

GIGABIT/FAST ETHERNET SWITCH TYPE SWT



USER GUIDE

V10 - July 2019

M0SWTA1907lv10

ZIV
Carrer de les Ciències, 149-151
08908 L'Hospitalet de Llobregat,
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
1 INTRODUCTION	6
1.1 GENERAL	6
1.2 MAIN CHARACTERISTICS	6
1.3 EQUIPMENT COMPOSITION	10
1.4 TECHNICAL SPECIFICATIONS	11
1.4.1 Switch characteristics	11
1.4.2 Unit interfaces	11
1.4.3 Accessories	12
1.4.4 Equipment management	13
1.4.5 Additional services	13
1.4.6 Certifications	13
1.4.7 Mechanical characteristics	14
1.4.8 Operating conditions	14
1.5 WARNINGS	16
1.5.1 Warnings before installing	16
1.5.2 Equipment safety considerations	17
2 MECHANICAL AND ELECTRICAL CHARACTERISTICS	18
2.1 10/100BASE-TX (RJ-45) PORTS	22
2.2 100BASE-FX (MULTIMODE, MT-RJ) PORTS	24
2.3 100BASE-FX (MULTIMODE, ST or SC) PORTS	24
2.4 100BASE-FX (MULTIMODE, LC) PORTS	25
2.5 100BASE-LX (SINGLEMODE, LC) PORTS	25
2.6 SFP PORTS	26
2.7 SRV PORT	28
2.8 I/O CONNECTOR	29

	Page
3	LED SIGNALLING 30
3.1	SWT WITH FRONT PORTS 30
3.2	SWT WITH REAR PORTS 34
4	ACCESS TO THE EQUIPMENT 37
4.1	CONSOLE 37
4.2	HTTP SERVER 38
5	CONFIGURATION AND MANAGEMENT 40
5.1	GENERAL PARAMETERS 41
5.1.1	Equipment identification 42
5.1.2	Access control 42
5.1.3	Others 42
5.1.4	Syslog 43
5.2	ADMINISTRATION 44
5.3	LAN CONFIGURATION 46
5.4	ETHERNET PORTS CONFIGURATION 47
5.5	VLAN CONFIGURATION 51
5.6	BANDWIDTH LIMIT CONFIGURATION 55
5.7	QoS CONFIGURATION 56
5.8	PORTS MONITORING CONFIGURATION 59
5.9	LLDP CONFIGURATION 61
5.10	SNMP CONFIGURATION 64
5.11	STP PROTOCOL CONFIGURATION 66
5.12	NTP/SNTP CONFIGURATION 70
5.13	MULTICAST CONFIGURATION 72
5.13.1	Static 75
5.13.2	GMRP 76
5.13.3	IGMP 78

	Page
5.14 ACCESS CONFIGURATION	79
5.15 SECURITY CONFIGURATION	82
5.15.1 802.1x	83
5.15.2 MAC list	84
5.16 OTHERS CONFIGURATION	85
5.17 REBOOT	86
5.18 CODE REFLASH	87
5.19 CONFIGURATION FILE	88
5.19.1 Upload (from the PC to the equipment)	88
5.19.2 Download (from the equipment to the PC)	89
5.20 EVENT FILES	89
6 STATISTICS	90
APPENDIX A	
BIBLIOGRAPHY AND ABBREVIATIONS	96
APPENDIX B	
DATA STRUCTURE IN CLI	101

1 INTRODUCTION

1.1 GENERAL

SWT is a Gigabit/Fast Ethernet switch intended for big scale LAN deployments where:

- port density,
- switching performance, and
- logical complexity

are the main challenges to surpass.

SWT devices bring the necessary capabilities to implement the automation of electrical substations according to the IEC 61850 standard.

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

The SWT also supports the SNMPv1, SNMPv2c and SNMPv3 protocols, as well as other protocols and services such as LLDP, GARP/GMRP, IGMP, NTP/SNTP, TACACS+ and RADIUS.

1.2 MAIN CHARACTERISTICS

Some of the SWT 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 equipment such as the SWT, or links between switching equipment, 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 ID (VID) identifier and the priority (tagged) or only the priority (priority tagged, VLAN = 0).

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

SWT

FIGURE 1 Traffic separation

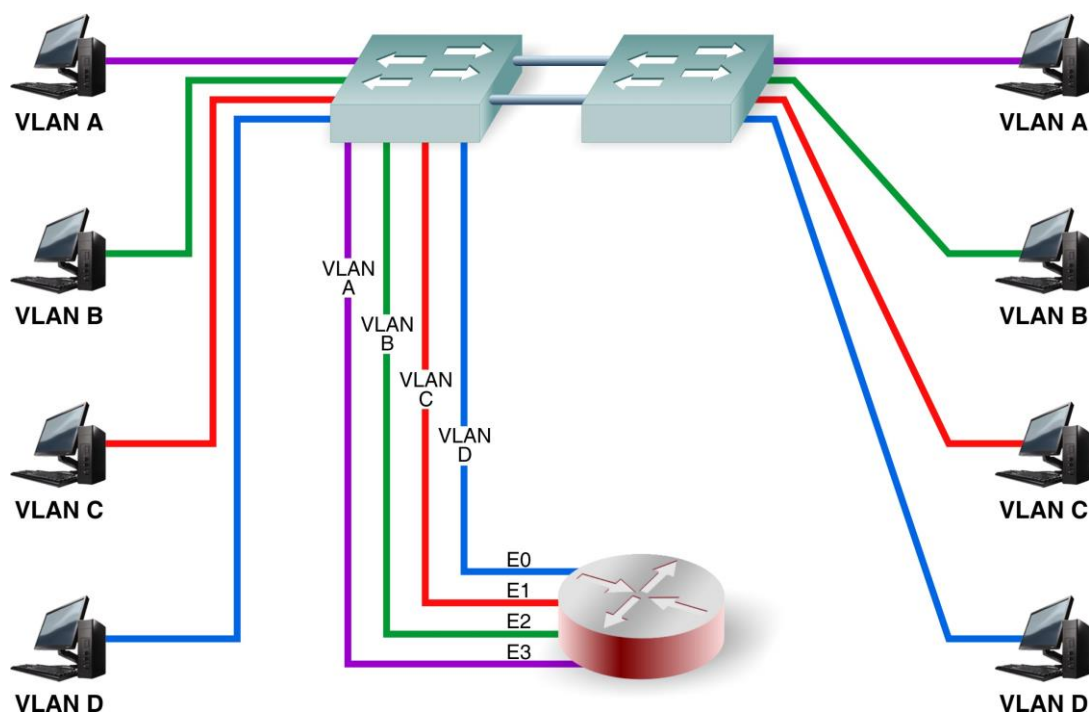


FIGURE 2 Star topology

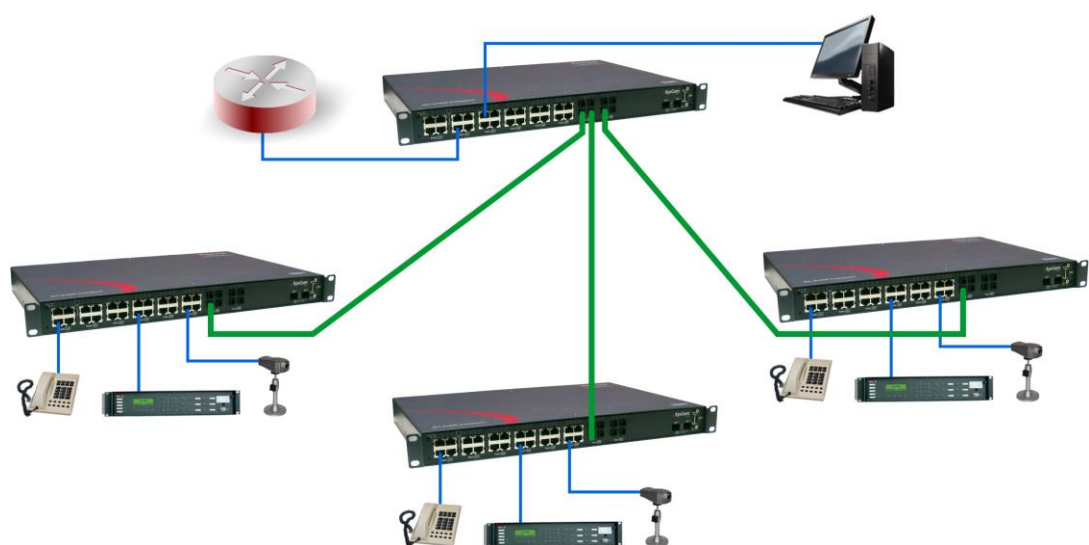
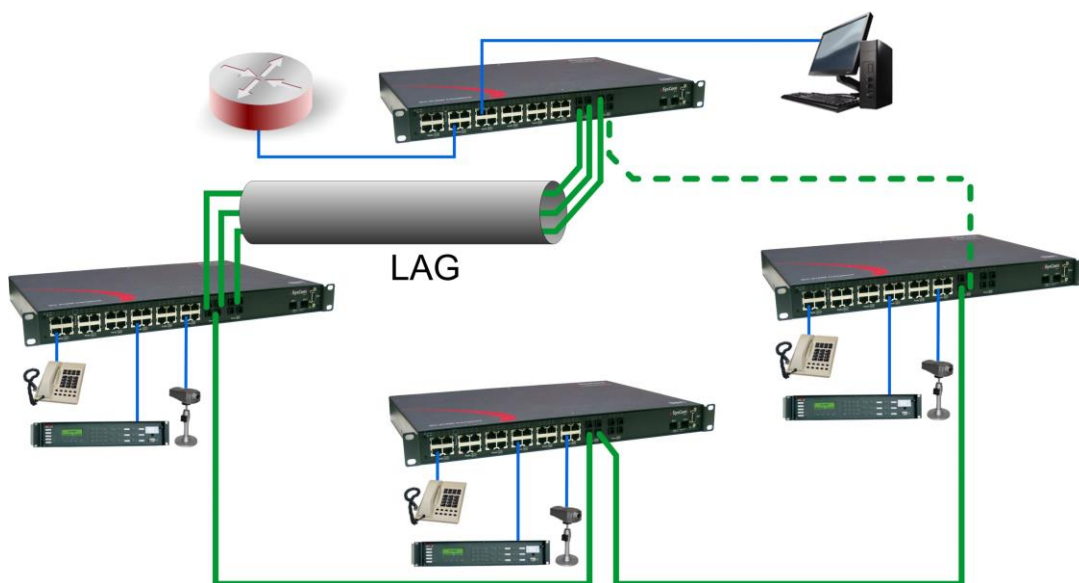


FIGURE 3

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 established, the set of parameters of the interface selected as *Leader* determines the behaviour of the group.

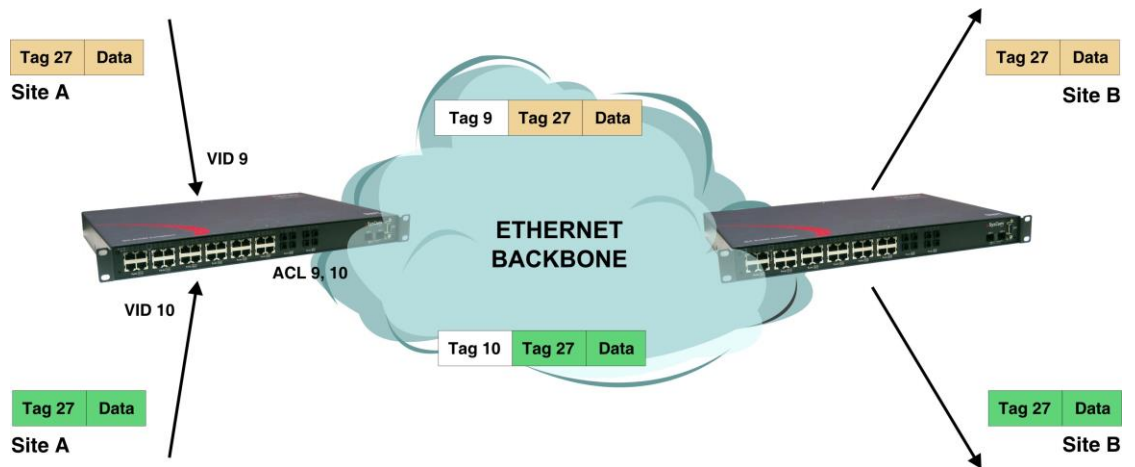
❖ Q-in-Q operation.

The SWT 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 SWT 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 SWT 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 SWT has Quality of Service (QoS), which identifies critical services, guaranteeing that all traffic receives the appropriate priority.

On the other hand, the SWT 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 SWT establishes maximum volume limits for different combinations of broadcast, multicast, and flooding messages, in each one of their ports.

❖ Multicast traffic.

The SWT 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 SWT the selective transmission of the multicast traffic desired by each of them.
- **IGMP.** The SWT manages multicast traffic based on the IGMP messages exchanged by the client equipment and the multicast routers (IGMP Snooping). To be operative, the GARP/GMRP protocol must be INACTIVE.

The SWT also establishes the multicast flows in an explicit and manual way.

❖ Port mirroring.

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

1.3 EQUIPMENT COMPOSITION

The SWT 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 Gigabit Ethernet SFP bays and up to 32 ports, front or rear.

The SWT 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 SWT 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 the first four electrical ports (1 to 4).

1.4 TECHNICAL SPECIFICATIONS

1.4.1 Switch 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 SWT can use the priority fields included in the IEEE 802.1p tag,
 - as well 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.

1.4.2 Unit interfaces

- Up to 32 ports, front or rear.

The chassis has a mechanical structure **of up to four blocks** for the installation of the ports. The type of blocks 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). One block of this type as maximum.
 - 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 **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.
- Block of **2** or **4** ports type **100Base-Fx multimode** (1300 nm) with **SC** 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.

- 1 service console (DCE mode).
- 4 Gigabit Ethernet SFP bays (see section 1.4.3, *Accessories*), front or rear.
- 1 I/O connector with one digital input and output that can be managed via SNMP.
The digital output can be configured as an alarm.

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 built-in web server, HTTP or HTTPS, SSH connection and Telnet.

1.4.5 **Additional services**

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

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: 445 mm ; Depth: 283 mm.
See FIGURE 5.
- 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 the first four electrical ports (1 to 4).

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 between electrical ports P1 to P4: 12 W.
- Temperature range: from -25°C to +70°C
- 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.

1.5 WARNINGS

1.5.1 Warnings before installing



- !
1. The installation of the SWT 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 SWT 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 SWT.
 - The environment in which it is to operate should be suitable for the SWT, 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. 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 SWT must be free of static electricity. An anti-static wristband and/or heel connected to earth should be worn.
- The room housing the SWT 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.

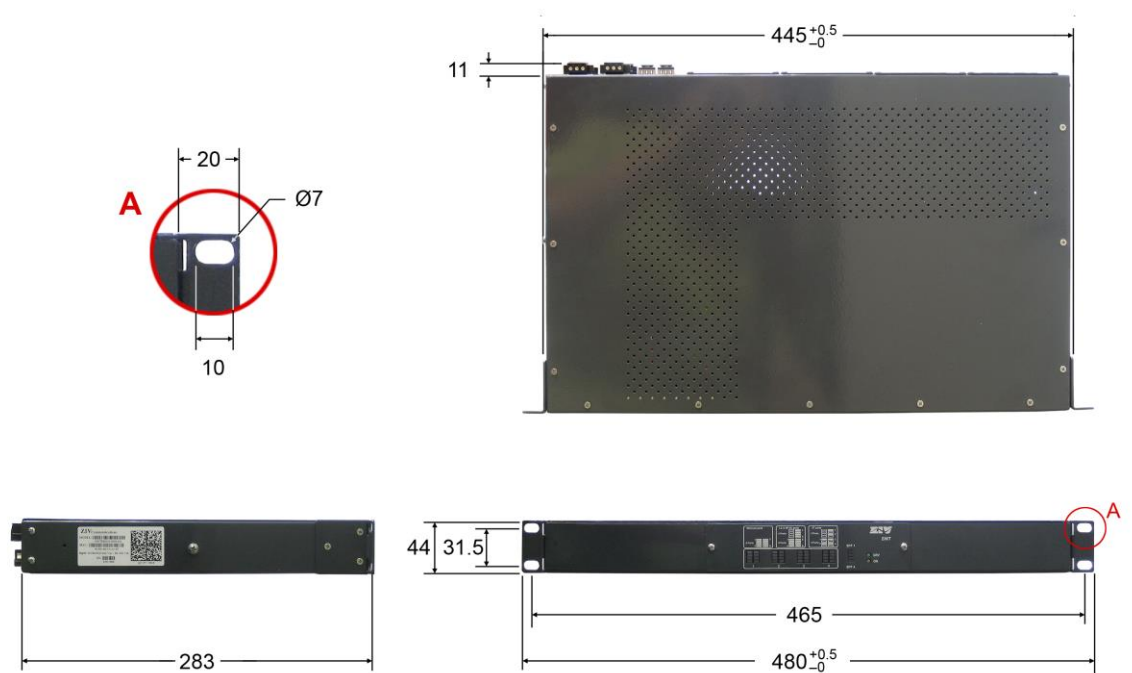
2. ZIV will not accept responsibility for any damage to the equipment caused by the non-fulfilment of point 1.

2 MECHANICAL AND ELECTRICAL CHARACTERISTICS

The diverse elements comprising the Gigabit/Fast Ethernet switch type SWT 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 SWT, as well as the position of the fastening holes.

