



XSLAN / XSLAN+ / XSMIL
SHDSL Switch
—————
SETUP GUIDE
—————

The XSLAN, XSLAN+ and XSMIL SHDSL switches are designed and manufactured by

ETIC TELECOM
405 rue Lavoisier
38330 MONTBONNOT SAINT MARTIN
FRANCE

TEL : + (33) (0)4-76-04-20-05
E-mail : hotline@etictelecom.com
web : www.etictelecom.com

OVERVIEW	7
1 Purpose of this manual	7
2 Main features of the XS family.....	7
PREPARING THE SETUP	9
1 Connecting a PC for configuration	9
1.1 Overview.....	9
1.2 First configuration	10
1.3 Changing the configuration later	10
2 Temporary return to the factory settings	10
3 Restoring the factory settings.....	11
4 Protecting the access to the administration server.....	11
5 Configuration steps	12
SETUP	13
1 IP addresses setting	13
2 SHDSL connection set up overview	15
2.1 Principle of operation	15
2.2 Connection profiles	16
3 Setting up a link using one twisted pair.....	17
3.1 Set up steps	18
3.2 Step 1 : SHDSL connection setup	18
3.3 Step 2 : SHDSL test and set up adjustment	20
4 Setting up a link using 2, 3 or 4 twisted pairs.....	22
5 Advanced setting up of an SHDSL link	23
6 RSTP	28
6.1 Overview	28
6.2 Set up.....	29
7 Fail-safe ring.....	32
8 Loop VPN	34
9 VLAN.....	36
9.1 Overview	36
9.2 Set up.....	37
9.3 Administration server and serial gateways.....	41
10 MACSec.....	42
10.1 Overview	42
10.2 Setting up MACSec.....	42
10.3 Password mode	43
10.4 MACSec state	44
10.5 Key management and secure erase	44
10.6 MTU considerations	45
11 IGMP snooping.....	46
11.1 Overview	46
11.2 Setting up the IGMP snooping function	46
12 SNMP.....	47
12.1 Overview	47
12.2 Setting up the SNMP function.....	47
12.3 Setting up the SNMP traps	49

TABLE OF CONTENTS

13	NTP	50
13.1	Overview	50
13.2	Setting up the NTP client.....	50
13.3	Setting up the NTP server	50
14	Quality of service (Qos) - DiffServ	51
14.1	Overview	51
14.2	Basic configuration.....	52
14.3	Advanced configuration	53
15	IP Routing	56
15.1	Overview	56
15.2	Static routes	56
15.3	RIP protocol.....	57
15.4	OSPF protocol	57
16	Advanced NAT	58
16.1	Overview	58
16.2	Set up.....	58
17	Firewall	60
17.1	Overview	60
17.2	Setting up the firewall.....	60
18	Remote power feeding	62
18.1	Overview	62
18.2	Safety aspects	62
18.3	State machine	62
18.4	Details.....	64
18.5	Setting up the Remote power supply.....	64
19	Alarms	66
19.1	SNMP Alarms.....	66
19.2	Digital output.....	66
20	Serial to IP gateways	67
20.1	Overview	67
20.2	Modbus gateway	68
20.3	Raw TCP gateway	73
20.4	Raw UDP gateway.....	75
20.5	Raw multicast gateway	76
20.6	Unitelway gateway.....	77
20.7	Telnet gateway.....	78

DIAGNOSTICS AND MAINTENANCE 79

1	Visual diagnostic.....	79
2	Log	79
3	Link quality measurement	80
4	SHDSL statistics	82
5	Gateways status	83
6	PING tool	84
7	Line Cut Detection (LCD)	85
7.1	Overview	85
7.2	Launching the LCD tool	85
7.3	Advanced results	86
7.4	Cable profile management.....	88
8	Repeater Discovery (RD).....	89
9	Saving and loading a configuration file	90

