBLIOGRAPHY AND ABBREVIATIONS

A.1 BIBLIOGRAPHY

[1] IEEE RFC 1058. June 1988. Routing Information Protocol.

[2] STD 56. IEEE RFC 2453. November 1998. RIP Version 2 (Obsoletes RFC 1723, RFC 1388).

[3] STD 15. IEEE RFC 1157. May 1990. A Simple Network Management Protocol (SNMP).

[4] STD 62. IEEE RFC 3416. December 2002. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) (Obsoletes RFC 1905).

[5] IEEE RFC 1305, March 1992. Network Time Protocol (Version 3) Specification, Implementation and Analysis.

A.2 ABBREVIATIONS

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
API	Application Programming Interface
APN	Access Point Name
ASDU	Application Service Data Units
BPDU	Bridge Protocol Data Units
DHCP	Dynamic Host Configuration Protocol
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name Server
DPD	Dead Peer Detection
DSCP	Differentiated Services Code Point
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IOA	Information Object Address
IP	Internet Protocol
IP Multicast	Extension of the Internet Protocol for providing support to multidiffusion communications
IPBX	Internet Protocol Private Branch Exchange
IPS	Intrusion Prevention System
IPSec	IP Security

ISDN	Integrated Services Data Network
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider
LAN	Local Area Network
NAT	Network Address Translation
NHRP	Next Hop Resolution Protocol
NTP	Network Time Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Server
RAS	Registration, Authentication and Status
RSVP	Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SIM	Subscriber Identity Module
SMTP	Simple Mail Transfer Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator

VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRID	Virtual Router Identifier
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WINS	Windows Internet Naming Service
WPA	Wi-Fi Protected Access Client Support

.

APPENDIX B

DATA STRUCTURE IN *CLI*

APPENDIX B

DATA STRUCTURE IN *CLI*

This appendix contains all the information required to use the CLI user console. It explains the access methods, commands available on the console and gives a step-by-step example of how to obtain information on the status and configuration of the equipment.

Conventions:

The equipment configuration parameters are laid out in a tree directory, in which parameters and related subdirectories are grouped, where:

- A name followed by "**/**" indicates the name of a directory. *E.g.* ***Main/***
- A name followed by "**[]/**" indicates a parameter with a matrix structure, as it contains several attributes. *E.g.* ***nat[]/***
- A name with nothing after, it is a parameter itself. *E.g.* ***action***

B.1 ACCESS METHODS

There are two ways of accessing the equipment through the CLI user console:

➤ in the local mode, through the serial port (SRV port).

➤ in local and remote mode, through Telnet.

Access through the SRV port

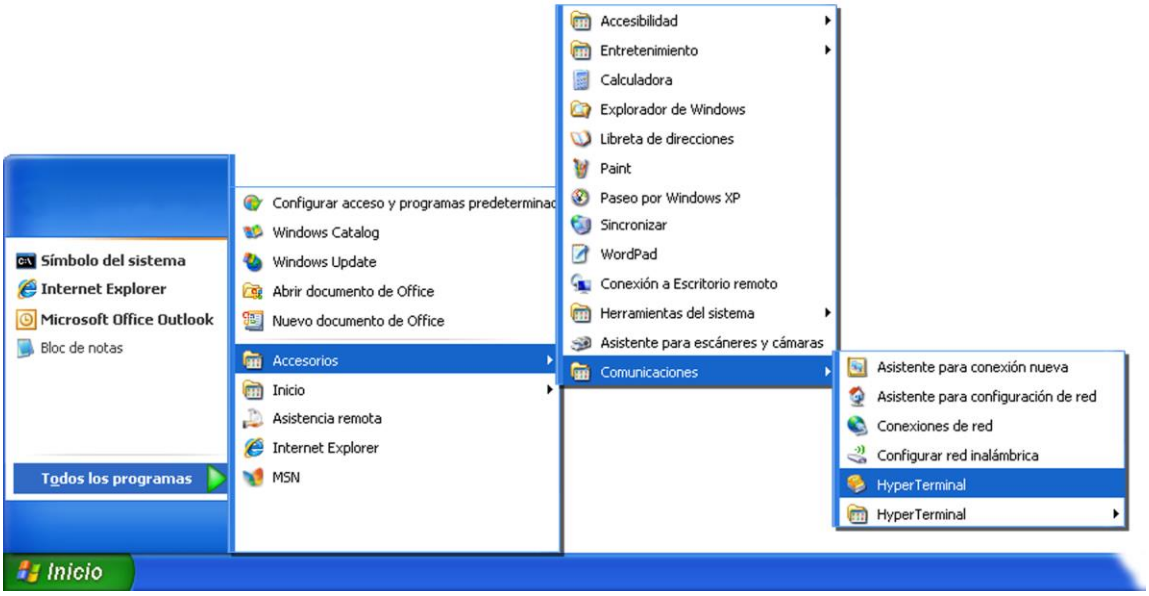
Local mode access is obtained through a flat serial cable that connects the serial port of the computer to the serial port of the equipment (SRV).

Communication between the computer and the equipment is established through a terminal emulation programme, such as Windows® *HyperTerminal*, configuring a serial connection with the following characteristics:

- Speed: 115.200 bps
- Data bits: 8
- Parity: No
- Stop bits: 1
- Flow control: No

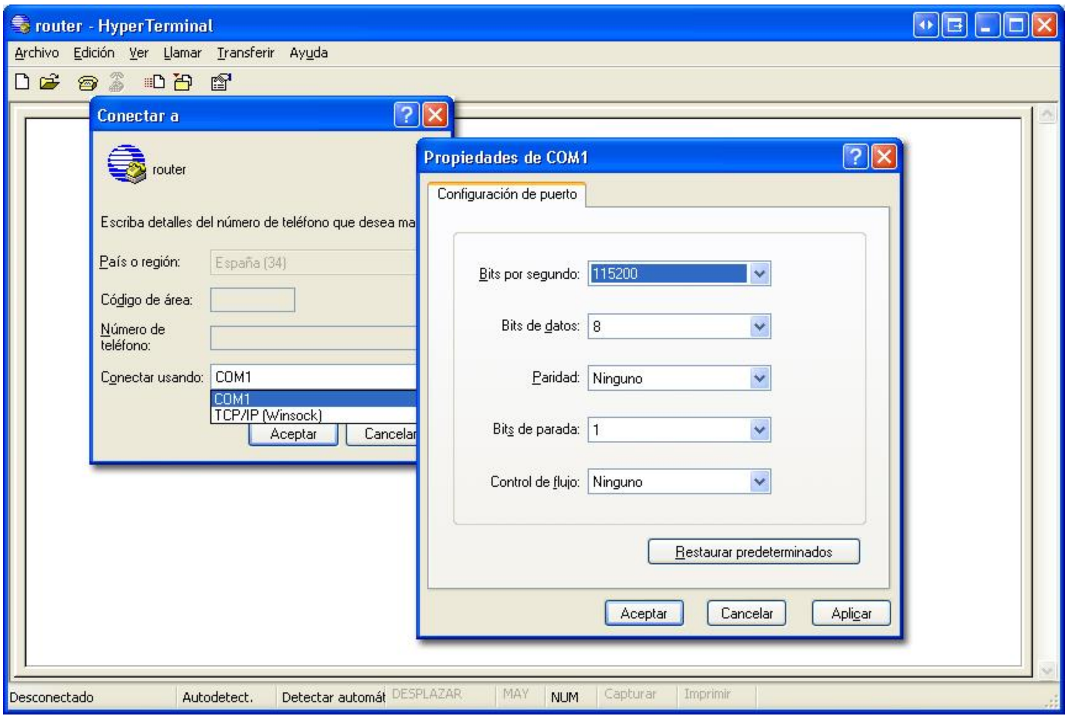
In Windows XP© execute *HyperTerminal* from *Start* → *All Programmes* → *Accessories* → *Communications* → *HyperTerminal* (see FIGURE 79).

FIGURE 79 Location of *HyperTerminal* in Windows XP©



On opening *HyperTerminal* a text box appears, requesting the necessary information to establish the connection (see FIGURE 80).

FIGURE 80 Connection configuration through the serial port with *HyperTerminal*



router

Escriba detalles del número de teléfono que desea ma

País o región: España (34)

Código de área:

Número de teléfono:

Conectar usando: COM1

COM1
TCP/IP (Winsock)

Bits por segundo: 115200

Bits de datos: 8

Paridad: Ninguno

Bits de parada: 1

Control de flujo: Ninguno

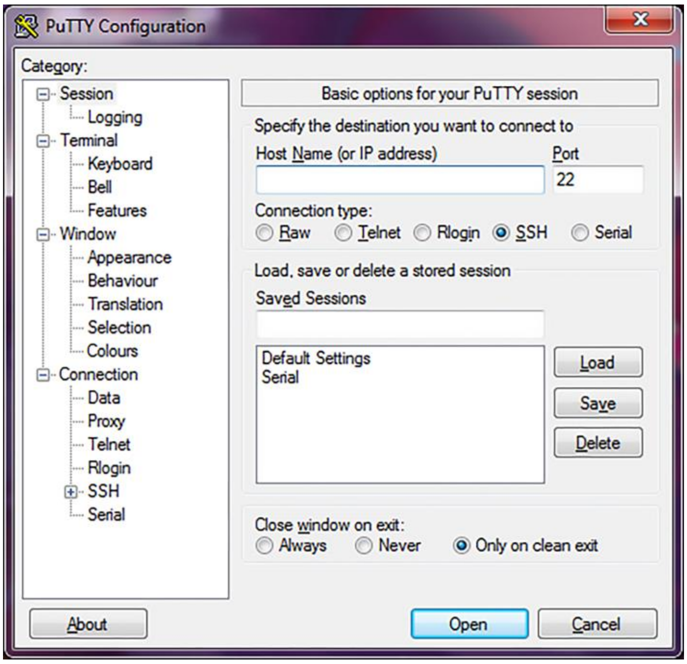
Run the *Call* option of the *Call* menu. Pressing return, a window is shown in which the ***swt login:*** prompt will appear, ready for the user to enter the *login* and code for starting the session (the logins and their respective passwords are the same as in the web interface).

> Remember that no text will appear in the *HyperTerminal* window when entering the password.

As operating systems like Microsoft Windows 7© no longer include the *HyperTerminal* program, the *Putty* program, free and executable, is also considered.

The *Putty* program is accessible on the www.putty.org web. Simply select the *Putty* that suits the operating system in use (usually the first, called **putty.exe**), copy it in the PC and run it.