FIGURE 5 General dimensions in mm of the SWT

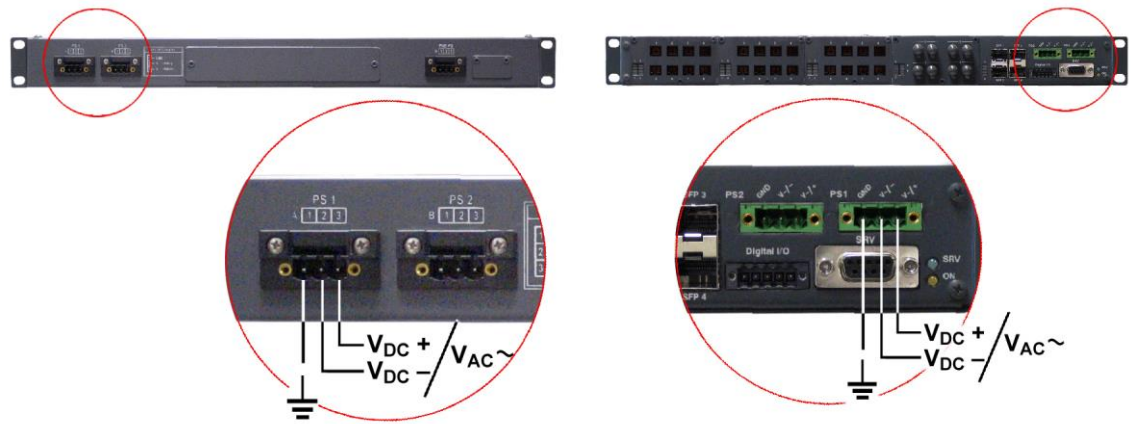


The SWT is powered with a nominal voltage of 48 V_{DC} (isolated) or allows DC and AC supply-voltage operation (80-360 V_{dc}, 80-260 V_{ac}), through the connector shown in FIGURE 6.

The female connector supplied with the equipment is suitable for rigid or flexible conductors of up to 2.5 mm².

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 SWT front port model, the first four 10/100Base-Tx ports, identified as ports 1 to 4, 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 SWT 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



SWT

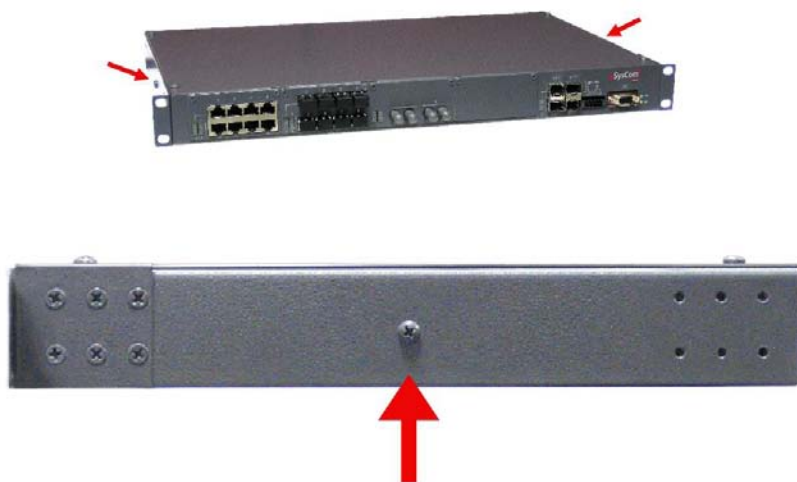


An earth connection is available (see FIGURE 8). When using the multirange model, this connection must be made before connecting any other power-supply cable.

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

FIGURE 8

Location of the earth connection



The SWT may have 4 Gigabit Ethernet SFP bays and up to 32 ports, front or rear.

The SWT 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.

FIGURE 9 shows an example of a front view of the SWT with 4 Gigabit Ethernet SFP bays and with 26 Fast Ethernet **front** ports, the first 16 in 10/100Base-Tx (RJ-45) configuration, the following 8 in 100Base-Fx (multimode, MT-RJ) configuration and the last 2 in 100Base-Fx (multimode, ST) configuration.

FIGURE 10 shows an example of a rear view of the SWT with 4 Gigabit Ethernet SFP bays and with 24 Fast Ethernet **rear** ports, the first 16 in 100Base-Fx (multimode, MT-RJ) configuration and the last 8 in 100Base-Fx (multimode, ST) configuration.

The electrical characteristics of the connectors and their use are indicated in sections 2.1 to 2.8.

SWT

FIGURE 9 Front view of the SWT shelf with 26 Fast Ethernet **front** ports and 4 SFP bays

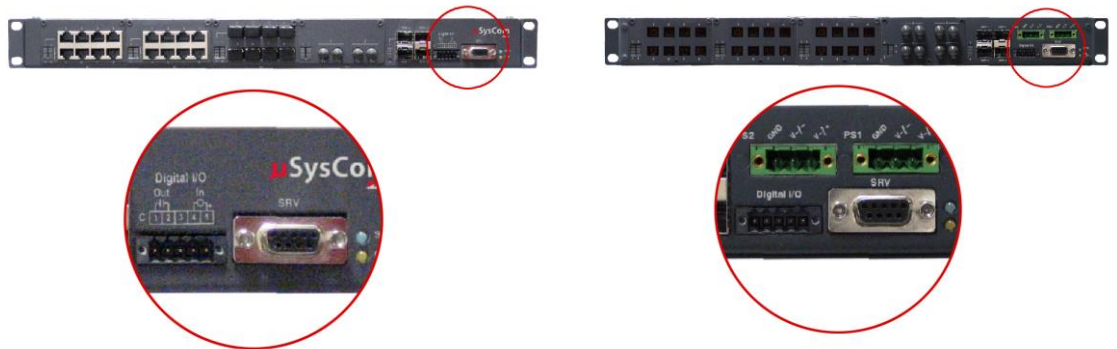


FIGURE 10 Rear view of the SWT shelf with 24 Fast Ethernet **rear** ports and 4 SFP bays



As is shown in FIGURE 11, there is a maintenance connector, identified as SRV, at the right of the SWT, for accessing the equipment through a console, and an I/O connector.

FIGURE 11 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

The electrical characteristics of the I/O connector are indicated in section 2.8.

The electrical characteristics of the maintenance connector and its use are indicated in section 2.7, *SRV port*. The connector has a protective cap.

SWT

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 12 shows the colour of the wires that make up each one of the pairs, according to ANSI/TIA/EIA-568-A standard.

FIGURE 12 Unshielded twisted pair category five cable (UTP-5) with RJ-45 connector according to ANSI/TIA/EIA-568-A standard

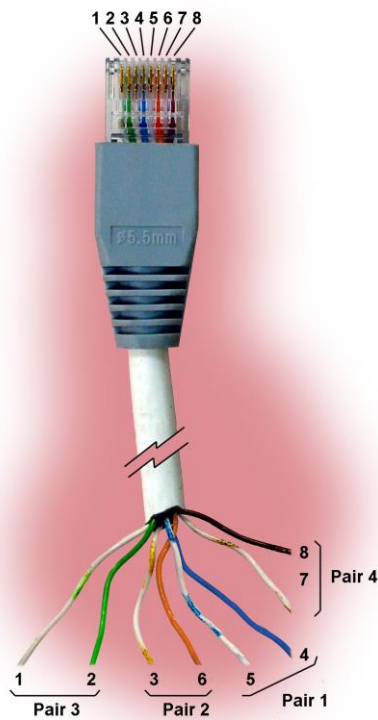
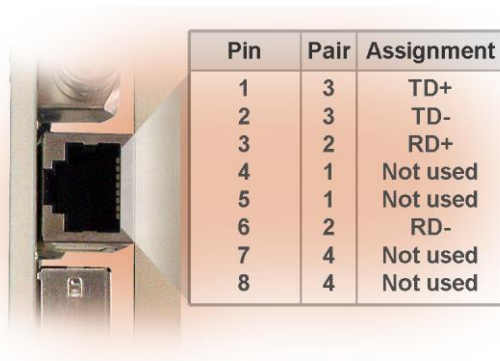


FIGURE 13 shows the use of each one of the pins of the RJ-45 connector, as well as the pair it belongs to according to ANSI/TIA/EIA-568-A standard, in the 10/100Base-Tx LAN interface.

SWT

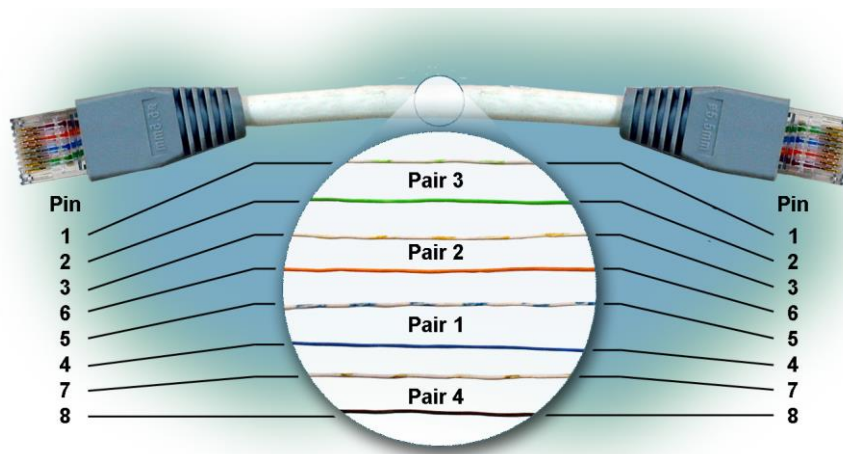
FIGURE 13 Signals of the RJ-45 connector in the 10/100Base-Tx LAN interface



Pair 1 is used for the $V_{DC}PoE+$ connection, and pair 4 is used for the $V_{DC}PoE-$ connection in the ports that admit the PoE power-supply option, electrical ports 1 to 4.

Straight-through cables must be used, see FIGURE 14, where the 4 pairs correspond at both ends of the cable.

FIGURE 14 Straight-through cable



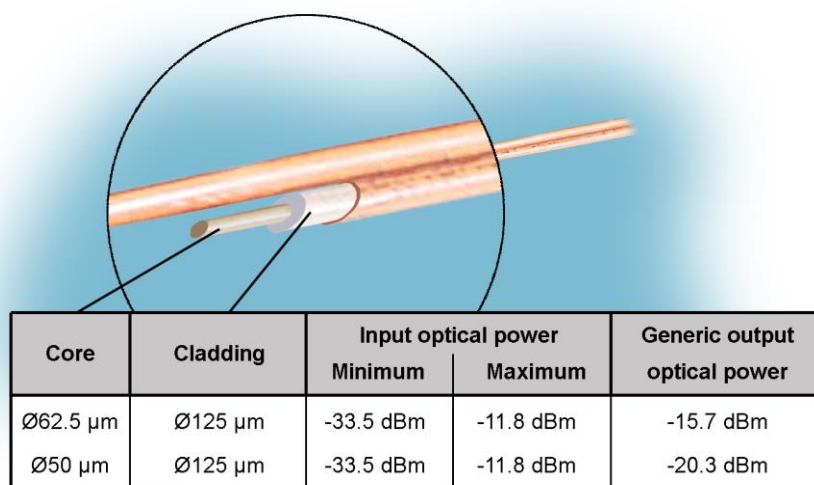
2.2 100BASE-FX (MULTIMODE, MT-RJ) PORTS

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 15. 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 15 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 15 Multimode optical fiber



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 15. 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 15 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 15. 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 15 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

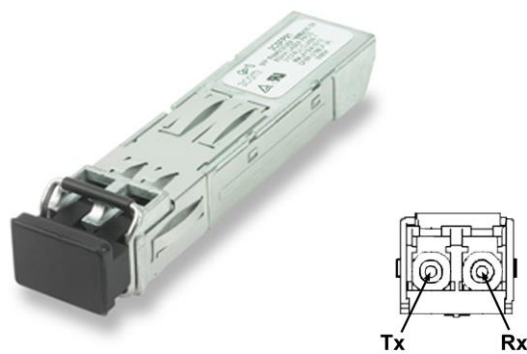
All the LC singlemode type connectors have a protective cap.

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 16 SFP modules



Inserting procedure of an SFP module

The inserting procedure of an SFP module is the following:

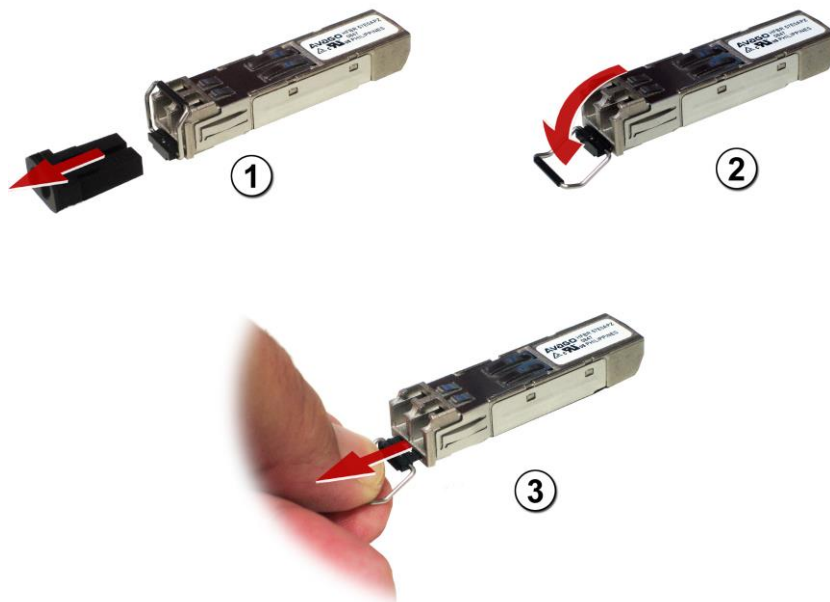
1. Remove the protective packaging of the SFP module.
2. Check that the SFP module is the correct one for your network configuration.
3. Hold the module between your thumb and forefinger.
4. Insert the module into the corresponding SFP slot on the front panel of the equipment.
5. Remove the protective 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 16).

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).

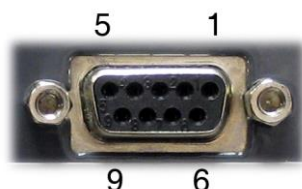
FIGURE 17 Removing an SFP transceiver



2.7 SRV PORT

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

FIGURE 18 Location of the SRV maintenance connector



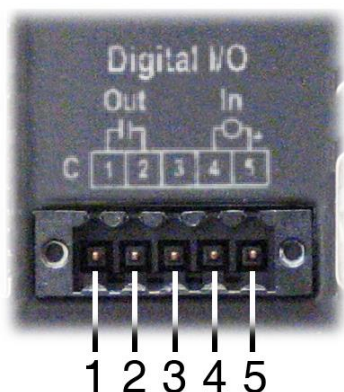
Pin	RS-232
2	RD
3	TD
5	GND

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 19 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 SWT has two basic LEDs (SRV and ON) and several specific LEDs associated with the Fast Ethernet ports and SFP modules.

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

3.1 SWT WITH FRONT PORTS

FIGURE 20 shows a front view of the SWT with front ports, showing the detail of the different LEDs. They are described below.

FIGURE 20 LEDs in the SWT with front 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 PoE (electrical ports 1 to 4)

PoE LED Two-coloured. There is a LED per interface associated with each PoE port (only electrical ports 1 to 4). When there is no connected equipment, the four amber LEDs are lit permanently, as long as there is always 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

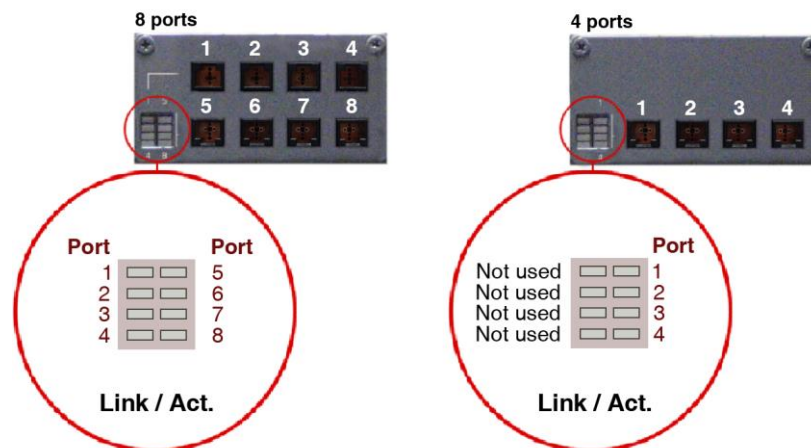
Link/Act. LED Amber. There is one LED per SFP interface. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.