TABLE OF CONTENTS

10	Updating the firmware	92
ANNEX 1 : SNMP MIB		93
1	Purpose of the document	93
2	Accessible OIDs and MIBs	93
2.1	Supported MIBs	93
2.2	Network interface indexes	94
2.3	Querying the MIB.....	94
3	Description of the supported OIDs	95
3.1	Sysdesc, Syslocation, SysName	95
3.2	Network interfaces table (IF-MIB::ifTable)	95
3.3	SHDSL MIB (HDSL2-SHDSL-LINE-MIB)	96
3.4	MIB : BRIDGE-MIB::dot1dBridge.....	97
ANNEX 2 : SHDSL data rate versus distance		99
ANNEX 3 : XSLAN and XSLAN+ switches compatibility		101

OVERVIEW

1 Purpose of this manual

This manual describes how to set-up the XSLAN, XLAN+ and XSMIL families of SHDSL switches manufactured by ETIC TELECOM.

It is applicable for products with firmware version 2.4.0 or higher.

This manual applies in particular to the models listed below :

XSLAN-1100	Industrial grade - 1 SHDSL port Ethernet switch
XSLAN+1xxx	Industrial grade - 1 SHDSL port Ethernet switch
XSLAN+2xxx	Industrial grade - 2 SHDSL ports Ethernet switch
XSLAN+4xxx	Industrial grade - 4 SHDSL ports Ethernet switch
XSMIL-4200	Military grade - 4 SHDSL ports Ethernet switch

In this document the name "XS" refers to both XSLAN, XSLAN+ and XSMIL products.

2 Main features of the XS family

The XS family of SHDSL switches enables the connection of remote Ethernet networks with one, two or four twisted pairs (depending on model).

Key features :

- 5,7 Mb/s over 3,7 Km (1 pair diam. 0,9 mm)
- 15 Mb/s over 700 m
- Concentrator with 4 SHDSL ports
- VLAN & SNMP, DiffServ QoS
- Network redundancy (RSTP or proprietary protocol)
- 2 or 4 ports Ethernet 10/100 BT
- 2 serial ports (option)
- T° : -20°C / +70°C
- Bypass feature (option)
- Configuration & diagnostic via html server

PREPARING THE SETUP

1 Connecting a PC for configuration

1.1 Overview

The XS is configured using a PC with a web browser. No additional software is required.

Online help :

For most pages of the administration server an help page is available by clicking **?** located at the top right of the page.

Administration server address :

When the product is delivered, the IP address of the administration web server is 192.168.0.128.

First setup :

For the first configuration, we advise to connect the PC directly to the LAN interface of the SHDSL switch. Subsequent changes can be made remotely.

Restoring the factory IP address :

The factory IP address 192.168.0.128 can be restored (see the User guide of the product).

Restricted access to the administration server :

If you do not have access to the administration server, it is probably that access has been restricted for security reasons or for other reasons.

Network IP address :

Later in the text, we often speak of "network IP address". We mean the lowest value of the addresses of the network.

For instance, if the netmask of a network is 255.255.255.0, the network IP address of that network is terminated by a zero (X.Y.Z.0.).

Characters allowed :

Accented characters are not supported.

PREPARING THE SETUP

1.2 First configuration

Step 1 : Create or modify the PC TCP/IP connection

Assign to the PC an IP address different but consistent with the factory IP address of the XS.
For the first configuration, assign for instance 192.168.0.1 to the PC.