FIGURE 81 *Putty* home window



Host Name (or IP address)

Port 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions

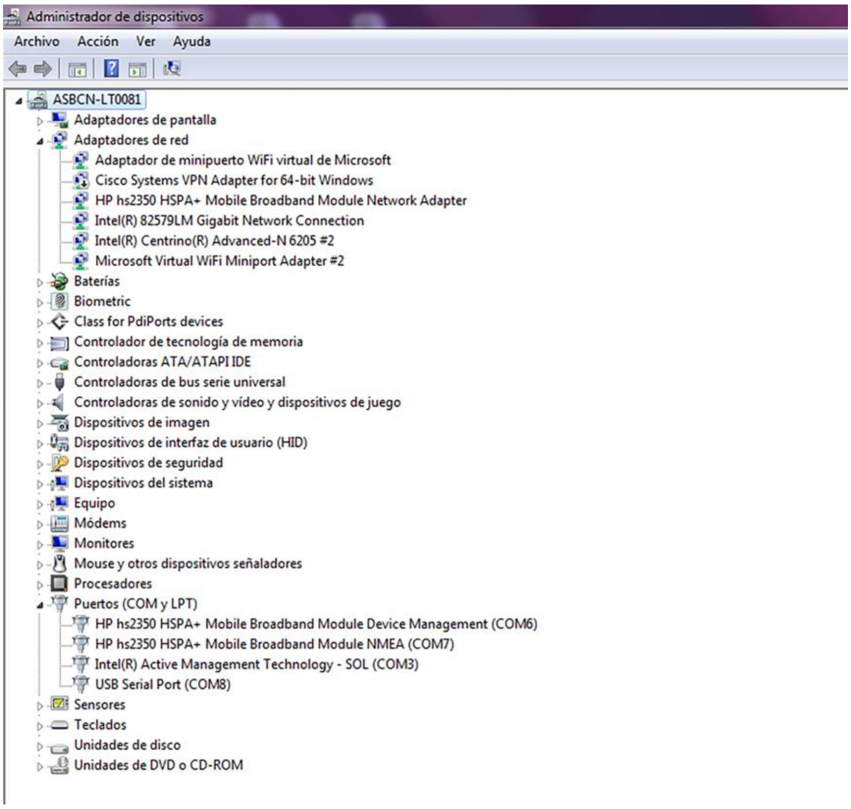
Default Settings
Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

In the ***Serial*** menu (last of all) the serial port is configured.

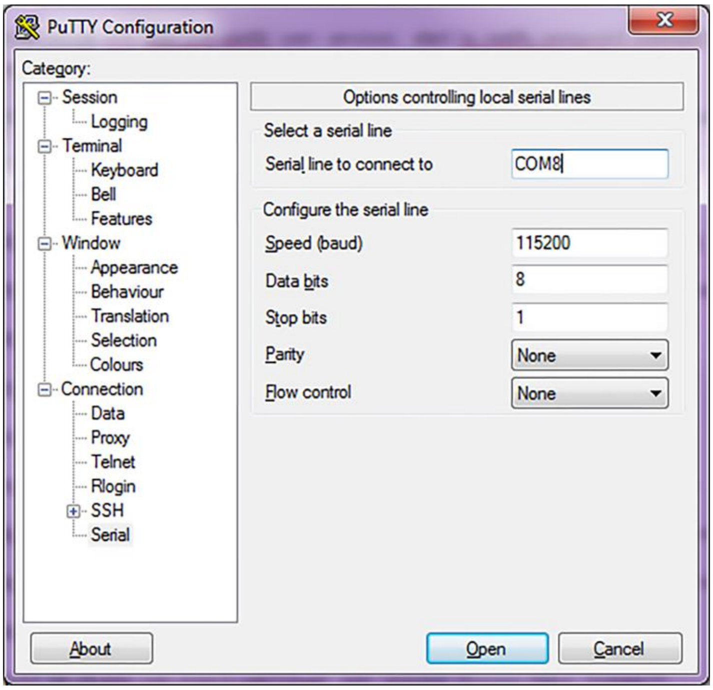
If an USB converter is used, first, consult the COM number in the *Device administrator* (Control panel).

FIGURE 82 *Device administrator* window



- ASBCN-LT0081
  - Adaptadores de pantalla
  - Adaptadores de red
    - Adaptador de minipuerto WiFi virtual de Microsoft
    - Cisco Systems VPN Adapter for 64-bit Windows
    - HP hs2350 HSPA+ Mobile Broadband Module Network Adapter
    - Intel(R) 82579LM Gigabit Network Connection
    - Intel(R) Centrino(R) Advanced-N 6205 #2
    - Microsoft Virtual WiFi Miniport Adapter #2
  - Baterías
  - Biometric
  - Class for PdiPorts devices
  - Controlador de tecnología de memoria
  - Controladoras ATA/ATAPI IDE
  - Controladoras de bus serie universal
  - Controladoras de sonido y vídeo y dispositivos de juego
  - Dispositivos de imagen
  - Dispositivos de interfaz de usuario (HID)
  - Dispositivos de seguridad
  - Dispositivos del sistema
  - Equipo
  - Módems
  - Monitores
  - Mouse y otros dispositivos señaladores
  - Procesadores
  - Puertos (COM y LPT)
    - HP hs2350 HSPA+ Mobile Broadband Module Device Management (COM6)
    - HP hs2350 HSPA+ Mobile Broadband Module NMEA (COM7)
    - Intel(R) Active Management Technology - SOL (COM3)
    - USB Serial Port (COM8)
  - Sensores
  - Teclados
  - Unidades de disco
  - Unidades de DVD o CD-ROM

FIGURE 83 Connection configuration through the serial port with *Putty*



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM8

Configure the serial line

Speed (baud): 115200

Data bits: 8

Stop bits: 1

Parity: None

Flow control: None

Pressing the *Open* button, and return if necessary, a window is shown in which the ***swt login:*** prompt will appear, ready for the user to enter the *login* and code for starting the session (the logins and their respective passwords are the same as in the web interface).

Remember that no text will appear in the *Putty* window when entering the password.

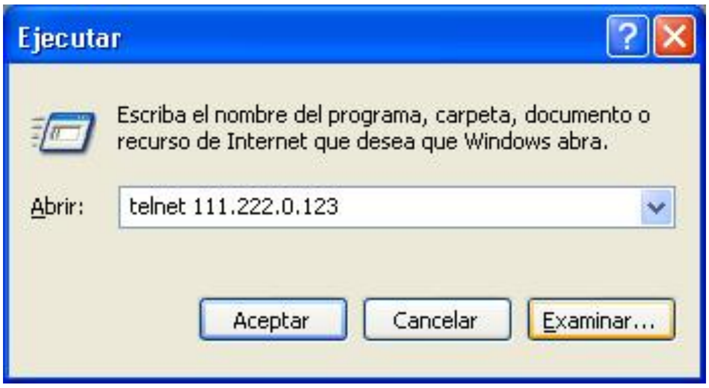
Access by means of Telnet

Access, in local and remote mode, is obtained with the *Telnet* command and equipment IP address.

> ! To use this access mode the equipment must have its IP address configured and be connected to the management computer network.

Telnet can be executed in Windows XP© from the Start button: *Start* → *Execute*, and in the text box, enter: *telnet* + *space* + *Equipment_IP_address* (111.222.0.123 in the example), and then press *Accept* (see FIGURE 84).

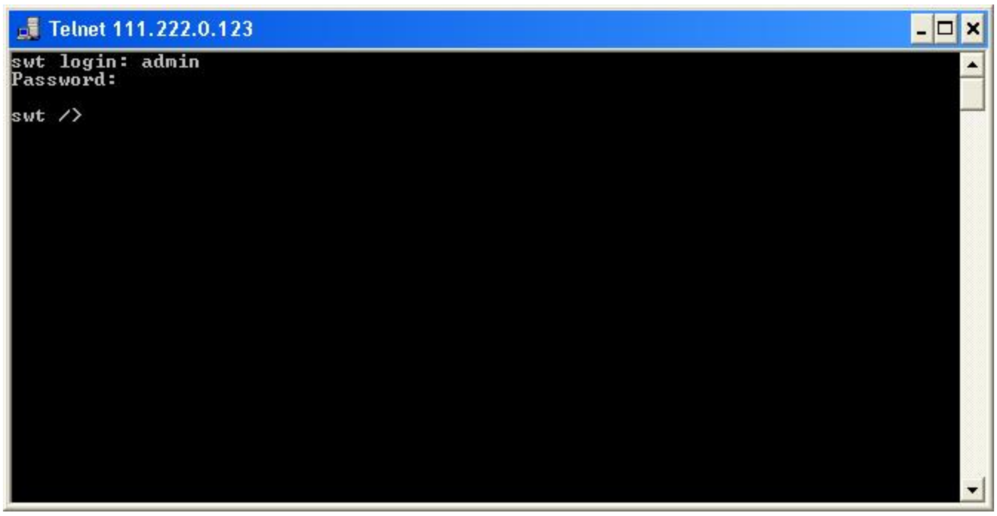
FIGURE 84 *Execute.. Telnet* text window to establish connection with the equipment


Ejecutar
Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea que Windows abra.
Abrir:
Aceptar
Cancelar
Examinar...

```
telnet 111.222.0.123
```

On pressing the Accept button a System symbol window will appear with the Telnet programme connected to the equipment (see FIGURE 85).

FIGURE 85 *Telnet* window



```
swt login: admin
Password:

swt />
```

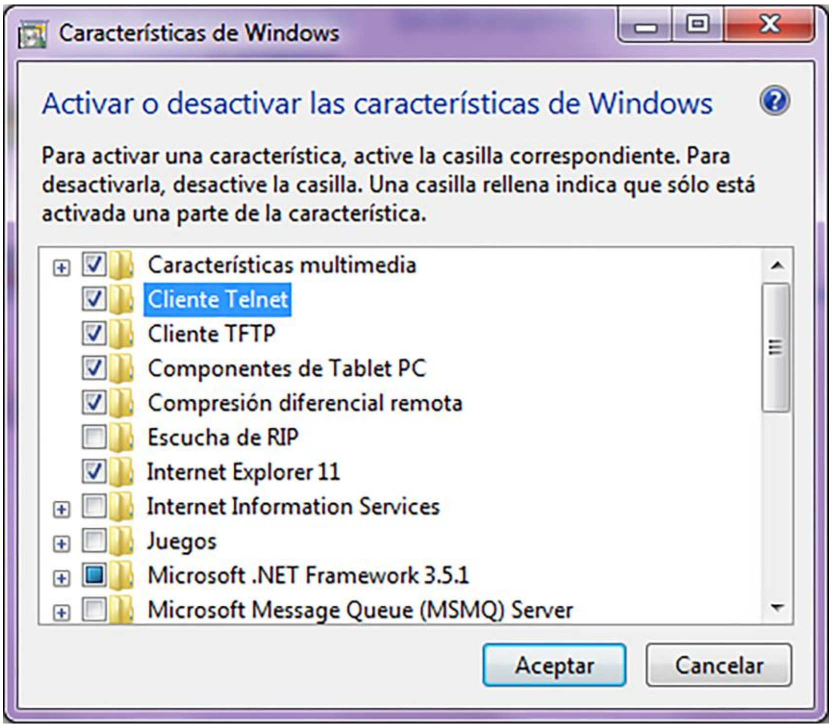
HyperTerminal can be used as the *Telnet* graphic interface. To do this, when configuring the connection select ***TCP/IP (Winsock)*** in the *Connect using* drop down menu.

Telnet can also be run from the *Putty* program. Simply, type the IP address of the equipment in the main window, and press *Open*.

Whatever the method chosen to establish connection with the equipment, the ***swt login*** prompt will appear: ready for the user to enter the *login* and code for starting the session (the logins and their respective passwords are the same as in the web interface).

> In operating systems like Microsoft Windows 7©, the Telnet client is disabled by default.
>
> To enable it, from the Start button: *Start* → *Control panel* → *All Programmes*, in *Programs and characteristics*, select *Activate or deactivate the Windows characteristics.*
>
> Then, in the window of *Characteristics of Windows*, select *Telnet client*, see FIGURE 86. By pressing *Accept,* the Telnet client of Windows may be used.

FIGURE 86 Window of characteristics of Windows



Características de Windows

Activar o desactivar las características de Windows

Para activar una característica, active la casilla correspondiente. Para desactivarla, desactive la casilla. Una casilla rellena indica que sólo está activada una parte de la característica.