LEDs associated with 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

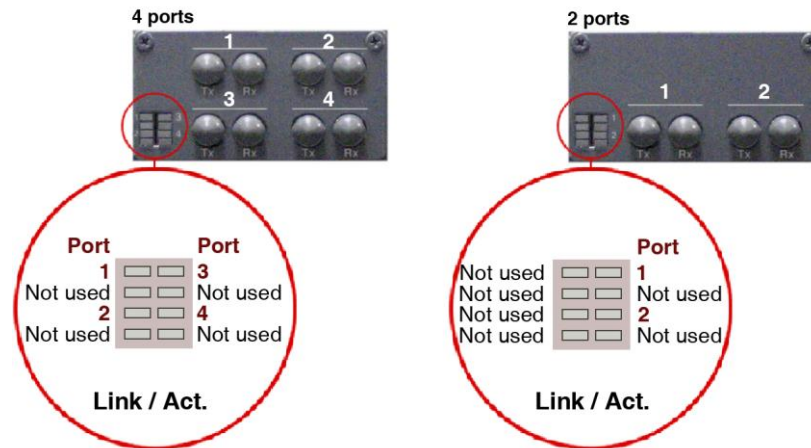
Link/Act. LED Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



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

Link/Act. LED

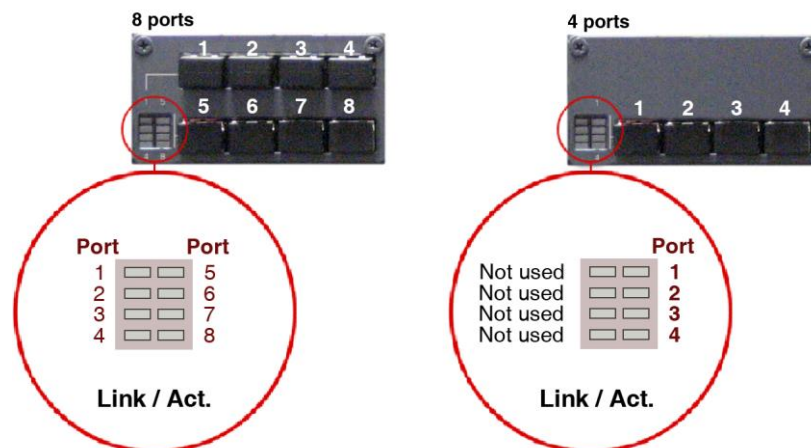
Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



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

Link/Act. LED

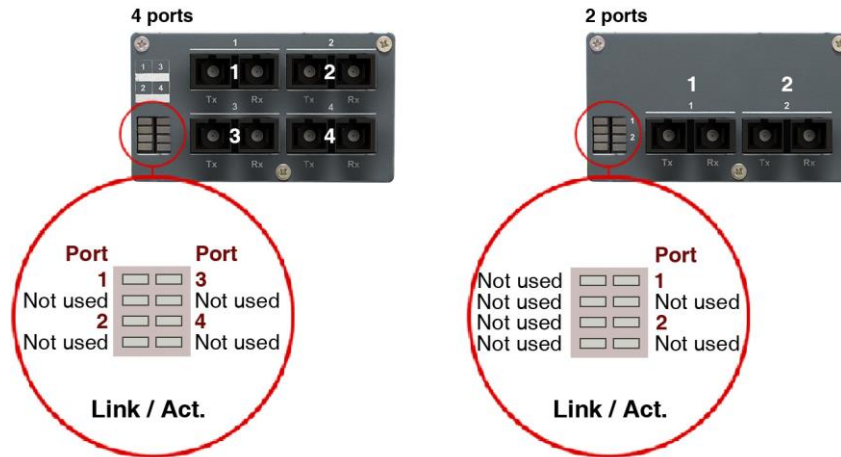
Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



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

Link/Act. LED

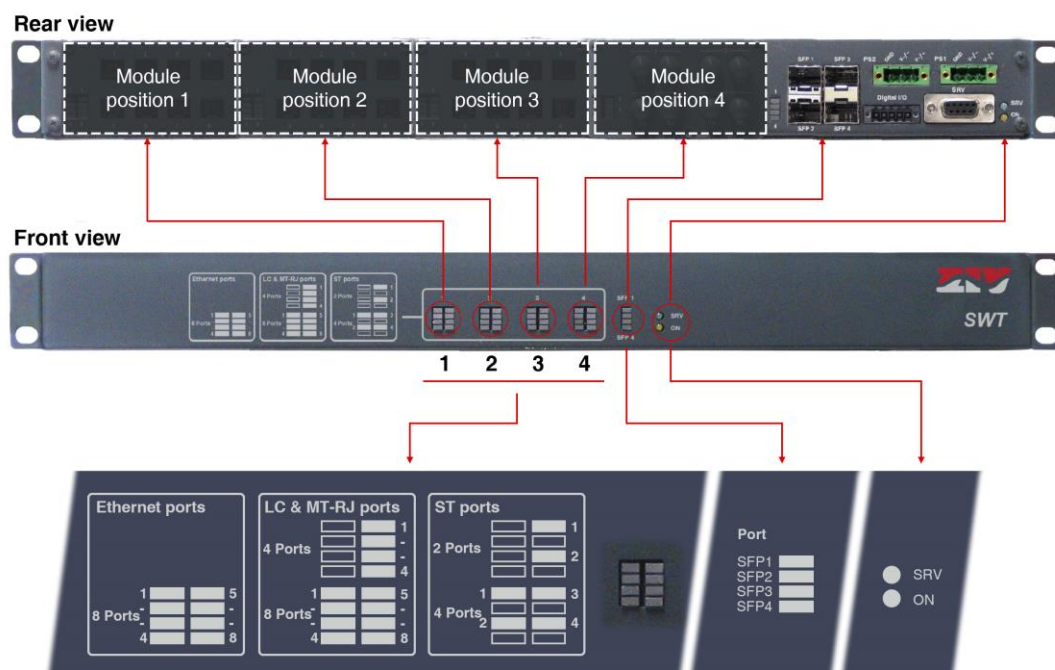
Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



3.2 SWT WITH REAR PORTS

FIGURE 21 shows a front view of the SWT with rear ports, showing the detail of the different LEDs. They are described below.

FIGURE 21 LEDs in the SWT with rear 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 Amber. There is one LED per SFP interface. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.

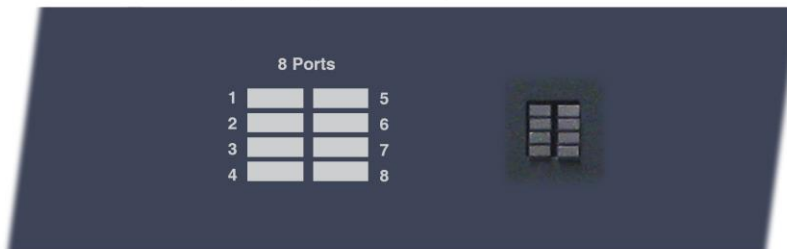
LEDs associated with 10/100Base-Tx (RJ-45) ports

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.



10/100Base-Tx (RJ-45) electrical ports



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.



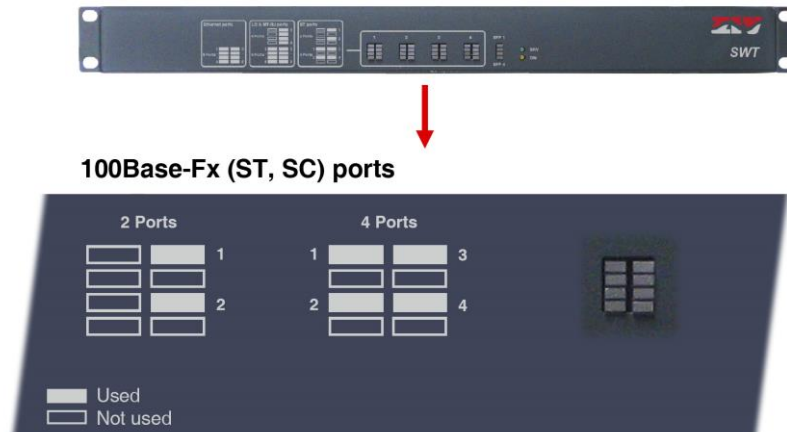
100Base-Fx (MT-RJ) ports



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

ST or SC ports LEDs

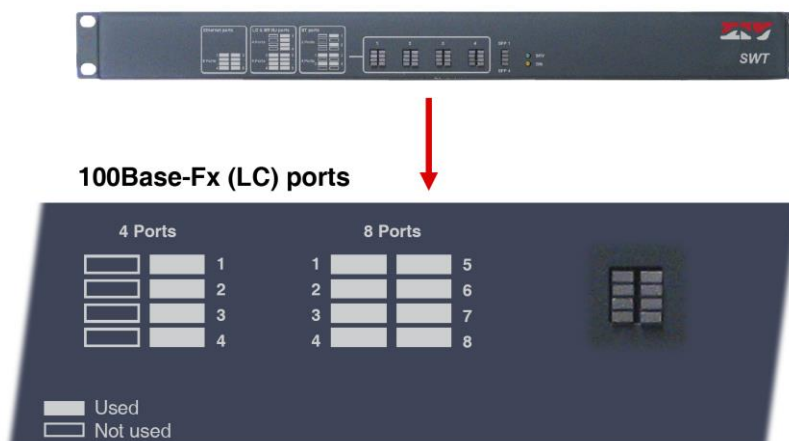
Green. There is one LED per port. It stays on when the link is established correctly and flashes in the case of emission or reception activity in the interface.



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

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 SWT 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 establish 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.

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. The commands indicated are shown on FIGURE 22.

For information about the **Reboot**, **Reflash Configuration files** and **Event files** commands see sections 5.17, 5.18, 5.19 and 5.20, respectively.

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

FIGURE 22 HTML page tree menu



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.

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 SWT 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 shown in the auxiliary graph.

Whenever changes are made, regardless of whether 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 executing **Apply** or **Save**, the **Send** button must be pushed to allow the equipment to obtain the new desired values.

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

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 23, which is shown when the SWT 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 23 Main HTML page

The screenshot displays a web interface with four main sections, each with a tree menu icon on the left:

- Identification**: Hostname (swt), Location (unknown), Contact (unknown), Product (3SWTEEEE00F2000A), Firmware version (3.31.1.23645), Firmware reference (4WF72030000-R000), Tracking # (000016056dbb), Serial # (1000000).
- Access Control**: Guest's login (guest), Guest's password (Change), Admin's login (admin), Admin's password (Change).
- Others**: Time zone (Madrid).
- Syslog**: Local Syslog Level (4), Remote Syslog Level (4), Syslog Log (checkbox), Syslog Server IP (0.0.0.0).

Buttons for 'Send' and 'Reload' are located at the bottom of the Syslog section.

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-established 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 a parameter that establishes the hour zone in relation to UTC.

5.1.4 Syslog

This section deals with four parameters. The first of them, **Local Syslog Level**, establishes the maximum level of severity which is stored in the local Log. The range admitted is between 1 and 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 its 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. 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**, establishes the maximum severity level to be sent to the Remote Syslog server. The range admitted is between 1 and 8. The default value is 4. See information about the levels in the previous parameter.

The third parameter, **Syslog Log**, is a *Checkbox* control. By default, it is NOT selected, which means that a remote server is configured and the traces are **NOT** stored in the local Log. When the control is selected, the traces are sent to the remote server and are **also** stored in the local Log with the corresponding severity level.

The last parameter, **Syslog Server IP**, establishes 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.

and the respective port.

The equipment also allows to enable FTP and FTPS separately.

The following files can be found in the root directory of the FTP server:


- 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.

The *FTP Idle Timeout (s)* parameter is the idle timeout in a FTP/FTPS established connection. Valid values are 0 to 3600 seconds. A value 0 for idle timeout means that the feature is disabled.

Telnet and SSH servers can be disabled, although by default they are enabled. In addition, in the case of the SSH server, both the service port and the idle timeout can be configured. For this last parameter, valid values are 0 to 300 seconds. A value 0 for idle timeout means that the feature is disabled.

FIGURE 24 **Administration** menu configuration page


 **CLI access**

Enable telnet

Enable SSH

SSH port

SSH Idle timeout (s)

 **Web Access**


HTTP

HTTP port

HTTPS¹

HTTPS port

1 Certificates must be loaded in CLI

 **Ftp Server**

FTP

FTPS²

FTP Idle Timeout (s)

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 the IP parameters for the switch administration and management.

The configuration parameters are the following:

- **Static IP.** When this control is selected, the equipment uses the data provided by the user in relation to the IP address and its mask. The main IP address and its mask are obtained automatically through the DHCP client if this control is not selected.
- **IP address.** It establishes the switch IP address.
- **IP mask.** It establishes the mask associated with the switch IP address.
- **VLAN id.** VLAN numeric identifier. When configuring multiple VLANs, this parameter specifies where the equipment will be accessed for management. It is configured with the value 1 by default, that is, it will be accessed from the interfaces assigned to the **vlan1** for management.
- **Default gateway.** This establishes the default router IP address (Default Gateway).
- **MAC address.** It shows the switch own Ethernet MAC address.

FIGURE 25 LAN menu configuration page

The screenshot shows the LAN configuration interface. At the top, there is a header with a network icon and the text 'LAN'. Below this, there are several configuration items:

- Static IP:** A checkbox that is checked with a green checkmark.
- IP address:** A text input field containing '172.16.30.93'.
- IP mask:** A text input field containing '255.255.255.0'.
- VLAN id:** A text input field containing '1'.
- Default gateway:** A text input field containing '172.16.30.254'.
- MAC address:** A text input field containing '00:E0:AB:02:18:7F'.

At the bottom of the configuration area, there are two buttons: 'Send' and 'Reload'.

5.4 ETHERNET PORTS CONFIGURATION

The **Ports** menu permits the configuration of the operating parameters of the Gigabit/Fast Ethernet ports in the equipment, and the assigning of each port to one of the VLANs defined in the equipment (see section 5.5).

By default, Web management is accessible from the interfaces assigned to **vlan1**. As a factory setting, all Gigabit/Fast Ethernet ports have a default VLAN id (VID) of value 1.

If the default VID of a given port is changed, the Web management will no longer be accessible from that port.

FIGURE 26 **Ports** menu configuration page

#	Enable	VLAN function	Mode	VID	VID ACL	Description	LAG	LAG leader
1	<input checked="" type="checkbox"/>	untag	auto	1	auto	swt-port	none	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	trunk	auto	1	auto	swt-port	none	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	edge	auto	10	auto	swt-port	none	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	edge	auto	1	10	swt-port	none	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
6	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
7	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
8	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
9	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
10	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
11	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
12	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
13	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
14	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
15	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
16	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
17	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>
18	<input checked="" type="checkbox"/>	edge	auto	1	auto	swt-port	none	<input type="checkbox"/>

Q in Q (Double tagging)
 S-TAG type

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.
- **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, tag, 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 equipment, so as to 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 if 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 private 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 speed and operation mode.

Auto (autonegotiation): Recommended and value by default.

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 speed**, that is to say, **they can operate at the speed 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 5.5, *VLAN configuration*.

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 acts 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 **all** 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. Establishes 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 equipment.

- **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 value by default is 0X88A8 according to the standards.

5.5 VLAN CONFIGURATION

A Virtual Local Area Network (VLAN) can be defined as a series of devices connected in a network which belong to one Local Area Network, even though they are connected in different interconnection equipment, remote geographical zones, different floors of a building or even different buildings. In other words a VLAN is a network with logical groups which are physically independent.

Each VLAN is distinguished from the rest by a specific identifier, usually called a VLAN tag, which is specified in standard IEEE 802.1q. The tag allows several VLANs to share resources, including switching equipment such as the SWT, or links between switching equipment, 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.

FIGURE 27 **VLANs** menu configuration page

VLAN OVERLAPPING
 Overlapping Enable

VLANs

#	Name	VID	PRI Override ¹	PRI	
1	<input type="text" value="vlan_name"/>	<input type="text" value="1"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="button" value="Delete"/>
2	<input type="text" value="vlan_name"/>	<input type="text" value="10"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="button" value="Delete"/>
3	<input type="text" value="vlan_name"/>	<input type="text" value="20"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="button" value="Delete"/>
4	<input type="text" value="vlan_name"/>	<input type="text" value="30"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="button" value="Delete"/>
5	<input type="button" value="Add"/>				

1 Will have no effect on Trunk ports

VLANs for Q-in-Q

#	VID	Name	
1	<input type="text" value="1"/>	<input type="text" value="vlan_name"/>	<input type="button" value="Undo"/>
2	<input type="button" value="Add"/>		

The screen associated to the **VLANs** menu has three distinct sections, which are described below.

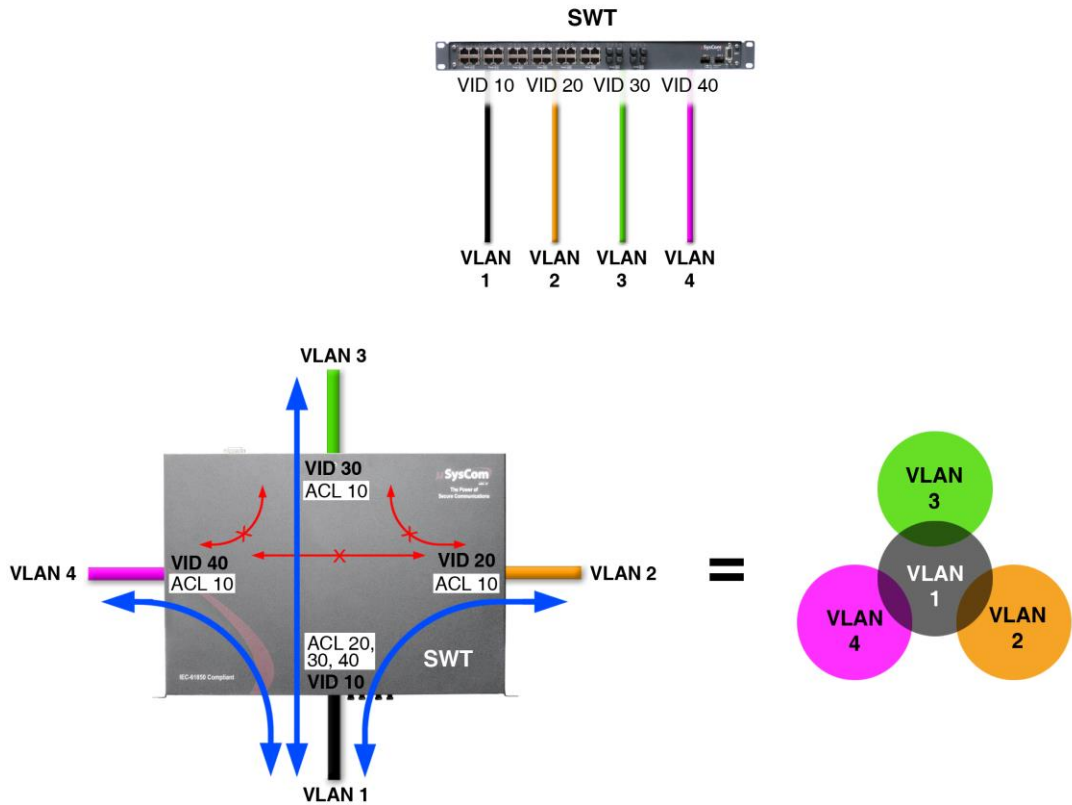
There is a global parameter that affects all the VLANs.