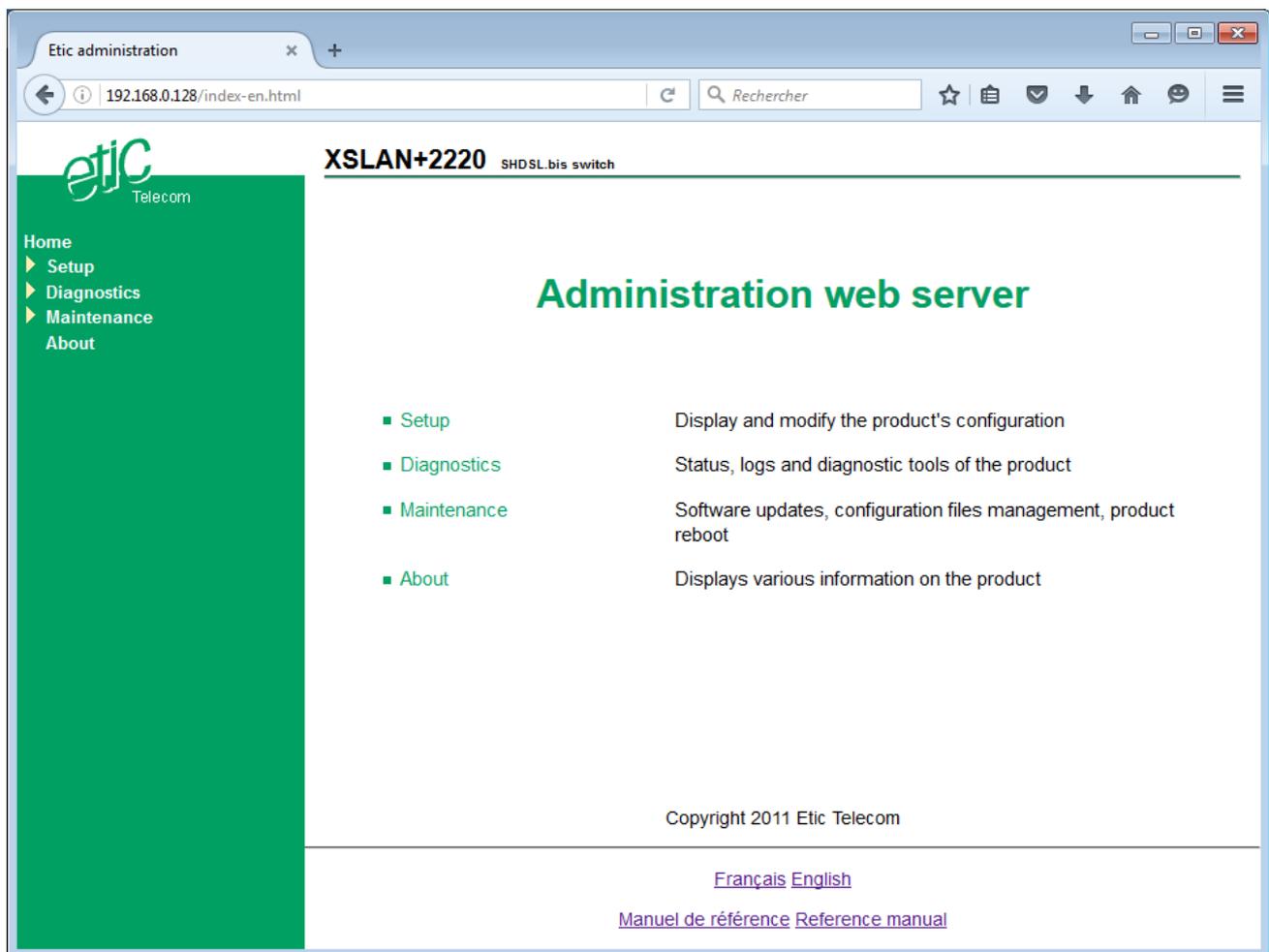
Step 2 : Connect the PC to the XS

Connect the PC directly to the XS with any Ethernet cable (straight or cross-wired);

Step 3 : Launch the web browser

Launch the web browser and then enter the IP address of the XS : 192.168.0.128

The Home page of the administration server is displayed.



Note : Access to the administration server is not protected when configuring the XS for the first time.

1.3 Changing the configuration later

Thereafter, the XS administration server is accessible from the Ethernet interface or remotely through the SHDSL line at the IP address assigned to the product.