- ☑ Características multimedia
- ☑ Cliente Telnet
- ☑ Cliente TFTP
- ☑ Componentes de Tablet PC
- ☑ Compresión diferencial remota
- □ Escucha de RIP
- ☑ Internet Explorer 11
- □ Internet Information Services
- □ Juegos
- ■ Microsoft .NET Framework 3.5.1
- □ Microsoft Message Queue (MSMQ) Server

B.2 USER CONSOLE COMMANDS

After starting the session with a valid login and password, the prompt will change to ***equipment />*** waiting for the user to enter a command.

The commands are instructions sent to the equipment to request or change a value or to “browse” through the tree in which the equipment parameters are organised.

The following table shows a full list of available commands with a brief description of each one and their availability depending on the type of user starting the session, highlighting the most useful ones.

TABLE 2 Full list of CLI user console commands

Command	Description	User	
		admin	guest
add	Adds a new item to a matrix-type parameter	✓	✗
apply	Applies the new configuration	✓	✗
cd	Changes the directory in the parameters tree	✓	✓
clear	Deletes the statistics	✓	✗
date	Shows the date stored in the equipment	✓	✗
download	Generates a configuration commands file	✓	✓
exit	Interrupts the connection with the equipment	✓	✓
get	Shows the parameter values	✓	✓
help	Shows the list of available commands	✓	✓
log	Shows the log file in use (current)	✓	✓
ls	Shows the lists of available parameters in the current directory	✓	✓
ping	Sends a ping to the indicated host	✓	✓
quit	Interrupts the connection with the equipment		
reboot	Reboots the equipment	✓	✗
reload	Loads a previously-saved configuration	✓	✗
remove	Eliminates an item from a matrix-type parameter	✓	✗
restore	Loads a default configuration	✓	✗
save	Saves all the changes made during the session	✓	✗
set	Modifies the value of a parameter	✓	✗
show	Allows the query of the log file in use and of the old log files. It also allows to display the file containing the customer default configuration	✓	✓
stats	Allows to obtain the status parameters of the equipment	✓	✓
tail	It is useful for monitoring the equipment during operation. It shows the list of events stored in the log file in use and it remains to show events as they occur. It closes with Ctrl+C	✓	✓
telnet	Open a telnet session without interrupting the connection with the equipment	✓	✓

Depending on the function of each command, they can be classified into different groups:

TABLE 3 Classification of commands based on their functions

Configuration	Control	Diagnostic
add	cd	clear
apply	exit	date
download	quit	help
get	reboot	log
remove	reload	ls
restore	telnet	ping
save		show
set		stats
		tail

Information in the log

The events that are generated at the system level and sent to the log include an identification level.

The system supports 8 different levels, separated into two blocks. The first set corresponds to unwanted situations, and the second block on information without affecting the functionality.

In the first block, the values are **emerg**, **alert**, **crit**, **err** and **warning**, which represents a decreasing level of severity in terms of the detected situation.

In the information block, the values are **notice**, **info** and **debug**, without having any connotation whatsoever for impact.

For more information, see section 5.1.4, *Syslog*.

Configuration commands

add Adds a new item to the matrix of a matrix-type parameter.

Syntax: swt /> **add** *name*

Arguments:

name Parameter to which a new item is to be added.

Observations: To add a new item to a matrix-type parameter, it is necessary to be in the directory in which it is located or enter the relative route.

The new item created has the next order number with respect to the last one. For instance, if *vif[1]* and *vif[2]* already existed, on executing the command add nat the item ***vif[3]*** is created.

Examples:

```
swt /> cd lan
swt /lan> add vif
swt /lan> cd vif[3]
swt/lan/vif[3]> set vid 3
```

apply This applies the configuration changes in the equipment, but without saving them.

Syntax: swt /> **apply**

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

This command DOES NOT save the changes made.

Example: swt /> **apply**

download This carries out a copy (back up) of the parameters configured in the equipment, which have a value different from the default value (factory) to be carried out. For this reason, this command is useful for configuring equipment with the same parameters as the current one.

Syntax: swt /> **download**

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

The list of commands shown starts with the command *restore*, which applies the factory configuration, followed by the commands required to obtain the current configuration.

It is a good idea to copy and save this list of commands in a .txt file, so it can be used in other equipment with the same characteristics.

> To apply the saved configuration in different equipment, it must be of the same model and version, and above all, have the same firmware version installed, since the factory configuration used to generate the commands list may be different in each one.

Example: swt /> **download**

get This shows the current values of one or several equipment configuration parameters.

Syntax: swt /> **get** [name]

Arguments: -

name (optional) name of the parameter to be shown.

Observations: The command *get* with no argument shows the values of all the configuration parameters in the current directory and its subdirectories. If the argument is the name of a directory it shows the values of the parameters in that directory. If the argument is the name of a configuration parameter, it shows the value of that parameter.

To show the complete configuration of the equipment, this command must be executed with no arguments, from the root directory.

If an argument is used, it must be in the current directory or the relative route must be entered.

Examples:

```
swt /> get
swt /> get main
swt /main> get hostname
swt /> get main/hostname
swt /admin> get ../main/hostname
```

remove This eliminates an item from the matrix of a matrix-type parameter.

Syntax: swt /> **remove** *name[nº]*

Arguments:

name Parameter from which the item is to be removed.

nº (Optional) Order number of the parameter item.

Observations: To remove an item from the matrix of a matrix-type parameter, it is necessary to be in the respective directory or enter the relative route.

If the order number of the item to be removed is indicated, that item will be removed. If the number is not indicated, the last one will be removed.

When removing an item that is not the last one, the other remaining items will be automatically renumbered.

Examples:

```
swt /> remove lan/vif[2]
swt /> remove lan/nat
swt /admin> remove ../lant/vif
```

restore This applies the factory configuration.

Syntax: swt /> **restore**

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

Example: swt /> **restore**

save This saves the changes made in configuring the equipment in its permanent memory. However, these changes will not take effect until the equipment is rebooted.

Syntax: swt /> **save**

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

Example: swt /> **save**

set This changes the value stored in the configuration parameters or in the attributes of an item in a matrix-type parameter.

Syntax: swt /> **set** [name][[nº][/name2]]

Arguments: -

name name of the parameter to be changed.

nº item number of a matrix-type parameter.

name2 name of an attribute in a matrix-type parameter.

Observations: When this command is executed the system waits for the new value to be entered.

The parameter to be changed must be in the current directory or its relative route must be entered.

In the case of wanting to change the value of any attribute in the item of a matrix-type parameter, the argument must include the parameter name, the item number and the attribute number.

Special attention should be paid when entering the arguments of this command, as if no argument is indicated the system will request the new value of each of the parameters in the active directory and its subdirectories, one by one. Consequently, if the *set* command is executed without an argument in the root directory, the system will request a new value for all the equipment configuration parameters.

If the *set* command is applied to a matrix-type parameter without indicating the attribute to be modified, the system will request a new value for each attribute of the indicated item. If the item number is omitted, the new values entered for each attribute will be applied to the last item in the matrix.

Examples:

```
swt /main> set hostname
swt /> set main/hostname
swt /admin> set ../main/hostname
```

Control commands

cd Changes the active directory.

Syntax: swt /> **cd** *name*

Arguments:

name Name of the destination directory.

Observations: The destination directory must be in the current directory or its relative route must be entered.

To activate the directory on the level immediately above it, two dots must be entered: ***cd ..***

When the directory is changed, the prompt shows the equipment identification letters and the name of the active directory. Example: ***swt /main>***.

Examples:

```
swt /> cd main
swt /main> cd ../admin
```

exit This closes the connection between the computer and the equipment, and therefore the CLI program session.

Syntax: swt /> **exit**

Arguments: -

Observations: -

Example: swt /> **exit**

quit This closes the connection between the computer and the equipment, and therefore the CLI program session.

Syntax: swt /> **quit**

Arguments: -

Observations: -

Example: swt /> **quit**

reboot This reboots the equipment without having to turn it off and on again, for instance, in order to apply the saved configuration changes.

Syntax: swt /> **reboot**

Arguments: -

Observations: -

Example: swt /> **reboot**

reload Reloads the saved configuration in the equipment.

Syntax: swt /> **reload**

Arguments: -

Observations: This command may be useful if it is required to reload the configuration saved in the equipment after the time it was saved.

Example: swt /> **reload**

telnet Open a telnet session, keeping the connection established between the computer and the equipment open.

Syntax: swt /> **telnet** *Host[Port]*

Arguments:

Host Name of the destination host to which open a Telnet session.

Port *(optional)* Number of the destination port where to open a Telnet session.

Observations: To restart the session, it is necessary to re-enter the login and password.
The 3 letters identifying the equipment can be used as the host name.

Example:

```
swt /> telnet swt
swt /> telnet 172.16.50.38 23
```

Status and Diagnostic Commands

clear Delete the statistics.

Syntax: swt /> **clear**

Arguments: -

Observations: -

Example: swt /> **clear**

date Shows the date and time recorded in the equipment.

Syntax: swt /> **date**

Arguments: -

Observations: -

Example: swt /> **date**

help Displays a list of all the available commands and a brief description of their functions.

Syntax: swt /> **help**

Arguments: -

Observations: -

Example: swt /> **help**

log Shows the list of events stored in the log file in use (current).

Syntax: swt /> **log**

Arguments:

- Without arguments, this command shows the events recorded in the current log file.

Observations: All the events taking place in the equipment are stored in files permanently. The maximum number of files is 5. The files are used in rotation but always remains a name that sets the timing, by using a suffix. The higher the suffix oldest is the file contents.

> Use the **show** command to display the oldest files.

You can filter at will the temporary log, using the text as a filter after the command. This operation works with any text in the filter, not only with the category (see section ***Information in the log***), so it is possible to filter traces of individual processes or selected events.

Example:

```
swt /> log
swt /> log crit
swt /> log debug
```

ls Shows a list from the active directory. This command is useful for verifying whether the configuration parameter to be consulted/changed is in the active directory.

Syntax: swt /> **ls**

Arguments: -

Observations: -

Example: swt /> **ls**

ping This sends ICPM ECHO_REQUEST packets to a specific host.

Syntax: swt /> **ping** *host*

Arguments:

host Host name or destination IP address.

Observations: When this command is executed the equipment starts to send pings to the indicated host until the user presses the ***Ctrl.***+***C*** keys.

Example:

```
swt /> ping 172.16.50.38
swt /> ping emr
```

show Shows the contents of the log file specified.

Syntax: swt /> **show** *file*

Arguments:

file Name of the file desired to display. The log file in use (current) is named *messages*. Oldest log files include a suffix, e.g. *messages.1*.

Observations: The maximum number of log files to display is 5: *messages* (current log), *messages.0, messages.1, messages.2* and *messages.3*. The files store data with periodic-continuous display. The higher the suffix oldest is the file contents.

The customer default configuration file is stored as *customer.txt*.

Example:

```
swt /> show messages
swt /> show messages.0
swt /> show messages.1
swt /> show messages.2
swt /> show messages.3

swt /> show customer.txt
```

stats This shows the equipment status parameters. These parameters are derived from the use made of the equipment, for instance, use of the memory of CPU, temperature, bytes transmitted, etc.

Syntax: swt /> **stats** [*parameter*]

Arguments:

parameter (Optional) Name of the parameter whose status is to be consulted.