- Overlapping Enable.** It establishes 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 5.4).

FIGURE 28 shows an example for using the **Overlapping Enable** parameter.

FIGURE 28 Example for using the **Overlapping Enable** parameter



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

VLANs:

The individual configuration parameters for each VLAN are:

- **#.** Indicates the position in the table.
- **Name.** A mnemonic descriptive field available to users.
- **VID.** It establishes the VLAN identifier. The admitted range goes from **1** to **4095**.
- **PRI Override.** This establishes whether the priority of the frames received in the ports assigned to the VLAN VID should be overridden in the PRI field value (enabled option), or whether it should be maintained (Disabled option). This field does **NOT** affect the ports in which the VLAN function parameter is configured as trunk.
- **PRI.** If the **PRI Override** option is enabled, the original priority of the frames received **with a tag** will be modified with the established value.

VLANS for Q-in-Q:

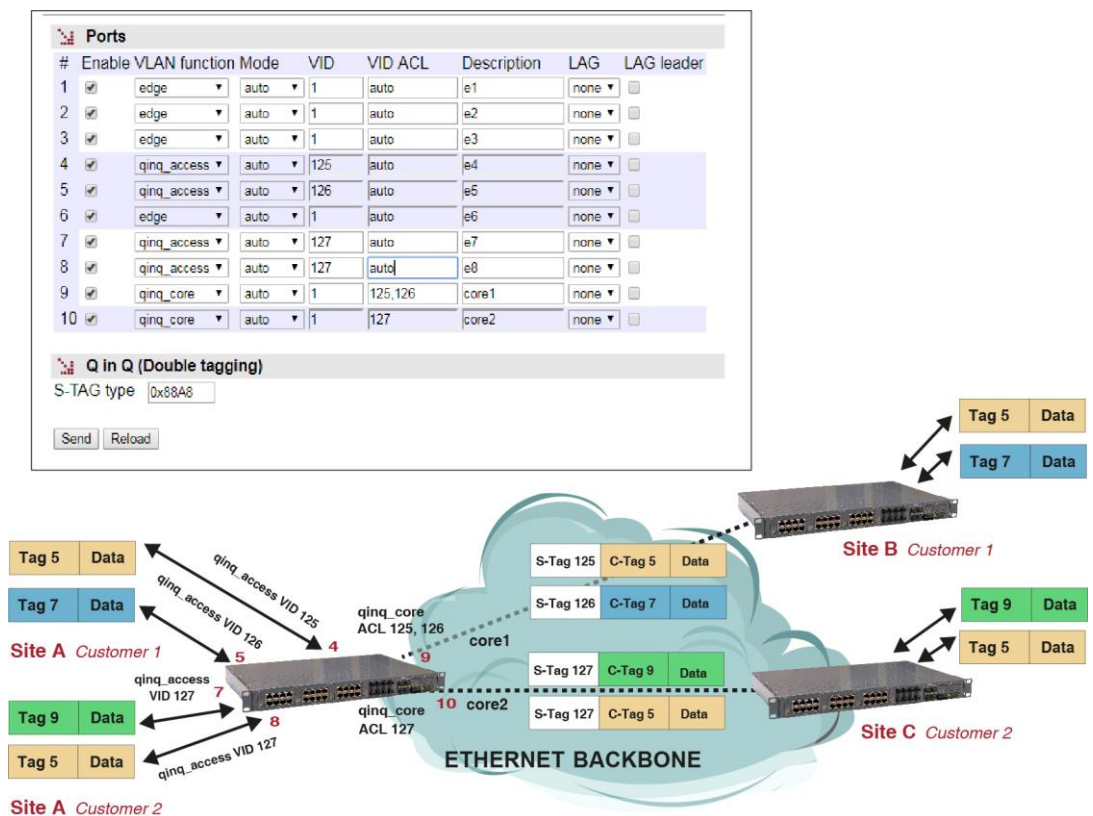
In this section must be indicated which of the VLANs will be the ones used in interfaces QinQ Access, that is, which of the VLANs accepted by the equipment will be sent on another network through the use of the double tagging. FIGURE 29 shows an example.

- **#.** 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 29 Example for using the **VLAN for Q-in-Q** parameter



BANDWIDTH LIMIT CONFIGURATION

The **Rate Control** menu permits bandwidth limits to be established in each one of the ports, both incoming and outgoing. The data volume limit may be established in general for all types of traffic, as well as for certain combinations that take into account the type of messages.

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**).

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.
- **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 when there is a flood in a short time, usually due to an incorrect topology, an inappropriate configuration, or a voluntary action by some client equipment.

- **Rate (bps)**. It establishes the maximum incoming bandwidth to the port: **64000** bps (64 kbps) to **250000000** bps (250 Mbps). The maximum speed 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.
- **Enable**. This permits each port to be enabled or disabled individually, by ticking or not ticking the respective *Enable* box.

- **Rate (bps).** It establishes the maximum outgoing bandwidth from the port: **64000** bps (64 kbps) to **250000000** bps (250 Mbps). The maximum speed only affects the Gigabit Ethernet ports.

FIGURE 30 **Rate Control** menu configuration page

Ingress Rate Control

Ports	#	Enable Traffic ¹	Rate (bps)
	1	<input type="checkbox"/>	all 64000
	2	<input type="checkbox"/>	all 64000
	3	<input type="checkbox"/>	all 64000
	4	<input type="checkbox"/>	all 64000
	5	<input type="checkbox"/>	all 64000
	6	<input type="checkbox"/>	all 64000
	32	<input type="checkbox"/>	all 64000
	33	<input type="checkbox"/>	all 64000
	34	<input type="checkbox"/>	all 64000

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

Egress Rate Control

Ports	#	Enable Rate (bps)
	1	<input type="checkbox"/> 64000
	2	<input type="checkbox"/> 64000
	3	<input type="checkbox"/> 64000
	4	<input type="checkbox"/> 64000
	5	<input type="checkbox"/> 64000
	6	<input type="checkbox"/> 64000
	32	<input type="checkbox"/> 64000
	33	<input type="checkbox"/> 64000
	34	<input type="checkbox"/> 64000

5.7 QoS CONFIGURATION

The Quality of Service (QoS) permits the traffic classification and service policy and establishes 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 establishing 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 priority 802.1q or the DSCP field in the IP header (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 Port Table**. 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 **VLANS** submenu, in such a way that the priority may be overridden. If, on the contrary, they only include the priority, they are processed in accordance with the section entitled **QoS Port Table**.

The sections and their configuration parameters are as follows:

Weight Fair Scheduling:

- **Weighted Fair.** This establishes 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**.

Priority:

This section establishes the classification conditions of the frames in each one of the three existing queues according to the 802.1q priority value, regardless of the assignation mechanism, or its process.

- **#.** This identifies the value of the priority associated with frame 802.1 (it covers the whole range of values permitted by the standard).
- **Queue.** This establishes the queue priority in which the traffic coinciding with the priority value indicated by the # field will be inserted. The values permitted 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:

This section establishes the classification conditions of the frames in each one of the three existing queues according to the DSCP field value of the main IP. A discreet value range is admitted for the DSCP field.

- **#.** This identifies the value of the DSCP field being processed.
- **Queue.** This establishes the queue priority in which the traffic coinciding with the DSCP value indicated by the # field will be inserted. The values permitted identify the three internal priorities: **High**, **Medium** or **Low**.

QoS Port Table:

This section establishes the conditions to obtain or assign the priority to each one of the ports.

- **#.** The physical interface identifier.
- **Priority.** Value of the priority assigned to frame 802.1p 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 established in the section entitled **Priority**.
- **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 established in the section entitled **Priority**.
- **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 established in the section entitled **DSCP**.

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 established by the user will be associated with an untagged frame.
- The priority present in the frame will be maintained in a tagged frame, provided the DSCP field is not present (traffic or IP) or does not coincide with any of the specified values.

FIGURE 31

QoS menu configuration page

Weight Fair Scheduling

Weighted Fair

Priority

Queue

0 medium ▾

1 medium ▾

2 medium ▾

3 medium ▾

4 medium ▾

5 medium ▾

6 medium ▾

7 medium ▾

DSCP

Queue

0 medium ▾

8 medium ▾

16 medium ▾

24 medium ▾

32 medium ▾

40 medium ▾

48 medium ▾

56 medium ▾

QoS Port Table

#	Priority	Use IEEE 802.1p	Use DSCP
1	0 ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	0 ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	0 ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	0 ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	0 ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>
31	0 ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>
32	0 ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>
33	0 ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>
34	0 ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>

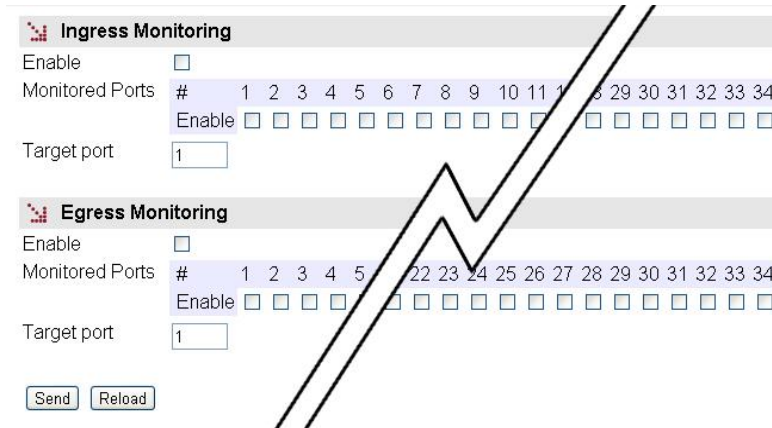
5.8

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 32 **Monitor** menu configuration page



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.

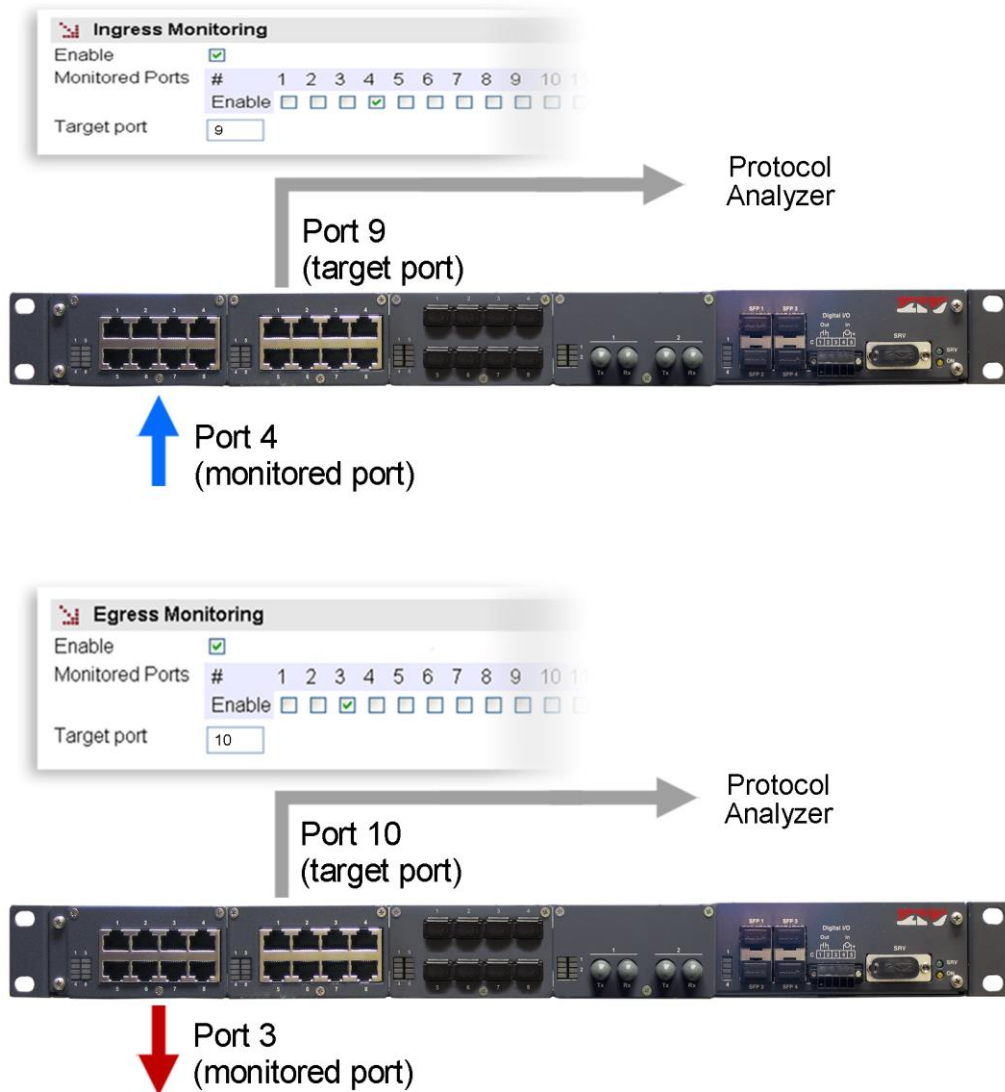
Ingress Monitoring:

- **Enable.** It permits enabling and disabling monitoring of the incoming traffic by ticking or not ticking the corresponding box.
- **Monitored Ports.** It establishes 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 establishes 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 establishes 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 establishes the port where the replicated packets will be sent to be monitored.

FIGURE 33 Example of **Monitor** menu configuration



5.9 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 5.4).
- **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 34 Example of configuration of **LLDP** menu

The screenshot shows the LLDP configuration interface. At the top, there is a section for 'LLDP' with an 'Enable' checkbox checked. Below this is a 'Ports' section containing a table with 10 rows, each representing a port configuration. The table columns are: #, Admin Status, Tx Interval, Hold, Reinit, Credit Max, Tx Interval Fast, Mess num, Fast Tx, Notif. Enable, PortDesc, SysName, SysDesc, SysCap, Tx Mgmt, and Mgmt Addr. Each row has a dropdown menu for 'TxRx' and various input fields and checkboxes. At the bottom of the table, there are 'Send' and 'Reload' buttons.

#	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		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0
2	TxRx	30	4	2	5	1	4		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0
3	TxRx	30	4	2	5	1	4		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0
4	TxRx	30	4	2	5	1	4		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0
5	TxRx	30	4	2	5	1	4		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0
6	TxRx	30	4	2	5	1	4		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0
7	TxRx	30	4	2	5	1	4		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0
8	TxRx	30	4	2	5	1	4		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0
9	TxRx	30	4	2	5	1	4		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0
10	TxRx	30	4	2	5	1	4		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0

5.10 SNMP CONFIGURATION

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

The agent admits the emitting of messages based on the SNMPv1 [1], SNMPv2c [2] 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.

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 operating 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 establish the authentication password (*Auth Password*). The password establishes 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 establish 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.

FIGURE 35 **SNMP** menu configuration page

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 equipment 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 established 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 establishes 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 equipment 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 value by default.
The *Type* control is used to establish 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.

5.11 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 equipment can communicate with each other and establish 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 equipment end up forming a tree structure with no loops from the root equipment.

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

FIGURE 36 STP menu configuration page

Bridge

Enable
 Version rstp ▼
 Bridge Priority 32768
 Max Age¹ 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	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
6	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
7	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
8	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
9	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
10	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
11	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
12	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
13	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
14	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
15	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
16	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
17	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>
18	<input checked="" type="checkbox"/>	128	200000	auto ▼	auto ▼	<input type="checkbox"/>

Send
Reload

The specific equipment configuration parameters are:

- **Enable.** A simple checkbox parameter to indicate whether the STP must be executed or not.
- **Version.** This establishes which of the possible protocol versions will be executed. STP or RSTP (Rapid STP).

- **Bridge Priority.** This sets the priority of the equipment communicating with the root equipment.
- **Max Age.** The maximum time during which the equipment considers the last BPDU message received as valid. In the case of the stipulated time expiring, the equipment assumes there has been a topological change and initiates the topological change communication process. The default value is 20 seconds, and the range admitted is between 6 and 40 seconds.
- **Hello Time.** This parameter establishes 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 the range admitted is between 4 and 30 seconds.
- **Tx Hold Count.** This establishes the maximum number of BPDU packets that can be transmitted in one second. The default value is 6 and the admitted range is between 1 and 10.

The configuration parameters for each port are:

- **Enable.** Establishes 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 establishes 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 establishes 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 37.