- Open the html browser and enter the IP address of the administration server of the XS.
- Enter, if any, the user name and password that protect the access to the administration server.

2 Temporary return to the factory settings

If the IP address of the XS could not be founded, or if it is impossible to access the administration server, for example, following a bad VLAN configuration, it is possible to restore the factory settings without losing the current configuration.

- Keep the push-button pressed for about 3 seconds;
- The LED  blinks red rapidly
- The administration server becomes accessible at the factory IP address (192.168.0.128), in HTTP without a password. The factory configuration is temporarily running. However, the current configuration is not lost and it is the one that is still displayed in the pages of the Administration Server.
- After reading the IP address or changing some parameters, press again the push button or reboot the product.
- The product can be reached at the registered IP address.

Note :

If the IP address of the XS is unknown, the software tool **EticFinder** can be used.

This software detects all ETIC branded products on a local network. After starting the software, click on the "Search" button, and when the product list is displayed, double-click on the product address to access the html server.

3 Restoring the factory settings

To restore the factory settings using the push button,

- Power off the XS,
- Keep the push-button pressed,
- Power on the XS,

The LED  turns red ; the XS boots and the factory configuration is restored.

Note : The factory configuration can also be restored via the menu **Maintenance > Configurations management** of the administration server.

4 Protecting the access to the administration server

- In the menu, choose **Setup > Security > Administration rights**
- Enter a user name and password to protect the administration server.
- Tick the **Password protect the web site access** checkbox

If the username and password to access the administration server are lost, you have to temporarily return to the factory settings; access to the administration server is then free.

5 Configuration steps

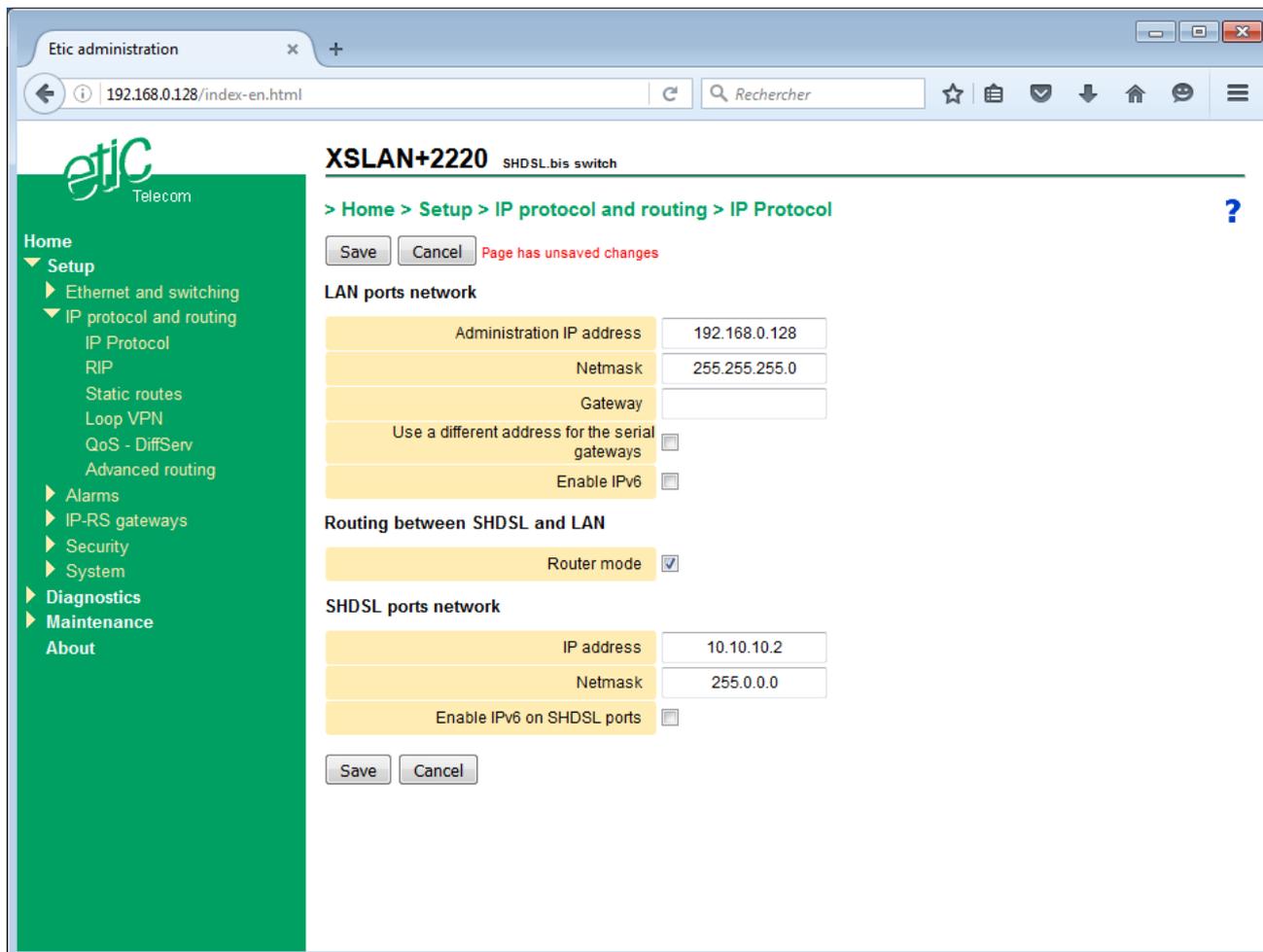
To configure the product, we advise to proceed as follows :