Observations: Like the configuration parameters, these are classified by categories, in the form of a directories tree.
The normal use of this command is without arguments and from the root directory; it shows all the equipment status parameters.
To show a parameter for a specific status or those of a specific directory, the names of each one must be known.

> Once at swt/mac>, the execution of the command ***stats*** shows the MAC addresses identified by the switch.

Examples:

```
swt /> stats
swt /> stats main
swt main/> stats temperature
swt main/> stats ../lan/vif[2]/txbytes
```

tail This command is useful for monitoring the equipment and detecting potential errors during operation. It shows the list of events stored in the log file in use (current) and it remains to show events as they occur. It closes with ***Ctrl.+C***.

Syntax: swt /> **tail**

Arguments:

- Without arguments, this command shows the events recorded in the equipment non-volatile memory.

Observations: When this command is executed, the equipment remains to show all the events taking place in the equipment until the user presses the ***Ctrl.***+***C*** keys.

Example: swt /> **tail**

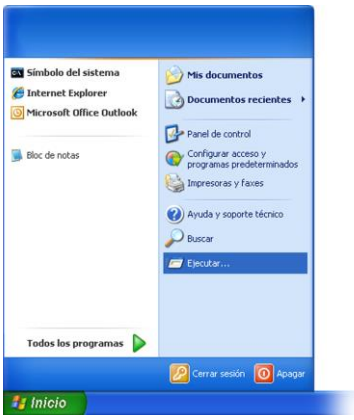
B.3 OBTAINING INFORMATION ABOUT THE STATUS AND EQUIPMENT CONFIGURATION

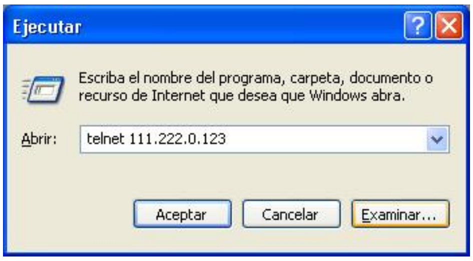
To obtain information about the status and equipment configuration, proceed as follows:

1- Connection with the equipment

As explained in chapter **B.1**, the equipment connection differs slightly depending on the chosen method. In this example, it is assumed that the equipment is connected to a network and with an IP address configured, which in the case of this example will be 111.222.0.123. In addition, the computer used to make the connection is also connected to that network and the O.S. used is *Windows XP*©.

To establish the connection through ***Telnet***, click on the *Windows XP*© ***Start*** button and once the menu has appeared, click on the command ***Execute***. In the window that appears, enter "***telnet 111.222.0.123***" (without inverted commas) and then press ***Accept***.

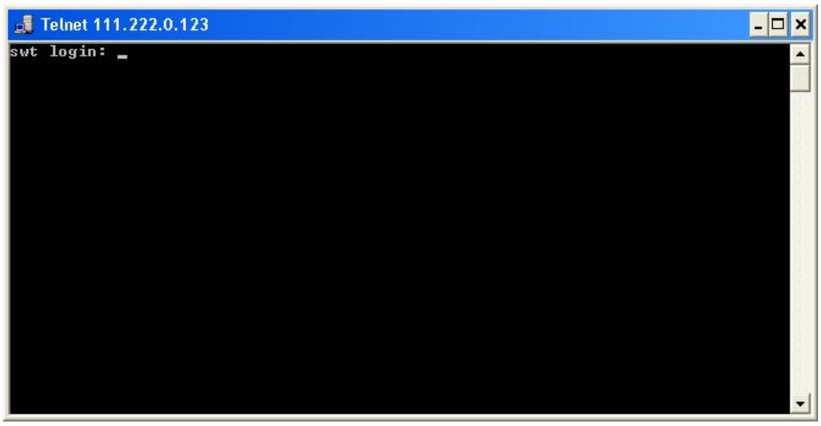



Ejecutar

Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea que Windows abra.

Abrir: telnet 111.222.0.123

If everything is functioning normally, a window will pop up with a system symbol, which is the interface for the connection.

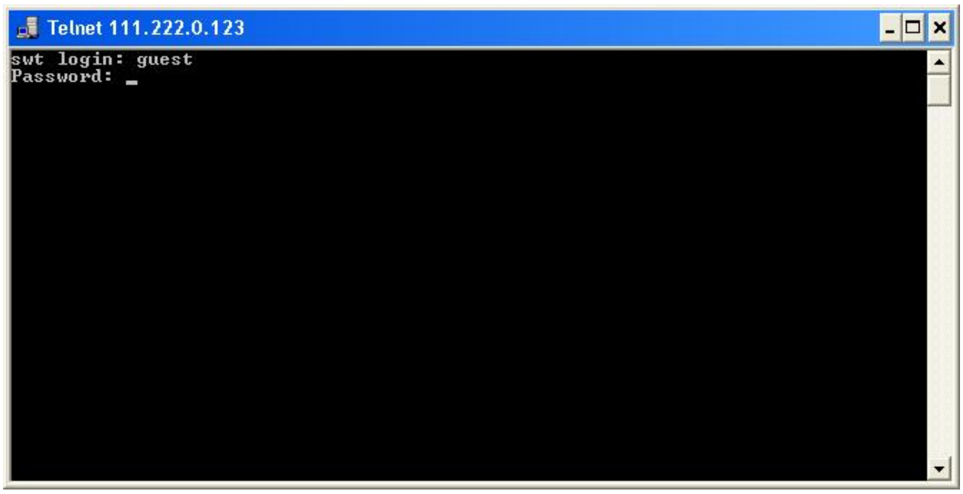

Telnet 111.222.0.123

```
swt login: _
```

2- User identification

On establishing connection with the equipment, the prompt ***swt login:*** indicates that the system is waiting for a user name to connect with the ***swt*** equipment.

Given that we only want information, it makes no difference which login is entered (***admin*** or ***guest***). Enter ***guest*** and then press ***enter.***

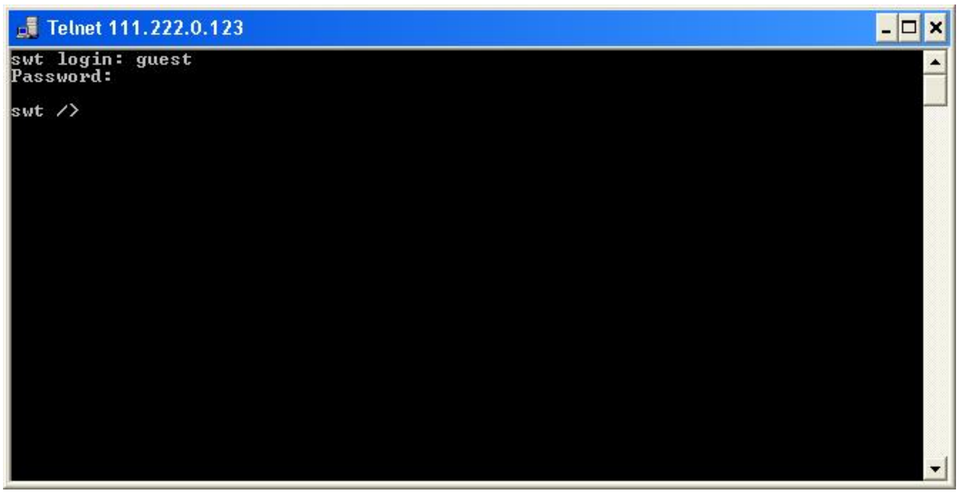


```
swt login: guest
Password: _
```

Now the system is waiting for us to enter the respective password. Enter ***passwd01*** which is the one associated with the *guest* user and press ***enter***.

> Remember that no text will appear in the *Telnet* window when entering the password.

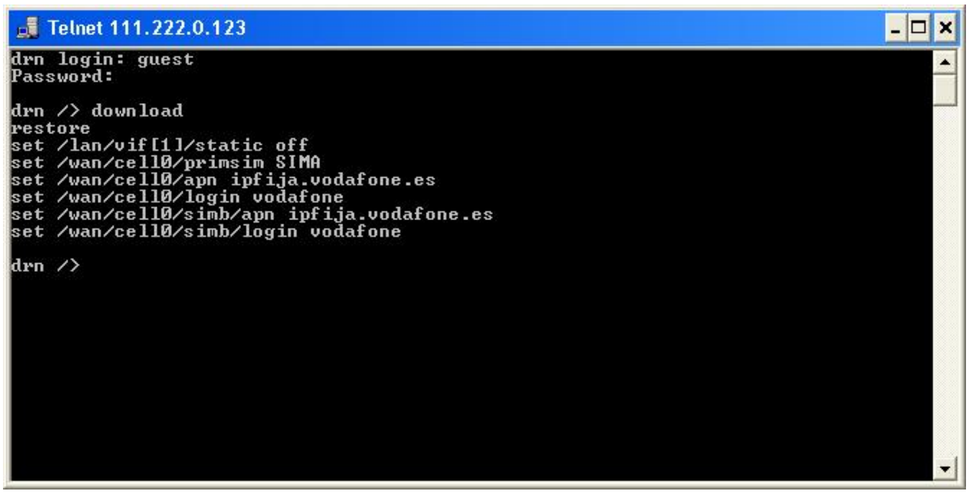
If the login and password entered are correct, the prompt ***swt />*** will appear, indicating that the equipment is waiting for a command to be entered.



```
swt login: guest
Password:

swt />
```

3- Obtaining the equipment configuration

The equipment configuration is obtained through the command ***download***. On pressing ***enter*** after this command, the full equipment configuration will be displayed. In this example, it is assumed that the equipment is a ***DRA-2***.

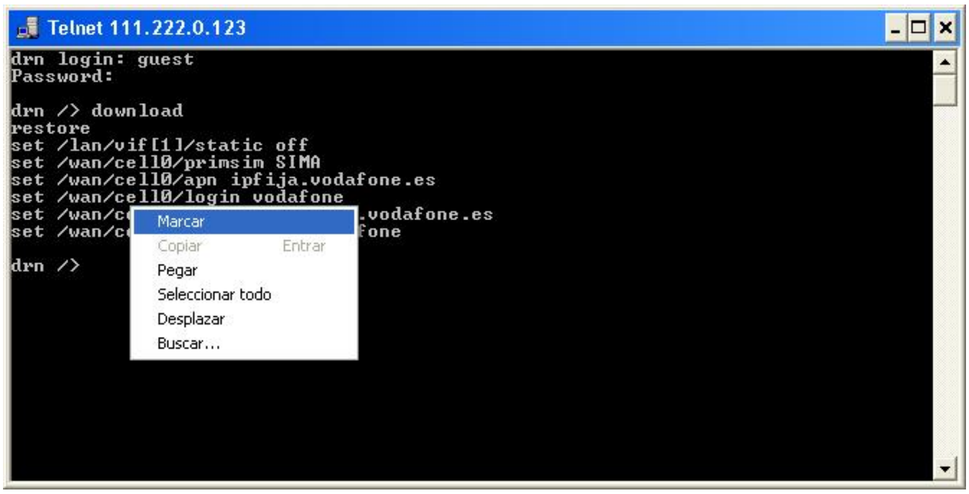


```
drn login: guest
Password:

drn /> download
restore
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/simb/apn ipfija.vodafone.es
set /wan/cell0/simb/login vodafone

drn />
```

If the information extends beyond the edges of the window, the system will only show the information at the start and it will be necessary to press ***enter*** once or several times for all the information to be shown. You will know whether the system has finished showing all the information when the equipment prompt reappears.