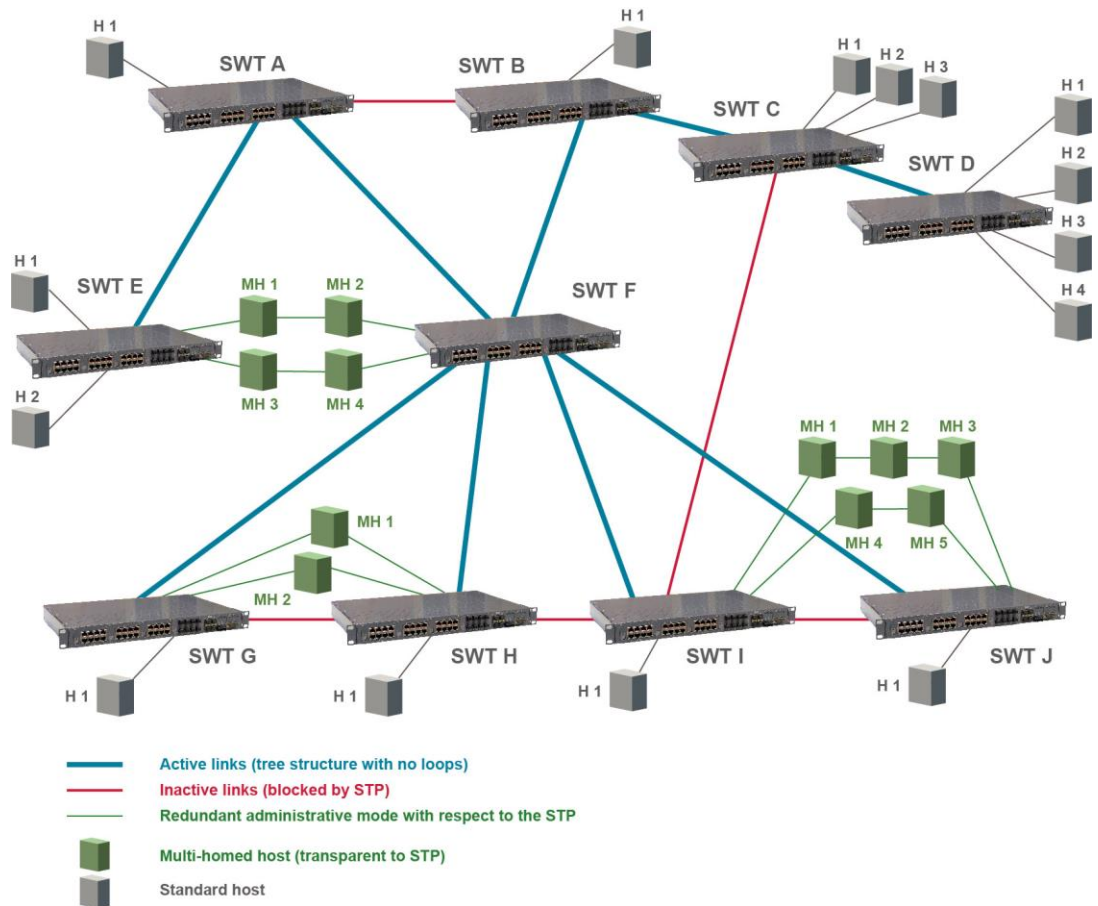
Even when the **Edge** parameter is **on**, the switch maintains activated the detection of other switch connection to the interface, so operating state can become **off**.

The operation mode of the interface, **on** or **off**, is shown in the STP statistics section.

- **PtP.** The PtP parameter establishes 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 37 Example of the **redundant** mode of the interface with respect to the STP



5.12 NTP/SNTP CONFIGURATION

The equipment has an NTP/SNTP client, meaning that it can synchronise time-related information by accessing NTP servers. The NTP [3] 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 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 (*multicast*).
- **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.

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.

FIGURE 38 **NTP/SNTP** menu configuration page

NTP

Enable

Protocol sntp ▾

Authentication Keys

#	Key Number	Key	
1	<input type="text" value="1"/>	<input type="text" value="xxxxxxxx"/>	<input type="button" value="Delete"/>
2	<input type="button" value="Add"/>		

NTP client

Server

#	IP	Type	minpoll	maxpoll	Authentication Enable	Authentication Key	
1	<input type="text" value="81.19.96.148"/>	unicast ▾	<input type="text" value="5"/>	<input type="text" value="10"/>	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="button" value="Delete"/>
2	<input type="text" value="176.126.242.239"/>	unicast ▾	<input type="text" value="5"/>	<input type="text" value="10"/>	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="button" value="Delete"/>
3	<input type="button" value="Add"/>						

Accept Broadcast

SNTP client

Server

#	IP	poll	units	Authentication Enable	Authentication Key	Timeout
1	<input type="text" value="81.19.96.148"/>	<input type="text" value="60"/>	minuts ▾	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="15"/>

5.13 MULTICAST CONFIGURATION

Under normal conditions, multicast traffic propagates automatically on all interfaces belonging to each VLAN, with client equipment 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 equipment in the network switches.

GARP is a base protocol on which GMRP operates. GARP requires the configuration of timers by accessing the screen shown in Figure 39.

FIGURE 39 **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

Send Reload

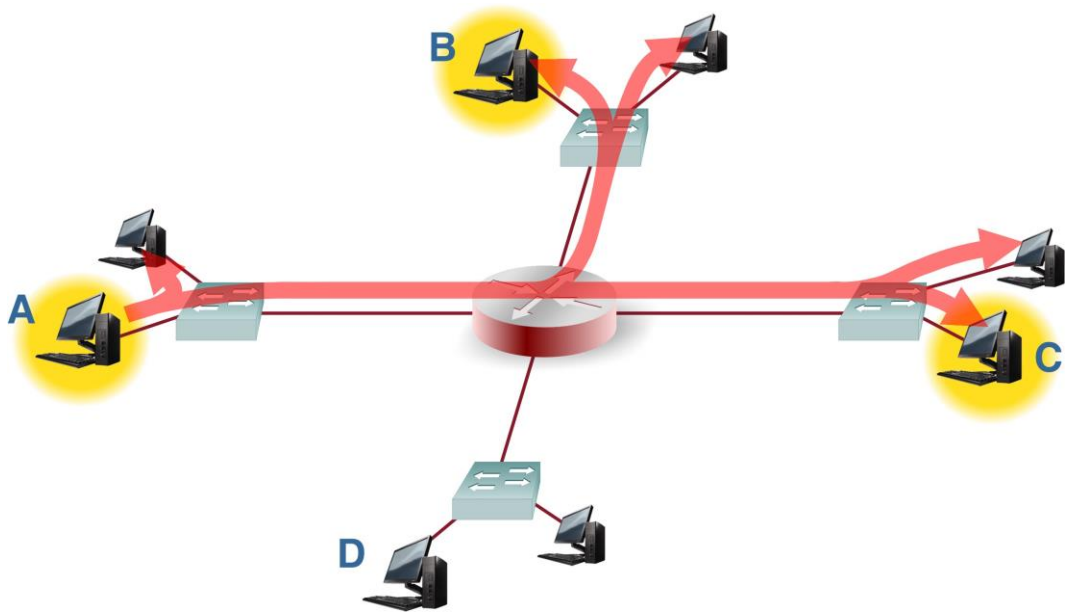
The IGMP is layer 3 protocol, and message exchange of reception requests for multicast flows takes place between the client equipment and the IGMP routers. In this case, the messages are spied by the switch to adapt the configuration of each port (IGMP Snooping). For the IGMP Snooping to be operative, 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 equipment. Any other multicast traffic will be discarded.

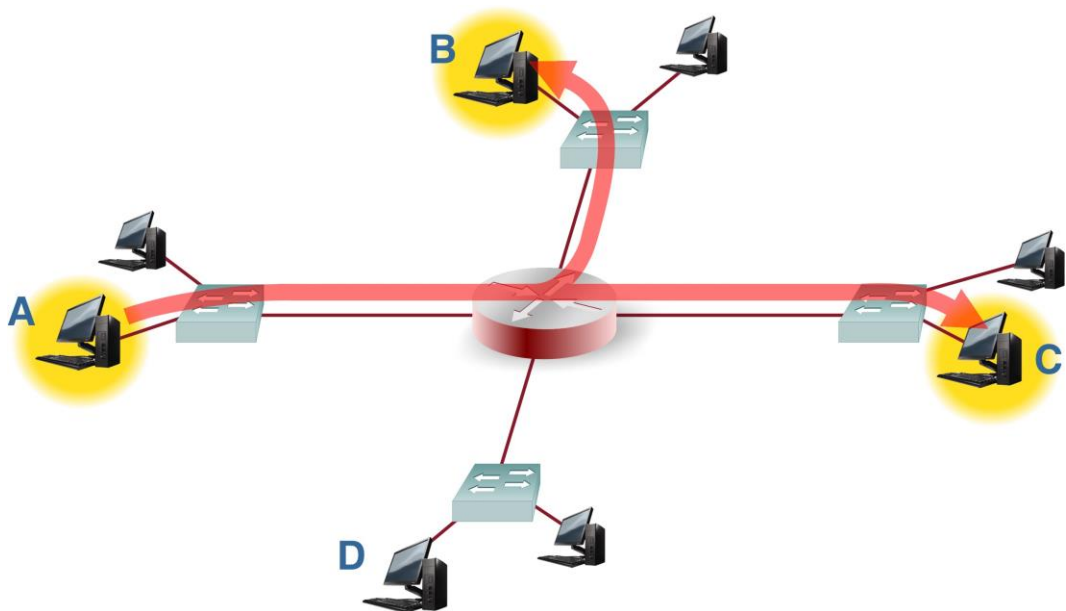
As an example, FIGURE 40 shows the advantages of using GARP/GMRP or IGMP Snooping. Figure 40a) shows a network made up by four level-2 switches, which in turn are connected to a router. Host A is a multicast message emitter, and the Hosts B and C are multicast receivers belonging to the same group as 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 40b) 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 40 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

5.13.1 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.

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**.

FIGURE 41 *Static* configuration page of *Multicast* menu

#	Address	Ports	VLANs	
1	01:00:5E:00:00:01	any	1	Delete
2	01:00:5E:00:00:02	any	2	Delete
3	Add			

Send Reload

5.13.2 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 equipment 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.

The parameters are the following:

GMRP:

A single parameter to indicate 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 establishes 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 equipment for the group address, and that only the multicast traffic registered in the interface will be treated.

FIGURE 42 **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 ▼

Send Reload

5.13.3 IGMP

The IGMP Snooping is an optimization to be used in level 2 equipment, such as the SWT. 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 SWT 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 indicate 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 equipment and routers in order to identify the ports where there is equipment actively participating in multicast groups; the objective is to limit selective data transmission based on the obtained information.

- **Enable.** A simple *CheckBox* to indicate if the IGMP periodic consultation service is active or not.
- **#.** It establishes the equipment physical port number.
- **IGMP forward.** It establishes 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 is client equipment registered in the corresponding group.

FIGURE 43 **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 ▼

1 Value ignored in case GMRP is enabled

Send
Reload

5.14 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.

FIGURE 44 **Access** menu configuration page

TACACS+

1 Server IP

2 Server IP

Encrypted

Secret shared Key [Change](#)

Guest Privilege Level

Admin Privilege Level

RADIUS

1 Server IP

2 Server IP

UDP port

Shared secret [Change](#)

Timeout

Guest Privilege Level

Admin Privilege Level

Console Access

Authentication method¹

¹ Fallback to local access always enabled

Web Access

Authentication method

Fallback to local access

Telnet Access

Authentication method

Fallback to local access

SSH Access

Authentication method

Fallback to local access

FTP Access

Authentication method

Fallback to local access

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.

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.

5.15 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.

The general configuration parameters for the ports are the following:

- **#.** Physical interface identifier.
- **Security Type.** It establishes 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 establishes the behaviour of the equipment in the event of reaching the maximum number of MAC addresses permitted, as established in the preceding parameter. The available options are **replace** or **restrict**.

FIGURE 45 Main **Security** menu configuration screen

#	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
31	none	10	replace
32	none	10	replace
33	none	10	replace
34	none	10	replace

1 'dot1x' stands for 802.1x

Send Reload

5.15.1 802.1x

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

The general configuration parameters are the following:

- **Enable.** A simple *CheckBox* parameter to indicate 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 have to be requested.
- **Reauthentication period (reAuthPeriod).** It establishes 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 establishes the maximum number of tries the equipment will send to request reauthentication. The value should be between 1 and 10.
- **Quiet time after failure (quietPeriod).** It indicates the period of time in which the equipment will not request new tries once the maximum number of configured tries is exceeded. The value range is from 1 to 65535; its units are seconds.
- **IP address.** It establishes the RADIUS server IP address.
- **UDP port.** It establishes the UDP port to which the RADIUS client will send requests to the server. The default value established in the standard is port 1812.
- **Shared secret.** It establishes the password to be used to encode the communication with the RADIUS server.

FIGURE 46 802.1x submenu configuration page

802.1x

Enable

Periodic reauthentication (reAuthEnable)

Reauthentication period (reAuthPeriod)

Reauthentication attempts (reAuthMax)

Quiet time after failure (quietPeriod)

RADIUS server

IP address

UDP port

Shared secret [Change](#)

5.15.2 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.

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 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 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.

FIGURE 47 **MAC list** submenu configuration page

#	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			

Send Reload

5.16 OTHERS CONFIGURATION

The **Others** menu enables/disables the use of the PoE power supply, allows to configure the time that the switch stores the MAC addresses of inactivity, as well as configure the digital output as an alarm.

FIGURE 48 **Others** menu configuration page

The screenshot shows a configuration page with three sections:

- MACS**: Bridge Age Time
- Digital Output**: Enable as Alarm
- POE**: POE enable

At the bottom of the configuration area are two buttons: **Send** and **Reload**.

The sections and their configuration parameters are as follows:

MACS:

- **Bridge Age Time.** It establishes the maximum time a learned MAC address of inactivity will remain in the switch MAC address table. The value to be configured, in seconds, is between 15 and 3600. The value established by default 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 SWT 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 four electrical ports (1 to 4).

5.17 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.

5.18 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 equipment.

A binary images that is appropriate for the equipment is necessary, which can be selected by pressing the button *Examine*.

FIGURE 49 **Reflash** configuration page

Reflash

Upload succeeded.

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

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.

5.19 CONFIGURATION FILE

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

FIGURE 50 Options for uploading (**Upload**) or downloading (**Download**) the configuration file

The screenshot shows a web interface for configuration file management. It is divided into two main sections: 'Upload configuration' and 'Download configuration'.
The 'Upload configuration' section features a text input field, a button labeled 'Examinar...', a checkbox labeled 'Only verify', and a button labeled 'Upload configuration'.
The 'Download configuration' section offers two options: 'Download configuration "conf.txt"' and 'Download configuration (xml format)"conf.xml"'. Both options are underlined, suggesting they are clickable links.

5.19.1 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.

5.19.2 Download (from the equipment to the PC)

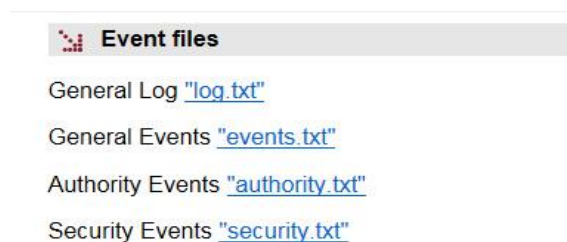
With this option the user obtains a local copy of the operating configuration in **.txt** format or **.xml** format.

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).

5.20 EVENT FILES

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

FIGURE 51 Event Files configuration page



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 accessible 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 six 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 (*Ports*) interfaces, the MAC addresses identified by the switch, STP protocol, LLDP protocol and the synchronization client (*NTP*), 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 executing the ***clear*** command in the prompt, or using the menu option ***Clear Statistics***.