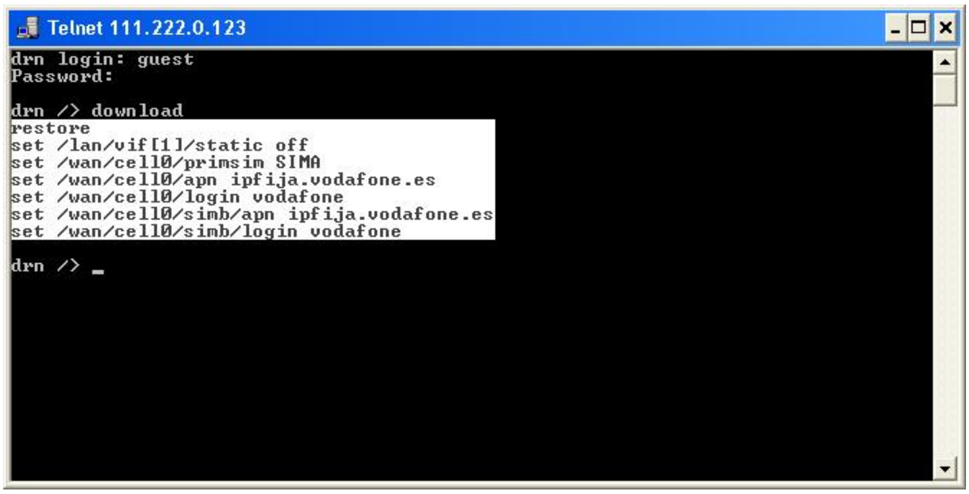
It is important to save the information in a ***.txt*** file using the *download* command so that it can be used whenever necessary.

To copy the text from the Windows XP© command window, right-click with the mouse and select ***Mark*** in the menu that appears.



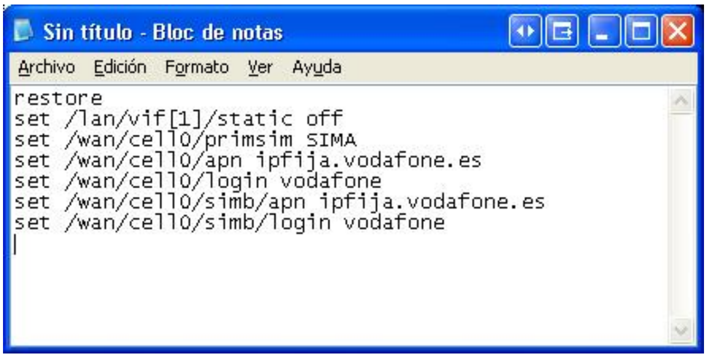
```
drn login: guest
Password:

drn /> download
restore
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/c                     .vodafone.es
set /wan/c                     fone

drn />
```

Then place the cursor at the start of the text to be copied, left-click with the mouse and drag the cursor, maintaining the button pressed, until all the text has been selected. After releasing the left button, press the ***enter*** key. That way, you will have copied the selected text into the Windows clipboard.



```
drn login: guest
Password:

drn /> download
restore
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/simb/apn ipfija.vodafone.es
set /wan/cell0/simb/login vodafone

drn /> _
```

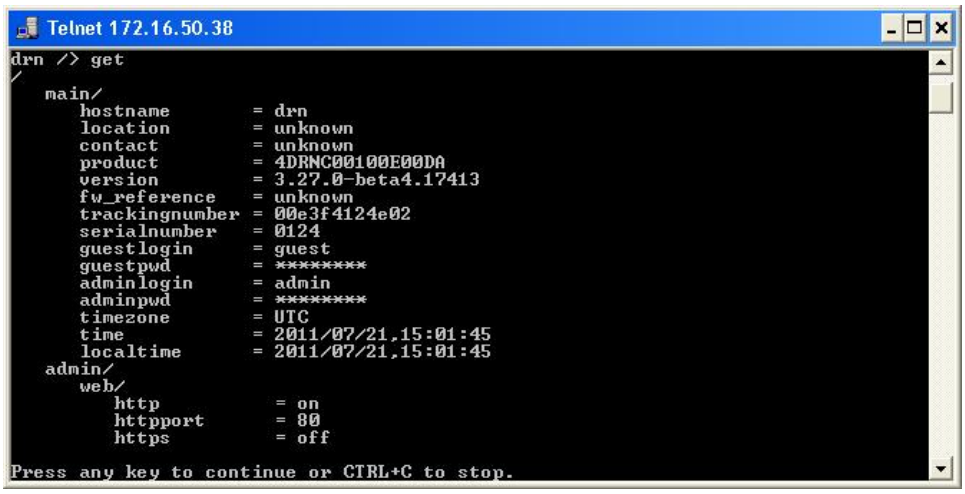
Now open Windows *Notepad* and paste the text (***Ctrl.*** + ***V***) in a ***.txt*** file and save it.



```
restore
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn ipfija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/simb/apn ipfija.vodafone.es
set /wan/cell0/simb/login vodafone
```

4- Obtaining the equipment status

The ***get*** command shows the full status of the equipment. Since the information shown is very lengthy, every time a window is filled, it will wait for the user to press a key to continue displaying the information. In this example, it is assumed that the equipment is a ***DRA-2.***



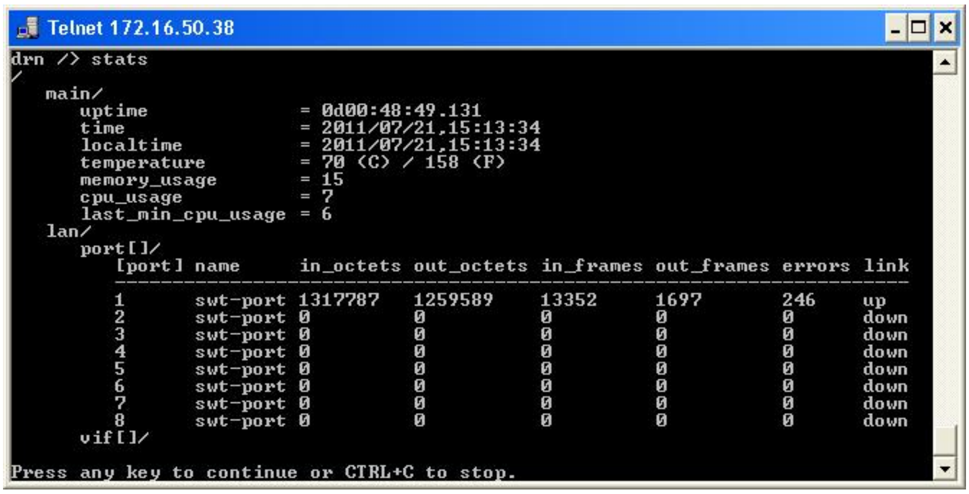
```
drn /> get
/
   main/
      hostname       = drn
      location       = unknown
      contact        = unknown
      product        = 4DRNC00100E00DA
      version        = 3.27.0-beta4.17413
      fw_reference   = unknown
      trackingnumber = 00e3f4124e02
      serialnumber   = 0124
      guestlogin     = guest
      guestpwd       = ********
      adminlogin     = admin
      adminpwd       = ********
      timezone       = UTC
      time           = 2011/07/21,15:01:45
      localtime      = 2011/07/21,15:01:45
   admin/
      web/
         http          = on
         httpport      = 80
         https         = off

Press any key to continue or CTRL+C to stop.
```

You will know whether the system has finished showing all the information when the equipment prompt reappears.

As with the *download* command, it is useful to save the information in a ***.txt*** file using the method described above.

5- Obtaining the equipment statistics

The equipment statistics list is shown through the command ***stats***. In this example, it is assumed that the equipment is a ***DRA-2.***



```
drn /> stats
/
   main/
      uptime             = 0d00:48:49.131
      time               = 2011/07/21,15:13:34
      localtime          = 2011/07/21,15:13:34
      temperature        = 70 (C) / 158 (F)
      memory_usage       = 15
      cpu_usage          = 7
      last_min_cpu_usage = 6
   lan/
      port[]/
         [port] name     in_octets out_octets in_frames out_frames errors link
         ---------------------------------------------------------------------
         1      swt-port 1317787   1259589    13352     1697       246    up
         2      swt-port 0         0          0         0          0      down
         3      swt-port 0         0          0         0          0      down
         4      swt-port 0         0          0         0          0      down
         5      swt-port 0         0          0         0          0      down
         6      swt-port 0         0          0         0          0      down
         7      swt-port 0         0          0         0          0      down
         8      swt-port 0         0          0         0          0      down
      vif[]/

Press any key to continue or CTRL+C to stop.
```

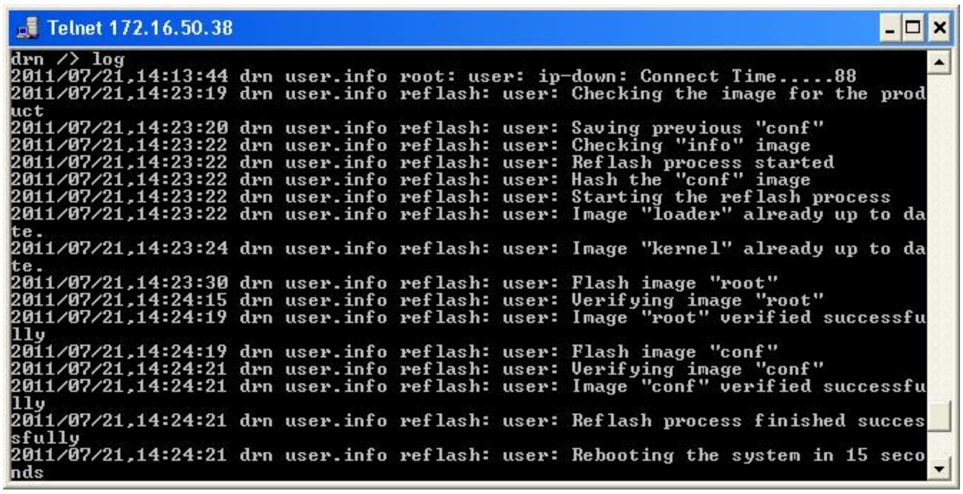
Like the previous commands, if the information to be displayed exceeds the edges of the window, it will stop and wait for the user to press a key to continue.

Remember to save the information in a ***.txt*** file as indicated above.

6- Obtaining events recorded in the equipment

The ***log*** command allows you to consult the list of events stored in the log file in use (current).

Use the ***show*** command to display the oldest log files. In this example, it is assumed that the equipment is a ***DRA-2.***



```
drn /> log
2011/07/21,14:13:44 drn user.info root: user: ip-down: Connect Time.....88
2011/07/21,14:23:19 drn user.info reflash: user: Checking the image for the prod
uct
2011/07/21,14:23:20 drn user.info reflash: user: Saving previous "conf"
2011/07/21,14:23:22 drn user.info reflash: user: Checking "info" image
2011/07/21,14:23:22 drn user.info reflash: user: Reflash process started
2011/07/21,14:23:22 drn user.info reflash: user: Hash the "conf" image
2011/07/21,14:23:22 drn user.info reflash: user: Starting the reflash process
2011/07/21,14:23:22 drn user.info reflash: user: Image "loader" already up to da
te.
2011/07/21,14:23:24 drn user.info reflash: user: Image "kernel" already up to da
te.
2011/07/21,14:23:30 drn user.info reflash: user: Flash image "root"
2011/07/21,14:24:15 drn user.info reflash: user: Verifying image "root"
2011/07/21,14:24:19 drn user.info reflash: user: Image "root" verified successfu
lly
2011/07/21,14:24:19 drn user.info reflash: user: Flash image "conf"
2011/07/21,14:24:21 drn user.info reflash: user: Verifying image "conf"
2011/07/21,14:24:21 drn user.info reflash: user: Image "conf" verified successfu
lly
2011/07/21,14:24:21 drn user.info reflash: user: Reflash process finished succes
sfully
2011/07/21,14:24:21 drn user.info reflash: user: Rebooting the system in 15 seco
nds
```

Remember to save the information in a ***.txt*** file, as indicated above.

7- Obtaining events taking place in the equipment in real time

The ***tail*** command allows users to monitor the events taking place in the equipment in real time. Once the command is activated, it will remain to show events as they occur until the user presses ***Ctrl.+C***.

Remember to save the information in a ***.txt*** file, as indicated above.

8- Example of a list showing the equipment status obtained with the get command and saved in a .txt file

```
swt /> get
/
   main/
      hostname       = l3ptp-2.108-3.37
      location       = unknown
      contact        = unknown
      product        = SW3MJYUJON3200A
      version        = 3.37.0.42192
      fw_reference   = 4WF72030004-R000
      trackingnumber = d4493c1f587b99ea
      serialnumber   = 1000004
      guestlogin     = guest
      guestpwd       =
tH4sIAOMmEVwCAzM0AAET7YLE4uLyFANDAOgqxwsQAAAAODBmZmIzZmE0YjcwVOGFiZjQ0Y2M4ZTFiOWE0YmEwYWUK
      adminlogin     = admin
      adminpwd       =
tH4sIAOMmEVwCAzM0AAET7YLE4uLyFAMjAFJ7zpIQAAAAOGQ3MmIyMTk5YjdlVZDA4M2MyY2Q2NzYzYjRlZDViN2MK
      timezone       = Madrid
      time           = 2018/12/12,15:18:59
      localtime      = 2018/12/12,16:18:59
   admin/
      web/
         http          = on
         httpport      = 80
         https         = on


Press any key to continue or CTRL+C to stop. [A
 [J      httpsport     = 443
         cert          = empty
         privatekey    = empty
         privatekeypwd =
tH4sIAOMmEVwCAzM0AAET7ZLU4pKMkpKCYgCxAS9dEQAAAGM5NmIxNTA5NjNiWMTRjNmQwNGU4Y2ZmMzg5NDRiZjhlCg==
         ftp           = on
         ftps          = on
      cli/
         syslog_level        = 8
         syslog_level_remote = 4
         syslog              = off
         syslog_server       = 0.0.0.0
      reset/
         enable = off
         period = 1
   qinq/
      stag = 0x88A8
   lan/
      port[]/
         [port] name     enable vlan_function mode vid vid_acl lag  lag_config
         ----------------------------------------------------------------------
         1      e1       on     edge          auto 1   auto    none off
         2      e2       on     edge          auto 1   auto    none off


Press any key to continue or CTRL+C to stop. [A
 [J        3      e3       on     edge          auto 1   auto    none off
         4      e4       on     edge          auto 1   auto    none off
         5      e5       on     edge          auto 1   auto    none off
         6      e6       on     edge          auto 1   auto    none off
         7      e7       on     edge          auto 1   auto    none off
         8      e8       on     edge          auto 1   auto    none off
         9      e9       on     edge          auto 1   auto    none off
         10     e10      on     edge          auto 1   auto    none off
         11     swt-port on     edge          auto 1   auto    none off
         12     swt-port on     edge          auto 1   auto    none off
         13     swt-port on     edge          auto 1   auto    none off
         14     swt-port on     edge          auto 1   auto    none off
         15     swt-port on     edge          auto 1   auto    none off
         16     swt-port on     edge          auto 1   auto    none off
         17     swt-port on     edge          auto 1   auto    none off
         18     swt-port on     edge          auto 1   auto    none off
         19     swt-port on     edge          auto 1   auto    none off
         20     swt-port on     edge          auto 1   auto    none off
         21     swt-port on     edge          auto 1   auto    none off
         22     swt-port on     edge          auto 1   auto    none off
         23     swt-port on     edge          auto 1   auto    none off
         24     swt-port on     edge          auto 1   auto    none off


Press any key to continue or CTRL+C to stop. [A
 [J        25     swt-port on     edge          auto 1   auto    none off
         26     swt-port on     edge          auto 1   auto    none off
         27     swt-port on     edge          auto 1   auto    none off
         28     swt-port on     edge          auto 1   auto    none off
      vlanoverlapping/
         enable = off
      vif[]/
         [vif] vid ip           mask          description dhcprelay dhcprelay_ip
         -----------------------------------------------------------------------
         1     1   10.212.2.108 255.255.254.0 vlan_name   off       192.168.0.1
         2     2   10.140.0.1   255.255.255.0 vlan_name   off       192.168.0.1
         3     3   10.150.0.1   255.255.255.0 vlan_name   off       192.168.0.1
         4     4   0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         5     5   0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         6     6   0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         7     7   0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         8     8   0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         9     9   0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         10    10  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         11    11  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         12    12  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         13    13  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1


Press any key to continue or CTRL+C to stop. [A
 [J        14    14  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         15    15  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         16    16  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         17    17  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         18    18  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         19    19  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
         20    20  0.0.0.0      255.255.255.0 vlan_name   off       192.168.0.1
   qos/
      qos2/
         weightfair_enable = on
         priority[]/
            [priority] queue
            -----------------
            0          medium
            1          medium
            2          medium
            3          medium
            4          medium
            5          medium
            6          medium
            7          medium
         dscp[]/


Press any key to continue or CTRL+C to stop. [A
 [J            [dscp] queue
            -------------
            0      medium
            8      medium
            16     medium
            24     medium
            32     medium
            40     medium
            48     medium
            56     medium
         port[]/
            [port] priority use_ieee8021p use_dscp
            --------------------------------------
            1      0        on            off
            2      0        on            off
            3      0        on            off
            4      0        on            off
            5      0        on            off
            6      0        on            off
            7      0        on            off
            8      0        on            off
            9      0        on            off


Press any key to continue or CTRL+C to stop. [A
 [J            10     0        on            off
            11     0        on            off
            12     0        on            off
            13     0        on            off
            14     0        on            off
            15     0        on            off
            16     0        on            off
            17     0        on            off
            18     0        on            off
            19     0        on            off
            20     0        on            off
            21     0        on            off
            22     0        on            off
            23     0        on            off
            24     0        on            off
            25     0        on            off
            26     0        on            off
            27     0        on            off
            28     0        on            off
         vlan[]/
            [vlan] vid priover priority
            ---------------------------


Press any key to continue or CTRL+C to stop. [A
 [J            1      1   off     0
   rate_control/
      ingress[]/
         [ingress] enable traffic rate
         ------------------------------
         1         off    all     64000
         2         off    all     64000
         3         off    all     64000
         4         off    all     64000
         5         off    all     64000
         6         off    all     64000
         7         off    all     64000
         8         off    all     64000
         9         off    all     64000
         10        off    all     64000
         11        off    all     64000
         12        off    all     64000
         13        off    all     64000
         14        off    all     64000
         15        off    all     64000
         16        off    all     64000
         17        off    all     64000


Press any key to continue or CTRL+C to stop. [A
 [J         18        off     all     64000
         19        off    all     64000
         20        off    all     64000
         21        off    all     64000
         22        off    all     64000
         23        off    all     64000
         24        off    all     64000
         25        off    all     64000
         26        off    all     64000
         27        off    all     64000
         28        off    all     64000
      egress[]/
         [egress] enable rate
         ---------------------
         1        off    64000
         2        off    64000
         3        off    64000
         4        off    64000
         5        off    64000
         6        off    64000
         7        off    64000
         8        off    64000


Press any key to continue or CTRL+C to stop. [A
 [J         9        off    64000
         10       off    64000
         11       off    64000
         12       off    64000
         13       off    64000
         14       off    64000
         15       off    64000
         16       off    64000
         17       off    64000
         18       off    64000
         19       off    64000
         20       off    64000
         21       off    64000
         22       off    64000
         23       off    64000
         24       off    64000
         25       off    64000
         26       off    64000
         27       off    64000
         28       off    64000
   monitor/
      ingress_enable    = off


Press any key to continue or CTRL+C to stop. [A
 [J      ingress_dest_port = 7
      egress_enable     = off
      egress_dest_port  = 7
      port[]/
         [port] ingress egress
         ---------------------
         1      off     off
         2      off     off
         3      off     off
         4      off     off
         5      off     off
         6      off     off
         7      off     off
         8      off     off
         9      off     off
         10     off     off
         11     off     off
         12     off     off
         13     off     off
         14     off     off
         15     off     off
         16     off     off


Press any key to continue or CTRL+C to stop. [A
 [J         17     off     off
         18     off     off
         19     off     off
         20     off     off
         21     off     off
         22     off     off
         23     off     off
         24     off     off
         25     off     off
         26     off     off
         27     off     off
         28     off     off
   mac/
      age_time = 300
   stp/
      enable        = off
      version       = rstp
      priority      = 32768
      max_age       = 20.000000000
      hello_time    = 2.000000000
      forward_delay = 15.000000000
      tx_hold_count = 6


Press any key to continue or CTRL+C to stop. [A
 [J      port[]/
         [port] enable priority cost   edge ptp  edge_tx_filter
         ------------------------------------------------------
         1      on     128      200000 auto auto off
         2      on     128      200000 auto auto off
         3      on     128      200000 auto auto off
         4      on     128      200000 auto auto off
         5      on     128      200000 auto auto off
         6      on     128      200000 auto auto off
         7      on     128      200000 auto auto off
         8      on     128      200000 auto auto off
         9      on     128      200000 auto auto off
         10     on     128      200000 auto auto off
         11     on     128      200000 auto auto off
         12     on     128      200000 auto auto off
         13     on     128      200000 auto auto off
         14     on     128      200000 auto auto off
         15     on     128      200000 auto auto off
         16     on     128      200000 auto auto off
         17     on     128      200000 auto auto off
         18     on     128      200000 auto auto off
         19     on     128      200000 auto auto off


Press any key to continue or CTRL+C to stop. [A
 [J         20     on     128      200000 auto auto off
         21     on     128      200000 auto auto off
         22     on     128      200000 auto auto off
         23     on     128      200000 auto auto off
         24     on     128      200000 auto auto off
         25     on     128      200000 auto auto off
         26     on     128      200000 auto auto off
         27     on     128      200000 auto auto off
         28     on     128      200000 auto auto off
   lldp/
      enable = on
      port[]/
```

```
         [port] admin_status transmit_interval hold_multiplier reinit_delay credit_max
trans_interval_fast number_message_fast_tx notification_enable tx_portdesc tx_sysname tx_sysdesc
tx_syscap tx_management management_address
         ----------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------
--------------------
         1      TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0
         2      TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0
         3      TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0
         4      TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0
         5      TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0
         6      TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0
         7      TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0