FIGURE 52 Example of statistics related to general data

General Statistics

Uptime	4d21:31:18.389
Time (UTC)	2005/01/01,00:00:00 Change
Time (Local)	2005/01/01,00:00:00 Change
Temperature	42 (C) / 108 (F)
Memory Usage (%)	51
Long term CPU Usage (%)	18
Short term CPU Usage (%)	18
IP Address	172.16.30.93

FIGURE 53 Example of statistics related to the Ethernet ports status

Statistics - Ports

Port	#	Name	In Octets	Out Octets	In Frames	Out Frames	Errors	Link
1		swt-port	327621662	2050463	869049	2236	498	up
2		swt-port 0	0	0	0	0	0	down
3		swt-port 27831	69765	241	409	0	0	down
4		swt-port 0	0	0	0	0	0	down
5		swt-port 0	0	0	0	0	0	down
6		swt-port 0	0	0	0	0	0	down
7		swt-port 0	0	0	0	0	0	down
8		swt-port 0	0	0	0	0	0	down
9		swt-port 0	0	0	0	0	0	down
10		swt-port 0	0	0	0	0	0	down
11		swt-port 0	0	0	0	0	0	down
12		swt-port 0	0	0	0	0	0	down
13		swt-port 0	0	0	0	0	0	down
14		swt-port 0	0	0	0	0	0	down
15		swt-port 0	0	0	0	0	0	down
16		swt-port 0	0	0	0	0	0	down
17		swt-port 0	0	0	0	0	0	down
18		swt-port 0	0	0	0	0	0	down
19		swt-port 0	0	0	0	0	0	down
20		swt-port 0	0	0	0	0	0	down
21		swt-port 0	0	0	0	0	0	down
22		swt-port 0	0	0	0	0	0	down
23		swt-port 0	0	0	0	0	0	down
24		swt-port 0	0	0	0	0	0	down
25		swt-port 0	0	0	0	0	0	down
26		swt-port 0	0	0	0	0	0	down
27		swt-port 0	0	0	0	0	0	down
28		swt-port 0	0	0	0	0	0	down
29		swt-port 0	0	0	0	0	0	down
30		swt-port 0	0	0	0	0	0	down
31		swt-port 0	0	0	0	0	0	down
32		swt-port 0	0	0	0	0	0	down
33		swt-port 0	0	0	0	0	0	down
34		swt-port 0	0	0	0	0	0	down

FIGURE 54 Example of statistics related to a specific port (selection of # parameter)

Statistics - Ports	
Port	3
Name	swt-port
Description	STP
Physical Address	00:E0:AB:02:53:82
In Octets	27831
Out Octets	69765
Total Octets	8919104248
In Frames	241
Out Frames	409
Total Frames	14298285
In Errors	0
Out Errors	0
Errors	0
In Unicasts	6514270
Out Unicasts	4083911
Total Unicasts	10598181
In Broadcasts	1913205
Out Broadcasts	19415
Total Broadcasts	1932620
In Multicasts	1761996
Out Multicasts	5488
Total Multicasts	1767484
CRC align errors	0
Fragments	0
Oversize frames	0
Jabbers	0
Collisions	0
Late collision	0
Frames 64 octets	1946027
Frames 65 to 127 octets	2221521
Frames 128 to 255 octets	486092
Frames 256 to 511 octets	102819
Frames 512 to 1023 octets	57591
Frames 1024 to 1536 octets	5375421
Ready	on
Link	down
Speed	100000000
Duplex	fullduplex
Tx Power	unknown
Rx Power	unknown

FIGURE 55 Example of statistics related to 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	learned
	8	00:1D:09:5A:0A:0A	1	yes	2	learned
	9	00:1D:09:5A:0A:0A	1	yes	2	learned
	10	00:1D:09:5A:0A:0A	1	yes	2	learned
	11	00:1D:09:5A:0A:0A	1	yes	2	learned
	12	00:1D:09:5A:0A:0A	1	yes	2	learned
	13	00:1D:09:5A:0A:0A	1	yes	2	learned
	14	00:1D:09:5A:0A:0A	1	yes	2	learned
	15	00:1D:09:5A:0A:0A	1	yes	2	learned
	16	00:1D:09:5A:0A:0A	1	yes	2	learned
	17	00:1D:09:5A:0A:0A	1	yes	2	learned
	18	00:1D:09:5A:0A:0A	1	yes	2	learned
	19	00:1D:09:5A:0A:0A	1	yes	2	learned
	20	00:1D:09:5A:0A:0A	1	yes	2	learned
	21	00:1D:09:5A:0A:0A	1	yes	2	learned
	22	00:1D:09:5A:0A:0A	1	yes	2	learned
	23	00:1D:09:5A:0A:0A	1	yes	2	learned
	24	00:1D:09:5A:0A:0A	1	yes	2	learned
	25	00:1D:09:5A:0A:0A	1	yes	2	learned
	26	00:1D:09:5A:0A:0A	1	yes	2	learned
	27	00:1D:09:5A:0A:0A	1	yes	2	learned
	28	00:1D:09:5A:0A:0A	1	yes	2	learned
	29	00:1D:09:5A:0A:0A	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

Reload

FIGURE 56 Example of statistics related to 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	none
5	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
6	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
7	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
8	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
9	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
10	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
11	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
12	disabled	discarding	0	80:00:00:e0:ab:11:55:ea	on	off	none
13	disabled	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 57 Example of statistics of the LLDP protocol

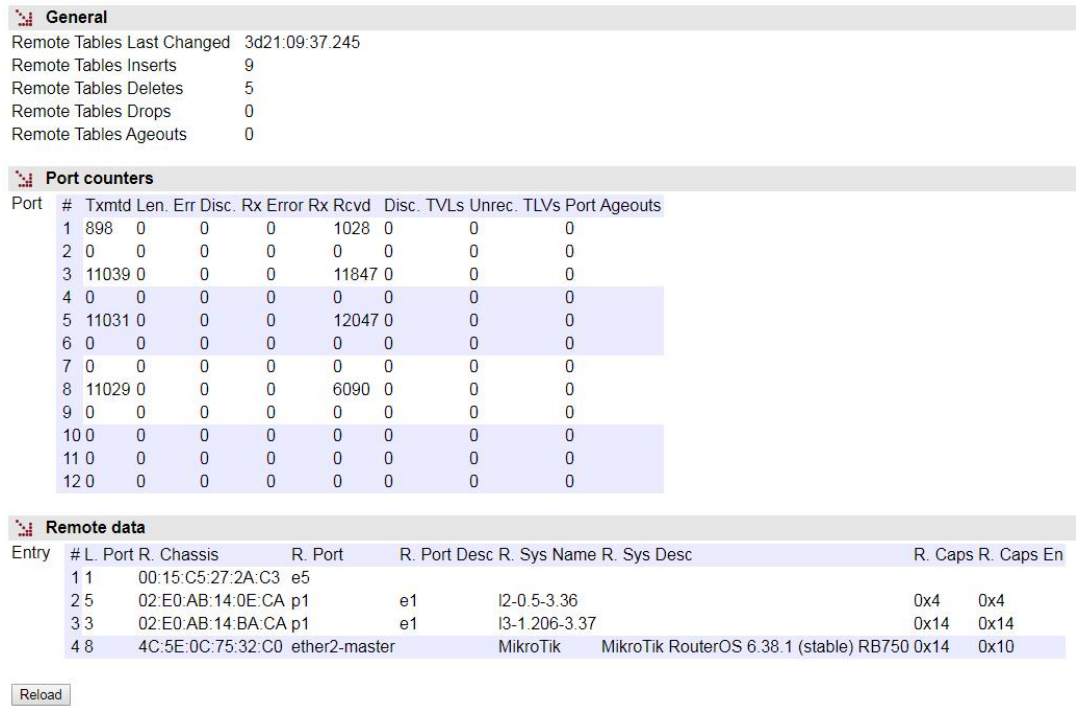
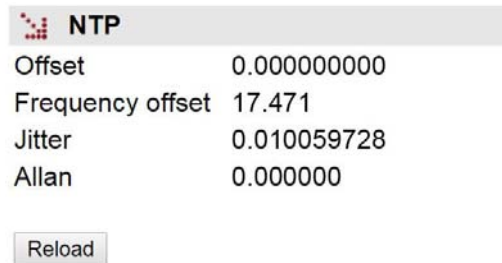


FIGURE 58 Example of statistics related to NTP



APPENDIX A

BIBLIOGRAPHY AND ABBREVIATIONS

APPENDIX A

BIBLIOGRAPHY AND ABBREVIATIONS

A.1 BIBLIOGRAPHY

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

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

[3] 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

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 in 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

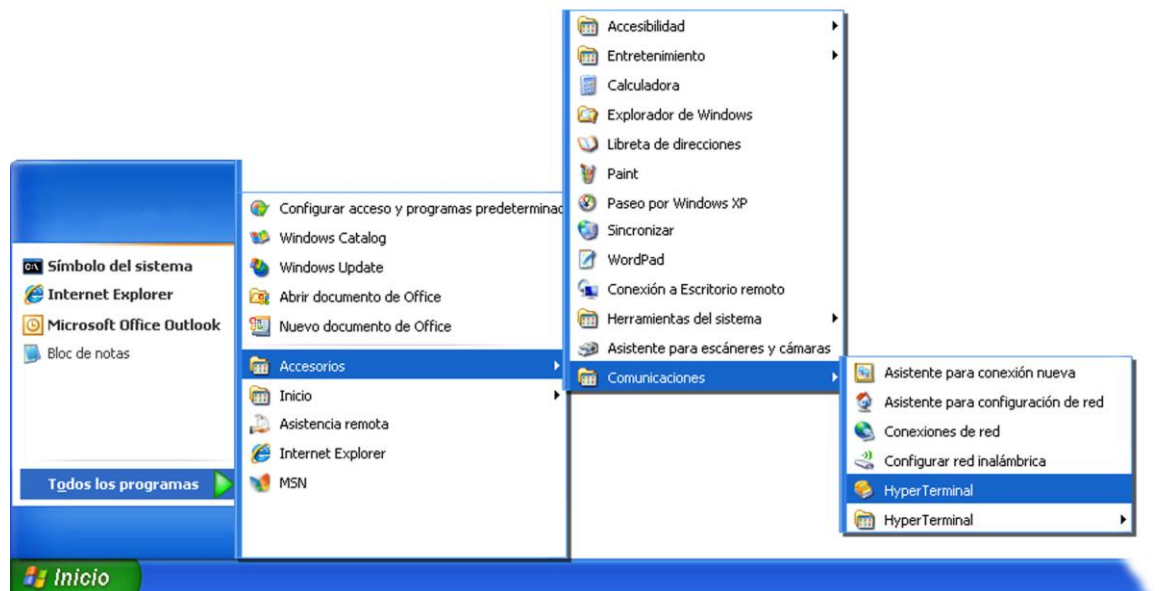
Local mode access is obtained through a flat serial cable that connects the serial port of the computer to the serial port of the equipment (SRV).

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 59).

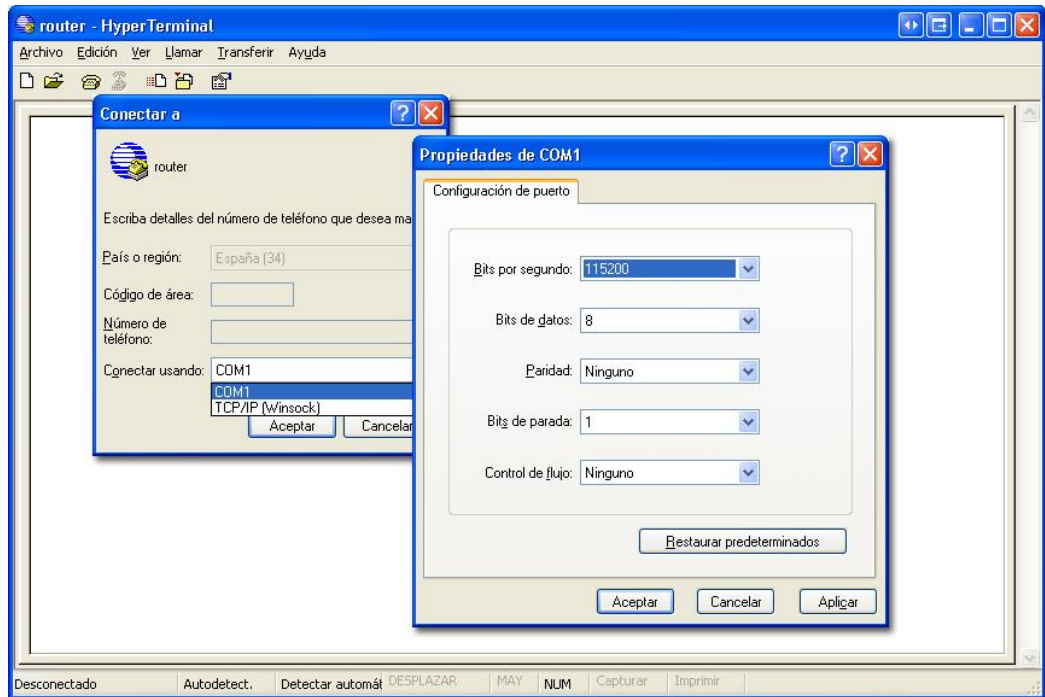
FIGURE 59 Location of *HyperTerminal* in Windows XP®



SWT

On opening *HyperTerminal* a text box appears, requesting the necessary information to establish the connection (see FIGURE 60).

FIGURE 60 Connection configuration through the serial port with *HyperTerminal*



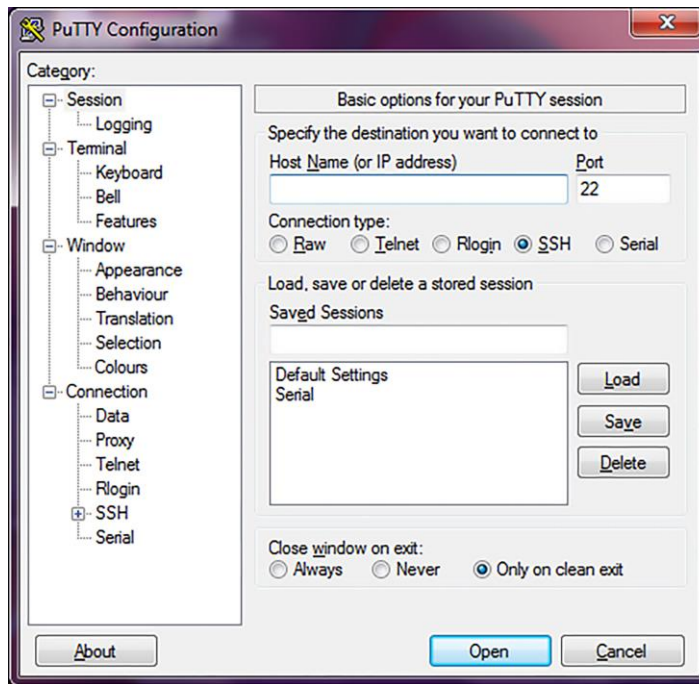
Run the *Call* option of the *Call* menu. Pressing return, a window is shown in which the **swt login:** prompt will appear, ready for the user to enter the *login* and code for starting the session (the logins and their respective passwords are the same as in the web interface).

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 61 *PuTTY* home window



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 62 *Device administrator* window

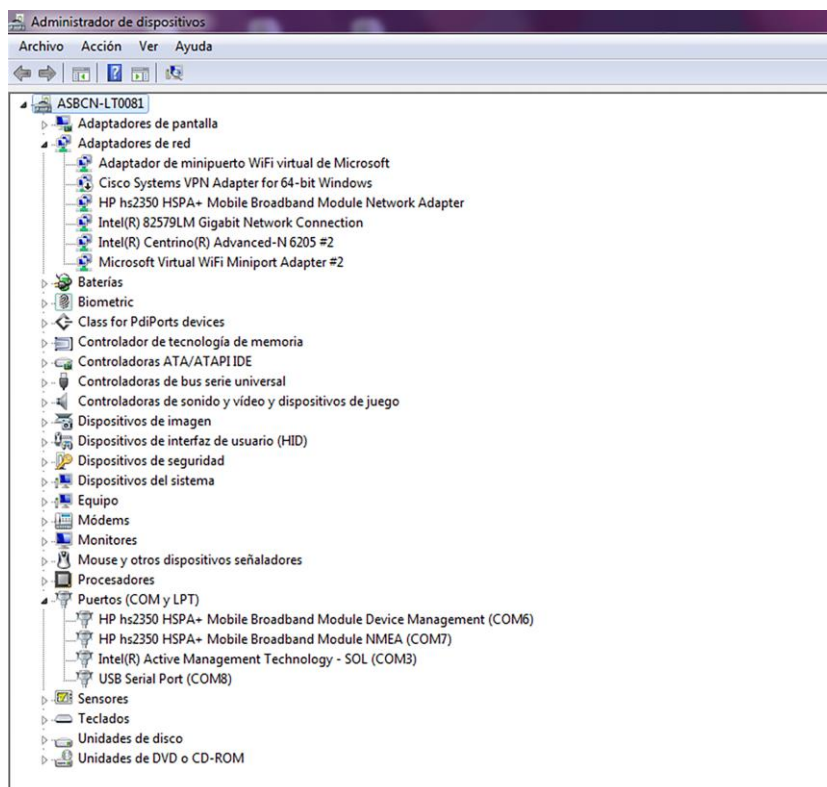
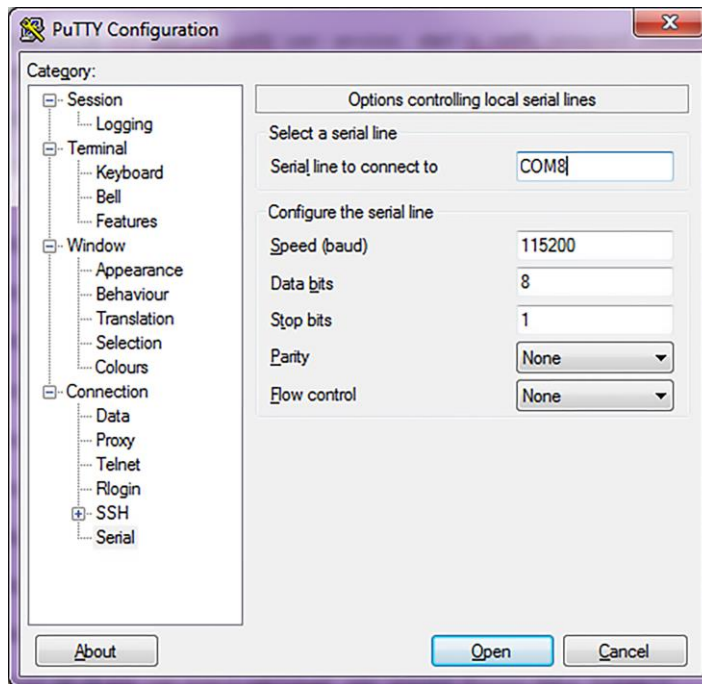


FIGURE 63 Connection configuration through the serial port with *Putty*



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.