         8      TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0


Press any key to continue or CTRL+C to stop. [A
 [J         9      TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0
         10     TxRx         30                4               2            5          1
4                      off                 on          on         off        on        off
0.0.0.0
         11     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         12     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         13     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         14     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         15     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         16     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         17     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         18     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         19     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         20     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         21     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         22     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         23     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         24     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         25     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         26     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         27     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
         28     TxRx         30                4               2            5          1
4                      off                 off         off        off       off        off
0.0.0.0
   igmp_snooping/
      enable = off


Press any key to continue or CTRL+C to stop. [A
 [J      port[]/
         [port] igmp_forward
         -------------------
         1      auto
         2      auto
         3      auto
         4      auto
         5      auto
         6      auto
         7      auto
         8      auto
         9      auto
         10     auto
         11     auto
         12     auto
         13     auto
         14     auto
         15     auto
         16     auto
         17     auto
         18     auto
         19     auto


Press any key to continue or CTRL+C to stop. [A
 [J         20     auto
         21     auto
         22     auto
         23     auto
         24     auto
         25     auto
         26     auto
         27     auto
         28     auto
   garp_timers/
      port[]/
         [port] join_time leave_time leaveall_time
         -----------------------------------------
         1      200       600        10000
         2      200       600        10000
         3      200       600        10000
         4      200       600        10000
         5      200       600        10000
         6      200       600        10000
         7      200       600        10000
         8      200       600        10000
         9      200       600        10000


Press any key to continue or CTRL+C to stop. [A
 [J         10     200       600        10000
         11     200       600        10000
         12     200       600        10000
         13     200       600        10000
         14     200       600        10000
         15     200       600        10000
         16     200       600        10000
         17     200       600        10000
         18     200       600        10000
         19     200       600        10000
         20     200       600        10000
         21     200       600        10000
         22     200       600        10000
         23     200       600        10000
         24     200       600        10000
         25     200       600        10000
         26     200       600        10000
         27     200       600        10000
         28     200       600        10000
   routing/
      static/
         default_st_rules[]/


Press any key to continue or CTRL+C to stop. [A
 [J            [default_st_rules] gateway      if    metric descr
            --------------------------------------------------
            1                  10.212.3.254 vlan1 1
      dns/
         dns_enabled = off
      rip/
         enable            = off
         advertised_policy = permit
      ospf/
         enable              = on
         router_id           = 10.212.2.108
         abr_type            = standard
         dist_default_policy = permit
         areas[]/
            [areas] network                  area    auth
            ---------------------------------------------
            1       10.212.2.0/255.255.254.0 0.0.0.0 on
         interfaces[]/
            [interfaces] if    cost hello_interval dead_interval media_type priority auth keyid
md5digest
            -------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
            1            vlan1 10   10             40           broadcast  1        on   2
tH4sIAOQmEVwCAzM0AAET7arMMiMDQzMAskOO6w8AAABhMWQyZGQxYjcyYTg2UZDFlNThkYTEyOGJhZTIyNzMxNAo=
         distribution[]/


Press any key to continue or CTRL+C to stop. [A
 [J            [distribution] type
            -------------------
            1              BGP
      bgp/
         enable           = on
         asn              = 64515
         router_id        = 10.212.2.108
         port             = 179
         cluster_id       = 0.0.0.0
         confederation_id = 0
         peers[]/
            [peers] ip           rem_as local_as_action local_as keepalive holdtime allowas_in weight
multihop next_hop_self default_originate passive reflec_client remove_priv_as port maximum_prefix
max_prefix_action max_prefix_warning_threshold max_prefix_restart
            -------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------
-----------------------------------------------------------
            1       10.212.1.205 64516  not-used        1        60        180       0          0      5
off           off               off     off           off            179  0              restart
0                            5
            2       10.212.2.109 64515  not-used        1        60        180       0          0      0
off           off               off     off           off            179  0              restart
0                            5
         distribution[]/
            [distribution] type
            ------------------------
            1              connected
            2              OSPF
   filter/
      local/
```

```
Press any key to continue or CTRL+C to stop. [A
 [J         policy = accept
      vlan/
         policy = accept
   dhcps/
      profiles[]/
         [profiles] name    lease dns1    dns2    wins    domain      tftp        bootfile
         ---------------------------------------------------------------------------------
         1          profile 5000  0.0.0.0 0.0.0.0 0.0.0.0 usyscom.com 192.168.0.1 bootfile
      servers[]/
         [servers] enable interface firstip      lastip        max_leases mask          gateway
profile
         ----------------------------------------------------------------------------------------------
----
         1         off                192.168.0.10 192.168.0.254 100        255.255.255.0 192.168.0.1
profile
   vrrp/
      pingkeep/
         remoteip     = 0.0.0.0
         gateway      = 0.0.0.0
         freq         = 0
         timeout      = 10
         bytes        = 1
         count        = 2
         evalmodel    = period
         evalperiod   = 10


Press any key to continue or CTRL+C to stop. [A
 [J         maxlostratio = 40
         action       = none
   ntp/
      enable   = on
      protocol = ntp
      authkeys[]/
         [authkeys] keynumber key
         -----------------------------
         1          1         xxxxxxxx
      client/
         broadcastenable = off
         server[]/
            [server] ip           type    minpoll maxpoll authenable authkey lowtraffic
            ---------------------------------------------------------------------------
            1        10.212.1.205 unicast 5       10      off        1       off
      sntp/
         client[]/
            [client] ip          poll units   authenable authkey timeout
            ------------------------------------------------------------
            1        192.168.0.1 1    minutes off        1       5
   ptp/
      enable                      = off


Press any key to continue or CTRL+C to stop. [A
 [J      profile                     = IEC 61850
      primary_sytonization_domain = 1
      vlan_syntonization_clock    = 1
      priority                    = 4
      enable_sync_clock           = off
      enable_ports[]/
         [enable_ports] port_enable port_asymmetry
         -----------------------------------------
         1              on          0
         2              on          0
         3              on          0
         4              on          0
         5              on          0
         6              on          0
         7              on          0
         8              on          0
         9              on          0
         10             on          0
         11             on          0
         12             on          0
         13             on          0
         14             on          0


Press any key to continue or CTRL+C to stop. [A
 [J         15             on          0
         16             on          0
         17             on          0
         18             on          0
         19             on          0
         20             on          0
         21             on          0
         22             on          0
         23             on          0
         24             on          0
         25             on          0
         26             on          0
         27             on          0
         28             on          0
   igmp/
      enable = off
   gmrp/
      enable = off
      port[]/
         [port] forward_all
         ------------------
         1      normal


Press any key to continue or CTRL+C to stop. [A
 [J         2      normal
         3      normal
         4      normal
         5      normal
         6      normal
         7      normal
         8      normal
         9      normal
         10     normal
         11     normal
         12     normal
         13     normal
         14     normal
         15     normal
         16     normal
         17     normal
         18     normal
         19     normal
         20     normal
         21     normal
         22     normal
         23     normal


Press any key to continue or CTRL+C to stop. [A
 [J         24      normal
         25     normal
         26     normal
         27     normal
         28     normal
   snmp/
      enable              = on
      trapenable          = off
      trap_v1_aggent_addr = none
      community[]/
         [community] name   access
         -------------------------
         1           public ro
      user[]/
         [user] name   access security auth_alg auth_passwd
priv_alg priv_passwd
         ----------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------
--------------------------------------------
         1      public ro     clear    MD5
tH4sIAOUmEVwCAzM0AAET7cTSktS8kszkxBIAqGHEjRIAAAAzYjM4ZjY0ZDllXMWY0MGViZTcyMDdjOTY1ZjNlODQ2Ngo= DES
tH4sIAOUmEVwCAzM0AAET7YrMtKLEktTi5NKiEgCgTr3sFAAAAGQ4YzRlOWFjZMjcxOGYwMjJhZTUzYjRlNmYyZmUzNDczCg==
      traps/
         dig_in_change  = off
         dig_out_change = off
         lldp_change    = off
   access/


Press any key to continue or CTRL+C to stop. [A
 [J      tacacsplus/
         server1_ip = 0.0.0.0
         server2_ip = 0.0.0.0
         encrypted  = on
         shared_key =
tH4sIAOUmEVwCAzM0AAETbQB1gaviCAAAAGNjZWEwZmM4Mjk3NTdjNWY0OTY4NNWQ3MmNkZTg1YzU4Cg==
         guest_lvl  = 1
         admin_lvl  = 2
      radius/
         server1_ip = 0.0.0.0
         server2_ip = 0.0.0.0
         udp_port   = 1812
         secret     =
tH4sIAOUmEVwCAzM0AAET7arMMkMjYxNTAPpzLn0QAAAAYTlmOGQzYmYxMzQ1VOGJlOTVmY2M4NmRiM2E5NjFjMTEK
         timeout    = 10
         guest_lvl  = 1
         admin_lvl  = 2
      console/
         method = local
      web/
         method = local
         local  = on
      telnet/
         method = local


Press any key to continue or CTRL+C to stop. [A
 [J         local   = on
      ssh/
         method = local
         local  = on
      ftp/
         method = local
         local  = on
   security/
      port[]/
         [port] type  max_addresses max_action
         -------------------------------------
         1      none  10            replace
         2      none  10            replace
         3      none  10            replace
         4      none  10            replace
         5      none  10            replace
         6      none  10            replace
         7      none  10            replace
         8      none  10            replace
         9      none  10            replace
         10     none  10            replace
         11     none  10            replace


Press any key to continue or CTRL+C to stop. [A
 [J         12      none  10            replace
         13     none  10            replace
         14     none  10            replace
         15     none  10            replace
         16     none  10            replace
         17     none  10            replace
         18     none  10            replace
         19     dot1x 10            replace
         20     none  10            replace
         21     none  10            replace
         22     none  10            replace
         23     none  10            replace
         24     none  10            replace
         25     none  10            replace
         26     none  10            replace
         27     none  10            replace
         28     none  10            replace
      dot1x/
         enable        = on
         reauth_enable = on
         reauth_period = 3600
         reauth_max    = 2


Press any key to continue or CTRL+C to stop. [A
 [J         quiet_period  = 60
         radius_server/
            ip       = 10.212.4.5
            udp_port = 1812
            secret   =
tH4sIAOUmEVwCAzM0AAETbSMjAzMDc2MDQ3MAX3QNbBIAAAA5Y2IyMGQwMjg0XYjNiYTkyZGFkNzk3MDk4ZjFjZDgwYwo=
   digital_out/
      enable_alarm = off

swt />
```

B.4 CERTIFICATE INSTALLATION FOR HTTPS MANAGEMENT

The server integrated in the equipment supports the HTTP and the HTTPS protocols, in the last case being necessary the installation of certificates.

The procedure for loading the certificates for HTTPS management, ***once the certificate, the private key and the password of the last one have been got***, is the following:

1- Access the configuration section of the web interface, through the SRV port (“**cd /admin/web**”).

2- Load in “**cert**” a valid **certificate** with the command “**upload cert raw**”.
The procedure for loading the certificate is the following. ***Copy*** in the clipboard ***the certificate***. Then, ***execute the indicated upload command*** and, when it is in wait period, ***paste the data from the clipboard***. Wait approximately 30s. When the time is elapsed, the data are shown.

3- Load in “**privatekey**” a valid **private key** with the command “**upload privatekey raw**”.
The procedure is the same that the one indicated previously for the certificate.

4- Introduce the **password of the private key** in “**privatekeypwd**” with the command “**set privatekeypwd**”.
Confirmation of the password is required twice as much.

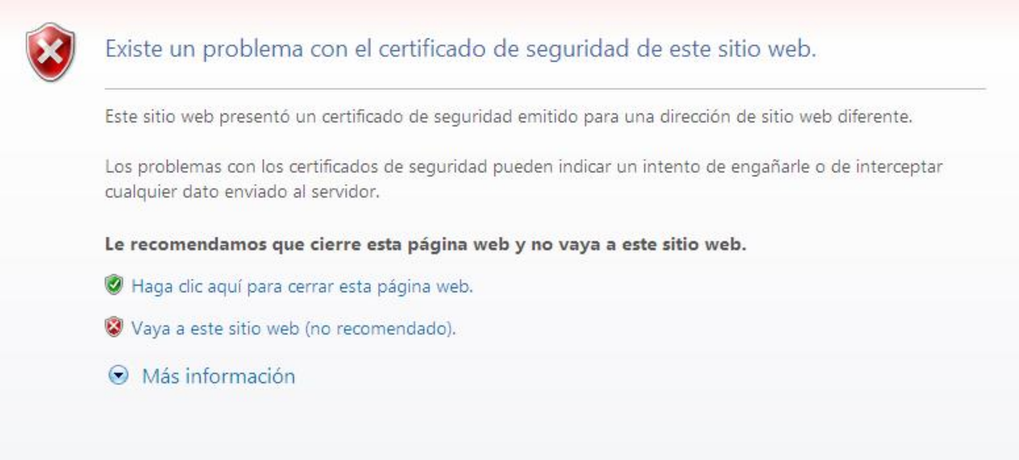
5- In the equipment, activate the access by means of HTTPS (“**set https on**”).

6- Apply the changes (“**apply**”).

7- Save the new data (optional) (“**save**”).

8- **Load** the equipment configuration web page in the browser (Microsoft Internet Explorer, Mozilla Firefox, etc. Google Chrome is not supported) [(1)]typing "**https://**" instead of http://".

The following message appears:



Existe un problema con el certificado de seguridad de este sitio web.

Este sitio web presentó un certificado de seguridad emitido para una dirección de sitio web diferente.

Los problemas con los certificados de seguridad pueden indicar un intento de engañarle o de interceptar cualquier dato enviado al servidor.

Le recomendamos que cierre esta página web y no vaya a este sitio web.

Haga clic aquí para cerrar esta página web.

Vaya a este sitio web (no recomendado).

Más información

Although the certificate operates correctly, this message is a warning indicating that the certificate has not been validated by a trusted authority.

Select "**Go to this web site (not recommended)**".

Then, the equipment access control requires the user **login** and **password**.

In the equipment with HTTPS operation, the ***certificate,*** the ***private key*** and the ***password of the last*** are part of the data obtained by means of the "**download**" command. Therefore, it is possible to add this information to the configuration pattern.

[(1)] The operation is a success with Microsoft Internet Explorer and Mozilla Firefox. Google Chrome doesn't accept the certificates authorized by you.

Example of download command in the equipment (EMR-2) with HTTPS operation:

```
emr2 /> download
restore
set /main/hostname emr2
set /main/timezone Madrid
set /admin/web/https on
set       /admin/web/cert       "-----BEGIN       CERTIFICATE-----
\nMIICWzCCAcQCCQCcL+NbBdYynDANBgkqhkiG9w0BAQUFADByMQswCQYDVQQGEwJF\
nUzESMBAGA1UECBMJQmFyY2Vsb25hMRIwEAYDVQQHEwlCYXJjZWxvbmExDDAKBgNV\n
BAoTA1pJVjEOMAwGA1UEAxMFSm9zZXAxHTAbBgkqhkiG9w0BCQEWDmouc2FsYXRA\ne
ml2LmVzMB4XDTEzMDMyNzE1NTAzOVoXDTE0MDMyNzE1NTAzOVowcjELMAkGA1UE\nBh
MCRVMxEjAQBgNVBAgTCUJhcmNlbG9uYTESMBAGA1UEBxMJQmFyY2Vsb25hMQww\nCgY
DVQQKEwNaSVYxDjAMBgNVBAMTBUpvc2VwMR0wGwYJKoZIhvcNAQkBFg5qLnNh\nbGF0
QHppdi5lczCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt49IfdfD/xVO\nGsqL2
17s6aumdFWr9NYoJw68LbrHY0VZ9OGwen+alXAjBcl2lqLZjf1lOh250aWE\neZLH31
lD5bxS9c+w8YrwXoWEnYOxUQpK49YGvH7DnqLAyI5ptyQbdyMoTkMcxBOZ\njNoToVi
oGiZ9GRBg6nKCDC4+PxN3/90CAwEAATANBgkqhkiG9w0BAQUFAAOBgQAT\n7QtOOJT6
lLcGciF4R5aooiRoZEiTJQBFm6PoTZ21apGGhF1Bz0FPn3LRxC1Mb6PI\nkNatYteCq
5FJNjGunF8hDIQVc1x7O2ju2vmGOiyVfSz1eqiy+Tx0dMYsgpBeY3K+\n8fb+J1jmLP
NzPhgMlzPK6VGNA70/QhfCG9l5xK1oWQ==\n-----END CERTIFICATE-----"
set    /admin/web/privatekey    "-----BEGIN    RSA    PRIVATE    KEY-----
\nMIICWwIBAAKBgQC3j0h918P/FU4ayovbXuzpq6Z0Vav01ignDrwtusdjRVn04bB6\
nf5qVcCMFyXaWotmN/WU6HbnRpYR5ksffWUPlvFL1z7DxivBehYSdg7FRCkrj1ga8\n
fsOeosDIjmm3JBt3IyhOQxzEE5mM2hOhWKgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB\nA
oGAOvDzYhVKhjodHlUzm3lbsZzAklKAKNorgn8kxbpYE/RM8mkV9f/Lb3jWhiEu\nxy
f7m7BmNMcex8bSRwduzrUnK66DW8jP3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S\nApu
oZFYmh34uBl6SJkUdihCs4jM1ocQBQMHQ7mXe7Sk1sgECQQDgpSDx45vm8Yk+\nGoX4
UzcRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcNOpU8bFtQbWfxjkThHthQBN\nrUeER
Ej9AkEA0S4ernXQGVJGm7b6JhJXFKkILVYo5vP0C3jx7ByRIMt4lkll4l7Q\ntzNepK
jlcmimzLWuHJAiyTBtvzfVcnU4YQJAaXOaX3HkwSgosIpq0QLfGp7yJNQu\nqt5h+vZ
O6FTuSFPm3tOD4G0K6MlN0nKNIEm2CAJpgOJU8BY66jupEqGrUQJAW7Wp\ns/lpJEDj
Pg/p+lkeHqvBLwdQZXldbM442rjnlAZBNzq01ZuWTEvUWcLG3fMt9iBN\nVq6G4cg+x
ZA4H7du4QJALq/zgc4N+Ft5OHkj+ay1XSt5nxH8U2Zk1u7ZWZZhOTcw\nezG/TDLBWk
ROF2n9VX6TYGesnZ2Ve/+DiMPhK7ZVQA==\n-----END RSA PRIVATE KEY------"
set /admin/web/privatekeypwd testhttps
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn gnftsg.com
set /wan/cell0/login pruebas_ziv1
set /wan/cell0/passwd pruebas_ziv1
set /snmp/enable on
set /access/tacacsplus/server1_ip 10.132.2.148
set /access/tacacsplus/server2_ip 10.132.2.168
set /access/tacacsplus/shared_key Sm4rt3Sy13
set /access/tacacsplus/admin_lvl 15
set /access/web/method tacacsplus
```

If there are no available certificate, private password and password of the last, it is possible to create them. For example, following the instructions in http://www.akadia.com/services/ssh_test_certificate.html, but in this case it is necessary a Linux equipment to execute the instructions.

An example of certificate, as well as private key, is shown in the following.

Pay attention that both the header and bottom lines are part of the certificate.

Example of a valid **certificate**:

```
-----BEGIN CERTIFICATE-----
MIICWzCCAcQCCQCcL+NbBdYynDANBgkqhkiG9w0BAQUFADByMQswCQYDVQQGEwJF
UzESMBAGA1UECBMJQmFyY2Vsb25hMRIwEAYDVQQHEwlCYXJjZWxvbmExDDAKBgNV
BAoTA1pJVjEOMAwGA1UEAxMFSm9zZXAxHTAbBgkqhkiG9w0BCQEWDmouc2FsYXRA
eml2LmVzMB4XDTEzMDMyNzE1NTAzOVoXDTE0MDMyNzE1NTAzOVowcjELMAkGA1UE
BhMCRVMxEjAQBgNVBAgTCUJhcmNlbG9uYTESMBAGA1UEBxMJQmFyY2Vsb25hMQww
CgYDVQQKEwNaSVYxDjAMBgNVBAMTBUpvc2VwMR0wGwYJKoZIhvcNAQkBFg5qLnNh
bGF0QHppdi5lczCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt49IfdfD/xVO
GsqL217s6aumdFWr9NYoJw68LbrHY0VZ9OGwen+alXAjBcl2lqLZjf1lOh250aWE
eZLH31lD5bxS9c+w8YrwXoWEnYOxUQpK49YGvH7DnqLAyI5ptyQbdyMoTkMcxBOZ
jNoToVioGiZ9GRBg6nKCDC4+PxN3/90CAwEAATANBgkqhkiG9w0BAQUFAAOBgQAT
7QtOOJT6lLcGciF4R5aooiRoZEiTJQBFm6PoTZ21apGGhF1Bz0FPn3LRxC1Mb6PI
kNatYteCq5FJNjGunF8hDIQVc1x7O2ju2vmGOiyVfSz1eqiy+Tx0dMYsgpBeY3K+
8fb+J1jmLPNzPhgMlzPK6VGNA70/QhfCG9l5xK1oWQ==
-----END CERTIFICATE-----
```

Example of a valid **private key**:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQC3j0h918P/FU4ayovbXuzpq6Z0Vav01ignDrwtusdjRVn04bB6
f5qVcCMFyXaWotmN/WU6HbnRpYR5ksffWUPlvFL1z7DxivBehYSdg7FRCkrj1ga8
fsOeosDIjmm3JBt3IyhOQxzEE5mM2hOhWKgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB
AoGAOvDzYhVKhjodHlUzm3lbsZzAklKAKNorgn8kxbpYE/RM8mkV9f/Lb3jWhiEu
xyf7m7BmNMcex8bSRwduzrUnK66DW8jP3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S
ApuoZFYmh34uBl6SJkUdihCs4jM1ocQBQMHQ7mXe7Sk1sgECQQDgpSDx45vm8Yk+
GoX4UzcRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcNOpU8bFtQbWfxjkThHthQBN
rUeEREj9AkEA0S4ernXQGVJGm7b6JhJXFKkILVYo5vP0C3jx7ByRIMt4lkll4l7Q
tzNepKjlcmimzLWuHJAiyTBtvzfVcnU4YQJAaXOaX3HkwSgosIpq0QLfGp7yJNQu
qt5h+vZO6FTuSFPm3t0D4G0K6MlN0nKNIEm2CAJpgOJU8BY66jupEqGrUQJAW7Wp
s/lpJEDjPg/p+lkeHqvBLwdQZXldbM442rjnlAZBNzq01ZuWTEvUWcLG3fMt9iBN
Vq6G4cg+xZA4H7du4QJALq/zgc4N+Ft5OHkj+ay1XSt5nxH8U2Zk1u7ZWZZhOTcw
ezG/TDLBWkROF2n9VX6TYGesnZ2Ve/+DiMPhK7ZVQA==
-----END RSA PRIVATE KEY-----
```