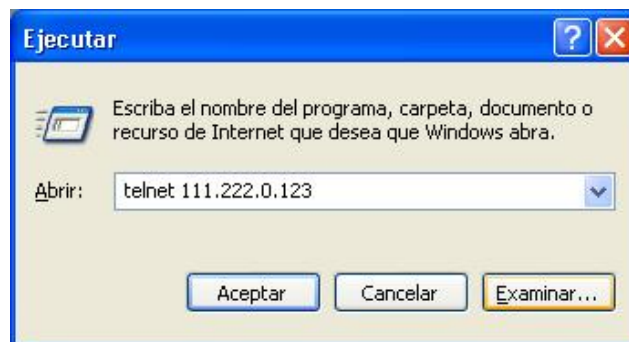
Access by means of Telnet

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.

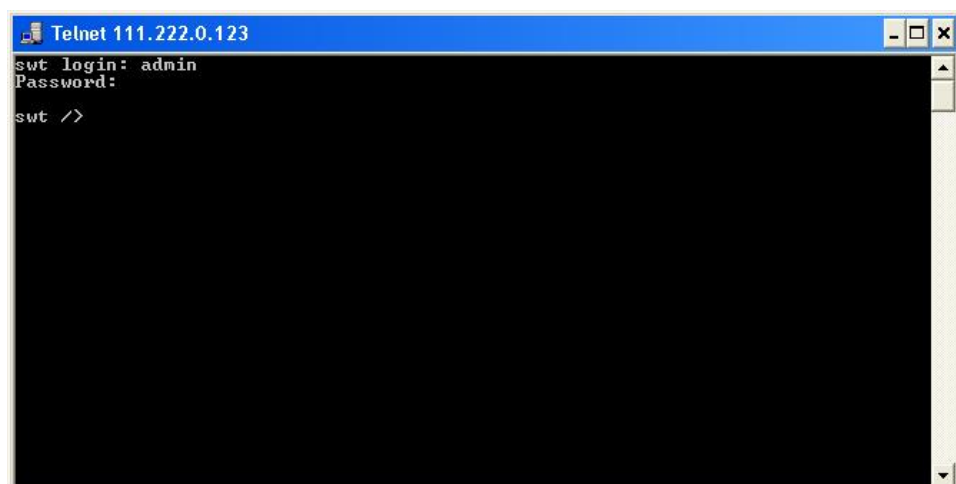
Telnet can be executed in Windows XP© from the Start button: *Start* → *Execute*, and in the text box, enter: *telnet* + space + *Equipment_IP_address* (111.222.0.123 in the example), and then press *Accept* (see FIGURE 64).

FIGURE 64 *Execute.. Telnet* text window to establish connection with the equipment



On pressing the *Accept* button a *System* symbol window will appear with the *Telnet* programme connected to the equipment (see FIGURE 65).

FIGURE 65 *Telnet* window



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 **equipment 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 66. By pressing *Accept*, the Telnet client of Windows may be used.

FIGURE 66 Window of characteristics of Windows



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	✓	✓
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	Equivalent to the log command and also allows the query of old log files by specifying the filename as a parameter	✓	✓
stats	Shows the equipment status	✓	✓
tail	Shows the list of events stored in the log file 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.

Configuration commands

add Adds a new item to the matrix of a matrix-type parameter.

Syntax: `drn /> 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 *nat[1]* and *nat[2]* already existed, on executing the command `add nat` the item *nat[3]* is created.

Examples: `drn /> add nat`
`drn /wan> add tunnel/tunnel`
`drn /admin> add ../nat`

apply This applies the configuration changes in the equipment, but without saving them.

Syntax: `drn /> 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: `drn /> 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: `drn /> 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: `drn /> download`

get This shows the current values of one or several equipment configuration parameters.

Syntax: `drn /> get [nombre]`

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:

```

drn /> get
drn /> get main
drn /main> get hostname
drn /> get main/hostname
drn /admin> get ../main/hostname

```

remove This eliminates an item from the matrix of a matrix-type parameter.

Syntax: `drn /> remove name[no]`

Arguments:

name Parameter from which the item is to be removed.
n^o (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:

```

drn /> remove nat[2]
drn /> remove nat
drn /admin> remove ../nat

```

restore This applies the factory configuration.

Syntax: `dn /> restore`

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

Example: `dn /> 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: `dn /> save`

Arguments: -

Observations: This command can be used irrespective of the directory where the user is.

Example: `dn /> save`

set This changes the value stored in the configuration parameters or in the attributes of an item in a matrix-type parameter.

Syntax: `drn /> set [name][[n°]/[name2]]`

Arguments: -

name name of the parameter to be changed.
n° 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:

```
drn /main> set hostname  
drn /> set main/hostname  
drn /admin> set ../main/hostname  
drn /> set nat[2]/origin
```

Control commands

cd Changes the active directory.

Syntax: drn /> **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: **drn /main>**.

Examples: drn /> **cd main**
drn /main> **cd ../admin**

exit This closes the connection between the computer and the equipment, and therefore the CLI programme session.

Syntax: drn /> **exit**

Arguments: -

Observations: -

Example: drn /> **exit**

quit This closes the connection between the computer and the equipment, and therefore the CLI programme session.

Syntax: drn /> **quit**

Arguments: -

Observations: -

Example: drn /> **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: dnr /> **reboot**

Arguments: -

Observations: -.

Example: dnr /> **reboot**

reload Reloads the saved configuration in the equipment.

Syntax: dnr /> **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: dnr /> **reload**

telnet Open a telnet session, keeping the connection established between the computer and the equipment open.

Syntax: dnr /> **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: dnr /> **telnet** dnr
 dnr /> **telnet** 172.16.50.38 23

Status and Diagnostic Commands

clear Deletes the statistics.

Syntax: drn /> **clear**

Arguments: -

Observations: -

Example: drn /> **clear**

date Shows the date and time recorded in the equipment.

Syntax: drn /> **date**

Arguments: -

Observations: -

Example: drn /> **date**

help Displays a list of all the available commands and a brief description of their functions.

Syntax: drn /> **help**

Arguments: -

Observations: -

Example: drn /> **help**

log Shows the list of events stored in the log file in use (current).

Syntax: `drn /> 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:
`drn /> log`
`drn /> log crit`
`drn /> log debug`

Is 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: `drn /> Is`

Arguments: -

Observations: -

Example: `drn /> Is`

ping This sends ICMP ECHO_REQUEST packets to a specific host.

Syntax: drn /> **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: drn /> **ping 172.16.50.38**
drn /> **ping emr**

show Shows the contents of the log file specified.

Syntax: drn /> **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: drn /> **show messages**
drn /> **show messages.0**
drn /> **show messages.1**
drn /> **show messages.2**
drn /> **show messages.3**

drn /> **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: `drn /> 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 `drn/mac>`, the execution of the command **stats** shows the MAC addresses identified by the switch.

Examples:

```
drn /> stats
drn /> stats main
drn main/> stats temperature
drn main/> stats ../lan/eth0/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: `drn /> 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: `drn /> tail`

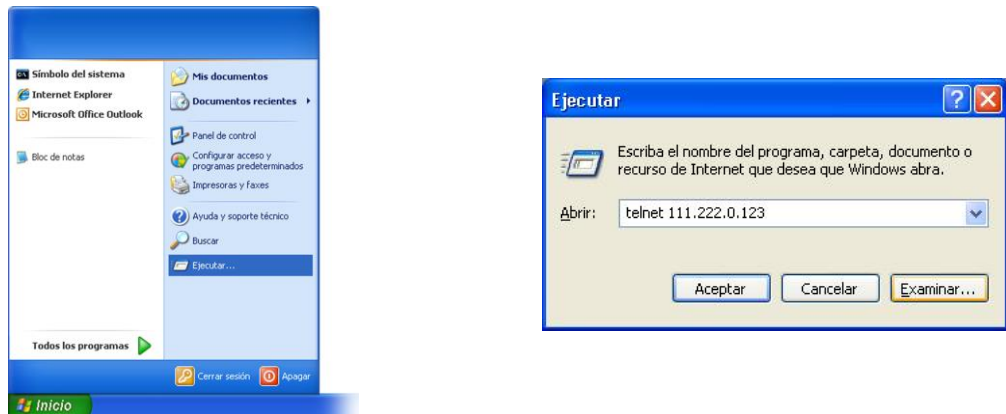
B.3 OBTAINING INFORMATION ABOUT THE STATUS AND CONFIGURATION OF A EQUIPMENT

To obtain information about the status and configuration of an equipment, proceed as follows:

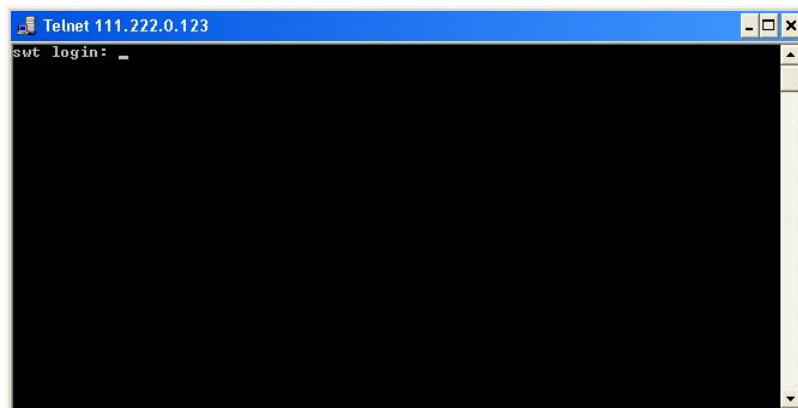
1- Connection with the equipment

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**.



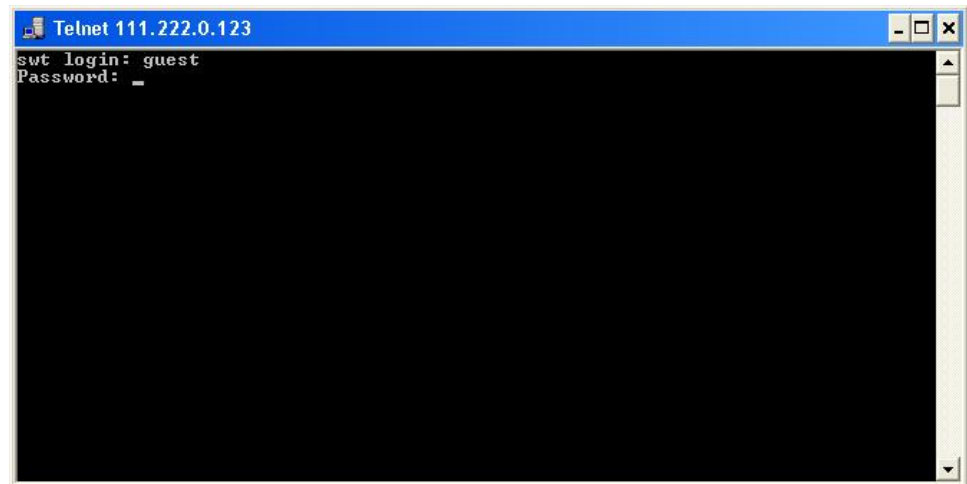
If everything is functioning normally, a window will pop up with a system symbol, which is the interface for the connection.



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.

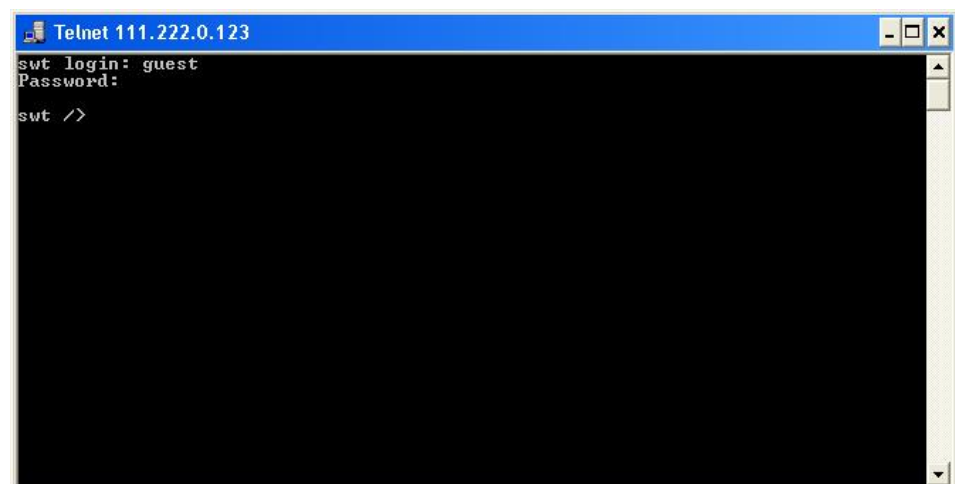
Given that we only want information, it makes no difference which login is entered (**admin** or **guest**). Enter **guest** and then press **enter**.



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**.

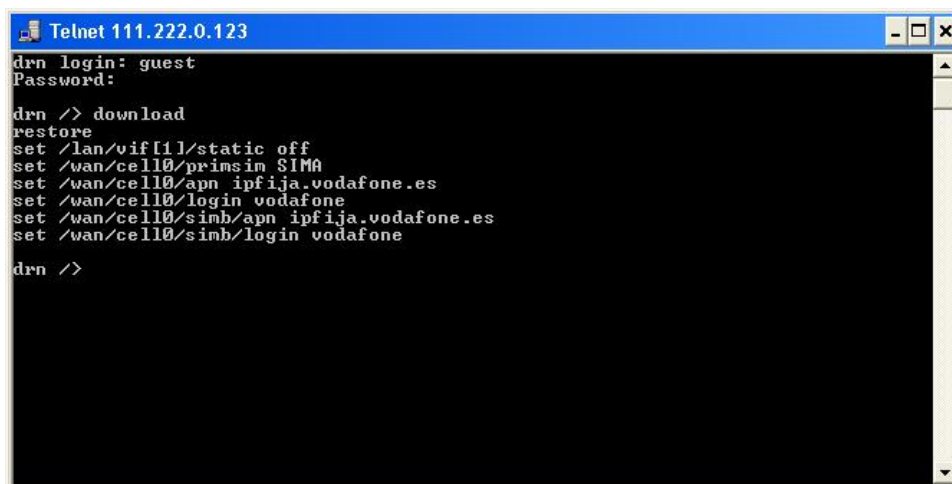
Remember that no text will appear in the *Telnet* window when entering the password.

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.



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**.



```

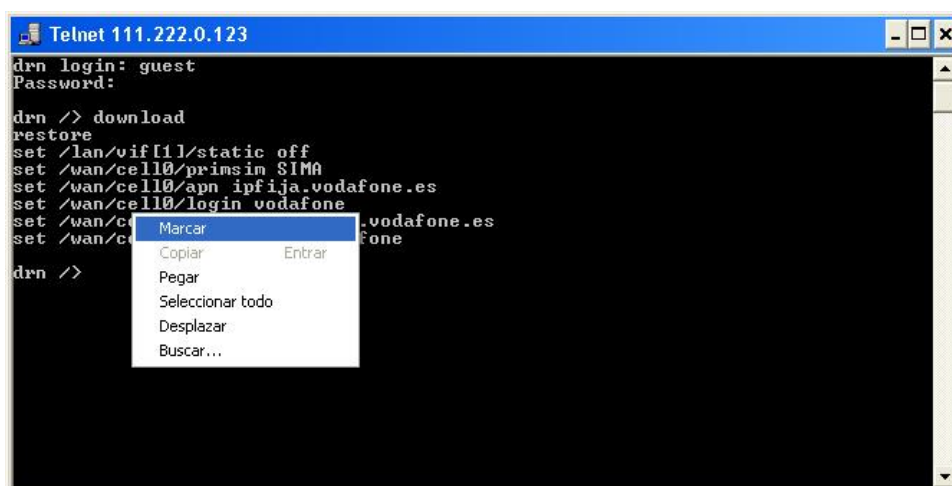
Telnet 111.222.0.123
drn login: guest
Password:

drn /> download
restore
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn ipfiija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/simb/apn ipfiija.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.




```

Telnet 111.222.0.123
drn login: guest
Password:

drn /> download
restore
set /lan/vif[1]/static off
set /wan/cell0/primsim SIMA
set /wan/cell0/apn ipfiija.vodafone.es
set /wan/cell0/login vodafone
set /wan/cell0/simb/apn ipfiija.vodafone.es
set /wan/cell0/simb/login vodafone
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.

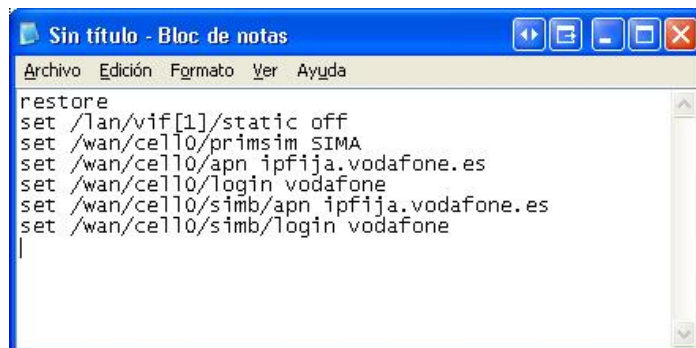


```
Telnet 111.222.0.123
drn login: guest
Password:

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.



```
Sin título - Bloc de notas
Archivo Edición Formato Ver Ayuda
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**.

```

Telnet 172.16.50.38
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**.

```

Telnet 172.16.50.38
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.

```

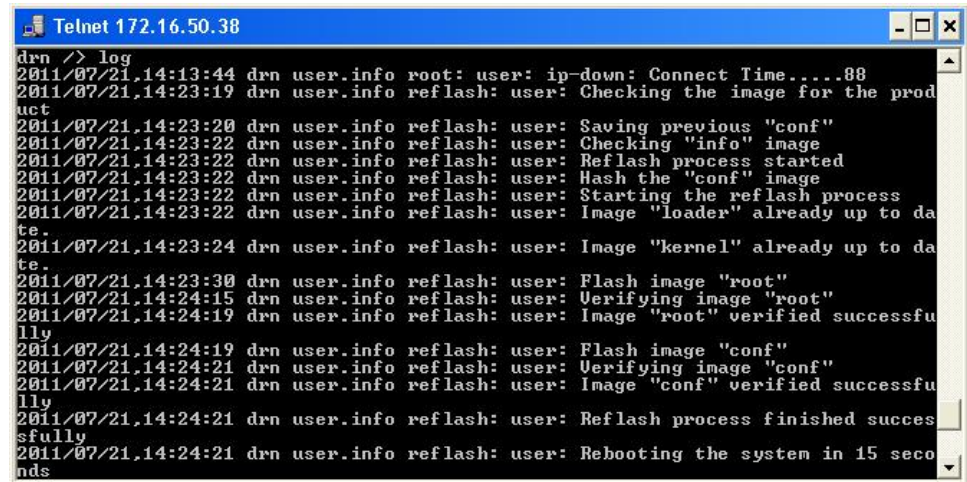
Like the previous commands, if the information to be displayed exceeds the edges of the window, it will stop and wait for the user to press a key to continue.

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 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 status of an equipment obtained with the get command and saved in a .txt file

```

swt /> get
/
main/
hostname          = 12-42.17-3.31_12
location          = unknown
contact           = pep
product           = 3SWTES001NM300AM
version           = 3.31.15.43718
fw_reference      = 4WF72030000-R014
trackingnumber    = 00001888b5d9
serialnumber      = 1000000
guestlogin        = guest
guestpwd          =
th4sIAAhvKF0CAzM0AAPtgsTi4vIUAMakoosAhaAAAA5M2N1NmFiN2I0MzA2UZDk0ZTE3YzM3YU0zjQ3Y2UwZgo=
adminlogin        = admin
adminpwd          =
th4sIAAhvKF0CAzM0AAPtgsTi4vIUAYMAKNS1mxAAAAB1MjRiMwM4NmNmMwI3UZDh1MWQyNDY5OWZiMWE3NWUyMAo=
timezone          = Madrid
time              = 2019/07/12,11:29:12
localtime         = 2019/07/12,13:29:12
admin/
web/
http              = on
httpport         = 80
https            = on
httpsport        = 443
cert              = empty
privatekey        = empty
privatekeypwd    =
th4sIAAhvKF0CAzM0AAPtktTikoySkojiADNy9u0RAAAAYjg00DzkZGR1YtdkvZGM0NWQ30T1iN2M5YjlmM2M5NWMK
ftp               = off
ftps              = off
ftp_idle         = 120
cli/
syslog_level      = 4
syslog_level_remote = 4
syslog            = off
syslog_server     = 0.0.0.0
shell/
telnet            = on
ssh               = on
sshport          = 22
sshidle          = 60
eth0/
static            = off
ip                = 192.168.0.1
mask              = 255.255.255.0
vlanid            = 1
dgw               = 0.0.0.0
mac               = 02:E0:AB:01:33:40
swt_int_mode      = Interrupt_mode
swt_int_devnum    = 0
qing/
stag              = 0x88A8
vlanoverlapping/
enable            = off
vlan[ ]/
[vlan] name       vid prioever priority
-----
1                 vlan_name 1   off    0
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
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                e11     on      edge      auto 1   auto   none off
12                e12     on      edge      auto 1   auto   none off
13                e13     on      edge      auto 1   auto   none off
14                e14     on      edge      auto 1   auto   none off
15                e15     on      edge      auto 1   auto   none off
16                e16     on      edge      auto 1   auto   none off
17                sfp1    on      edge      auto 1   auto   none off
18                sfp2    on      edge      auto 1   auto   none off
19                sfp3    on      edge      auto 1   auto   none off
20                sfp4    on      edge      auto 1   auto   none off
qos/
weightfair_enable = on
priority[ ]/
[priority] queue
-----
0                 medium
1                 medium
2                 medium
3                 medium
4                 medium
5                 medium
6                 medium
7                 medium
dscp[ ]/
[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
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

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
18     off      all      64000
19     off      all      64000
20     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
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

monitor/
ingress_enable = off
ingress_dest_port = 1
egress_enable = off
egress_dest_port = 1

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
17     off      off
18     off      off
19     off      off
20     off      off

mac/
age_time = 300

stp/
enable = on
version = rstp
priority = 32768
max_age = 20.000000000
hello_time = 2.000000000
forward_delay = 15.000000000
tx_hold_count = 6

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
20     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
-----
-----
4      1      TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      2      TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      3      TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      4      TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      5      TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      6      TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      7      TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      8      TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      9      TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      10     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      11     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      12     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      13     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      14     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      15     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      16     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      17     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      18     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      19     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0
4      20     TXRx  on  30      on  4      on  2      off  5      off  1      off
0.0.0.0

igmp_snooping/
enable = off
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
20     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
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

ntp/
enable = on
protocol = ntp
client/
broadcastenable = off
server[]/
[server] ip          type  minpoll maxpoll authenable authkey
-----
1      10.212.43.205 unicast 5      10    off    1

snmp/
client[]/
[client] ip          poll units  authenable authkey timeout
-----
1      192.168.0.1 1    minutes off    1      5

igmp/
enable = off

gmrp/
enable = off
port[]/
[port] 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

snmp/
enable = on
trapenable = on
trap_v1_agent_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
tH4sIAA1vKF0CAzM0AAPT0uLUnMTSkoyCxOLi8vyiFADVIuggGAAAADCwODc2cy2FmZGE1OGUwNDUwNTcyMTU2M2Eymz1mOTJhCg==
DES
tH4sIAA1vKF0CAzM0AAPT0uLUnIKizLKcXOLi8vyiFAB+BTWOGAAAAGN1ZTc1cmj1mOWVmOTUXOGMzMDU1MjRlZmZhNDgxYjBhCg==
traphost[]/
[traphost] community type ip          port
-----
1      public  v2c  10.212.40.13 162

traphostv3[]/
[traphostv3] user  type security auth_alg auth_passwd
priv_alg priv_passwd
ip          port
-----

1      public trap clear  MD5
tH4sIAA1vKF0CAzM0AAPT0uLUnMTSkoyCxOLi8vyiFADVIuggGAAAADCwODc2cy2FmZGE1OGUwNDUwNTcyMTU2M2Eymz1mOTJhCg==
DES
tH4sIAA1vKF0CAzM0AAPT0uLUnIKizLKcXOLi8vyiFAB+BTWOGAAAAGN1ZTc1cmj1mOWVmOTUXOGMzMDU1MjRlZmZhNDgxYjBhCg==
10.212.40.13 162
traps/
dig_in_change = on
dig_out_change = on
lldp_change = on

access/
tacacsplus/
server1_ip = 0.0.0.0
server2_ip = 0.0.0.0
encrypted = on
shared_key = tH4sIAA1vKF0CAzM0AANTAHFEx4YIAAAANDI5OTM3YzMyN2VmYjU4MTC2NjM3MmMy10WJ1mWniOGQK
guest_lv1 = 1
admin_lv1 = 2

radius/
server1_ip = 0.0.0.0
server2_ip = 0.0.0.0
udp_port = 1812
secret =

tH4sIAApvKF0CAzM0AAPTqswyQyNjEIMAgNPFdBAAAABiZTJlODhjYjNkNDJhbnJhZmNwYXMDZkMGM1OTUyYjviZaO=
-----

```



```

timeout = 10
guest_lvl = 1
admin_lvl = 2
console/
method = local
web/
method = local
local = on
telnet/
method = local
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
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
dot1x/
enable = off
reauth_enable = on
reauth_period = 3600
reauth_max = 2
quiet_period = 60
radius_server/
ip = 0.0.0.0
udp_port = 1812
secret = tH4sIAApvKF0CAzM0AANTAHFEx4YIAAAANDI50TM3YzmyN2VmYjU4MTC2NjM3MMmYlOWJlMWNiOGQK
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.

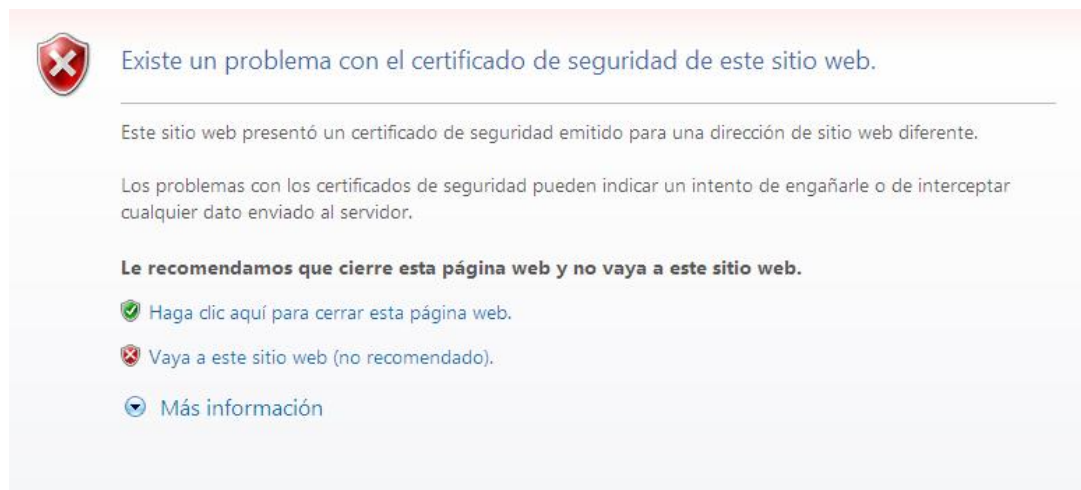
5- In the equipment, activate the access by means of HTTPS
(**"set https on"**)

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:



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 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+NbBdYynDANBqkqhkiG9w0BAQUFADByMQswCQYDVQQGEWJF\
nUZESMBAGA1UECBMJQmFyY2Vsb25hMRlWEAYDVQQHEW1CYXJjZWxvbmExDDAKBGNV\n
BAoTA1pJVjEOMAwGA1UEAxMSm9zZXAxHTAbBgkqhkiG9w0BCQEWdmouc2FsYXRRA\ne
m12LmVzMB4XDTEzMDMyNzE1NTAzOVowXDE0MMDMyNzE1NTAzOVowc2E1MAkGA1UE\n
BhMCRVVMXEAjAQBGNVBAGTCUJhcmlbG9uYUUESMBAGA1UEBxMjQmFyY2Vsb25hMQww\n
nCgYDVQKEWNaSVYxZjAMBGNVBAMTBUpvc2VWMR0wGwYJKozIhvcNAQkBFg5qLnNh\n
\ nbGF0QHppdi5lczBzANBqkqhkiG9w0BAQEFAAOBjQAwYkCgYEA49IfdFD/xVO\n
\n Gsql217s6aumdfwr9NYoJw68LbrHY0Vz9OGwen+a1XajBc121qLZjf11Oh250awE\n
\n eZLH317D5bxS9c+w8YrXowEnYoxUQpK49YGvH7DnqLayI5ptyQbdyMoTkMcxBOZ\n
\n njNoToViogIz9GRBg6nKCDC4+Pxn3/90CAWEAATANBqkqhkiG9w0BAQUFAAOBqQAT\n
\n n7Qt00JT61LcGciF4R5aooiRoZEiTJQBfM6PotZ21apGGhF1Bz0FPn3LRxC1Mb6PI\n
\n nkNatYteCq5FJNjGunF8hDIQVc1x702ju2vmG0iyVfsz1eqiy+Tx0dMYsgpBeY3K+\n
\n n8fb+J1jmlPNzPhgm1zPK6VGNA70/QhfCG915xK1owQ==\n-----END CERTIFICATE-----"
set /admin/web/privatekey "-----BEGIN RSA PRIVATE KEY-----
\nMIICWwIBAAKBgQC3j0h918P/FU4ayovbxuzpq6z0Vav01ignDrwtusdjRVn04bB6\n
\n nf5qVcCMFyXawotmN/WU6HbnRprYR5ksffwUP1vFL1z7DxivBehYSdg7FRckrj1ga8\n
\n fsOeosDIjmm3Jbt3IyhOQxzEE5mM2hohwKgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB\n
\n nAOGA0vDzYhVKhjodHlUzm3lbsZzAk1KAKNorgn8kxpbYE/RM8mkv9f/Lb3jwhiEu\n
\n nxyf7m7BmNmCex8bSRwduzrUnK66DW8jP3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S\n
\n nApuozFYmh34uBl6SJKudihCs4jm1ocQBQMhQ7mXe7Sk1sgECQDgpdSDx45vm8Yk+\n
\n nGoX4UzCRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcnOpU8bFtQbWfxjkThHthQBN\n
\n nrUeEREj9AkeA0S4ernXQGVJGm7b6JhJXFKkILVyo5vP0C3jx7ByRIMt41k11417Q\n
\n ntzNepkjlcmimzLWuHJAiyTbtvzfVcnu4YQJAax0ax3HkwSgosIppq0QLfGp7yJNQu\n
\n nqt5h+vZ06FTuSFpm3t0D4G0K6M1N0nKNIEm2CAJpg0JU8BY66jupEqGrUQJAW7wp\n
\n ns/1pJEDjPg/p+1keHqvBLwdQZx1dbM442rjn1AZBNzq01ZuwTEvUWCLG3fMt9iBN\n
\n nvq6G4cg+xZA4H7du4QJALq/zgc4N+Ft50Hkj+ay1Xst5nxH8U2Zk1u7ZWZZhOTcw\n
\n nezG/TDLBwkROF2n9VX6TYGesnZ2Ve/+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+NbBdYynDANBggkqhkiG9w0BAQUFADByMQswCQYDVQQGEWJF
UZESMBAGA1UECBMJQmFyY2Vsb25hMRIWEAYDVQQHEW1CYXJjZWxvbmExDDAKBgNV
BAoTA1pJVjEOMAwGA1UEAxMFSm9zZXAxHTAbBgkqhkiG9w0BCQEWdmouc2FsYXRA
eml2LmVzMB4XDTEzMDMyNzE1NTAzOV0xOTUyMDE1MDUyMDE1NTAzOV0wZjE1MAkG
A1UEBhMCRVMxEjAQBGNVBAgTCUJhcmNlbg9uYTESMBAGA1UEBxMJQmFyY2Vsb25hMQww
CgYDVQQKEWNaSVYxZjAMBGNVBAmtBUpvc2VwMR0wGwYJKoZIhvcNAQkBFg5qLnNh
bGF0QHppdi5lczCBnzANBggkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA49IfdFD/xVO
GsqL217s6aumdfwr9NYoJw68LbrHY0VZ90Gwen+a1XajBcl2lqLzjf11oh250awe
eZLH311d5bxS9c+w8YrwxowEnYoxUqPK49YgVH7DnqLayI5ptyQbdyMotkMcxB0Z
jNoToVioGiZ9GRBg6nKCDC4+Pxn3/90CAWEAATANBgkqhkiG9w0BAQUFAAOBgQAT
7Qt00JT61LcGciF4R5aooiRoZEiTJQBfM6PoTZ21apGGhF1Bz0FPn3LRxC1Mb6PI
kNatYteCq5FJNjGunF8hDIQvc1x702ju2vmG0iyvFsZ1eqiy+Tx0dMYsgpBeY3K+
8fb+J1jmlPNzPhgMlzPK6VGNA70/QhFCG915xK1owQ==
-----END CERTIFICATE-----
```

Example of a valid **private key**:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQC3j0h918P/FU4ayovbXuzpq6Z0Vav01ignDrwtusdjRVn04bB6
f5qVccmFyXawotmN/WU6HbnRpYR5ksffwUPlvFL1z7DxivBehYSdg7FRckrj1ga8
fs0eosDIjmm3JBt3IyhOQxzEE5mM2hOhwkgaJn0ZEGDqcoIMLj4/E3f/3QIDAQAB
AoGA0vDzYhVKhjodH1Uzm3lbsZzAk1KAKNorgn8kxbyE/RM8mkv9f/Lb3jwhiEu
xyf7m7BmNmCex8bSRwduzrUnk66Dw8jp3b2tsxJHLYU9UpN1XKDNBHGvgJ7Gis+S
ApuoZFYmh34uB16SJKUdihCs4jm1ocQBQMHQ7mXe7Sk1sgECQQDgPsdX45vm8Yk+
Gox4UzCRIDoU47P3uHnnPTYUQMMqDta3K4bzualwcnOpU8bFtQbwfxjkThHthQBN
rUeEREj9AkeA0S4ernxQGVJGm7b6JhJXFkkILVyo5vP0C3jx7ByRIMt41k11417Q
tzNepKj1cmimzLWuHJAiyTbtvzfvcnU4YQJAaxOax3HkwSgosIpp0QLfGp7yJNQu
qt5h+vZ06FTuSFPm3t0D4G0K6M1N0nKNIEm2CAJpgOJU8BY66jupEqGrUQJAW7wp
s/lpJEDjPg/p+1keHqvBLwdQZx1dbm442rjn1AZBNzq01ZuWTEVUWCLG3fMt9iBN
Vq6G4cg+xZA4H7du4QJALq/zgc4N+Ft50Hkj+ay1Xst5nxH8U2Zk1u7ZWZZhOTcw
ezG/TDLBwkROF2n9VX6TYGesnZ2Ve/+DiMPhK7ZVQA==
-----END RSA PRIVATE KEY-----
```