- Set up the LAN interface
- Set up the SHDSL connections
- Set up the RSTP or failsafe ring redundancy protocol
- Set up VLAN
- Set up SNMP
- Set up QoS
- Set up the routing functions
- Set up the serial gateways

SETUP

1 IP addresses setting

- In the menu, choose **Setup > IP protocol and routing > IP Protocol**



- Configure **LAN ports network** parameters :

Administration IP address

This is the IP address assigned to the Ethernet interface of the XS on the local network.

This is the IP address of the administration server and the serial gateways.

Factory value : 192.168.0.128

Netmask

The netmask defines the local network size and which IP address belongs to that network.

Factory value : 255.255.255.0

Default gateway

This is the IP address of the default router on the local network.

SETUP

Use a different address for the serial gateways

By default, the IP address of the serial gateways is the IP address of the administration server of the XS. It may be necessary to set a different IP address for the serial gateways especially when VLAN is enabled; in this case, this box must be checked and an IP address and a subnet mask must be entered.

Default value : Unchecked

Enable IPV6

The IP addresses assigned to the XS must be entered in IPV4 format.

However, the switch also supports IPV6 addressing. If this is checked, IP addresses must also be entered in IPV6 format.

Default value : Unchecked

- Configure **Routing between SHDSL and LAN** parameters:

Router mode

The XS acts as a managed switch.

However, if this box is checked, the XS provides basic IP router features between two interfaces:

LAN Ethernet 10/100BT ports,
and SHDSL ports.

The Ethernet ports are considered as a single interface; SHDSL ports (1 to 4 depending on model) are also considered as a single interface. The XS must have two IP addresses. The one previously defined only applies to LAN Ethernet ports and a new one must be defined for SHDSL ports.

The main purpose is to prevent the broadcast frames or other frames to congest the SHDSL lines.

Default value : Unchecked

The following parameters are only displayed when the IP router mode is selected.

IP address

This is the unique IP address assigned to the SHDSL interfaces of the XS.

Default value : none

Netmask

Subnet mask for the network on the SHDSL port side.

Default value : 255.255.255.0

Enable IPV6 on SHDSL ports

See above.

Default value : Unchecked

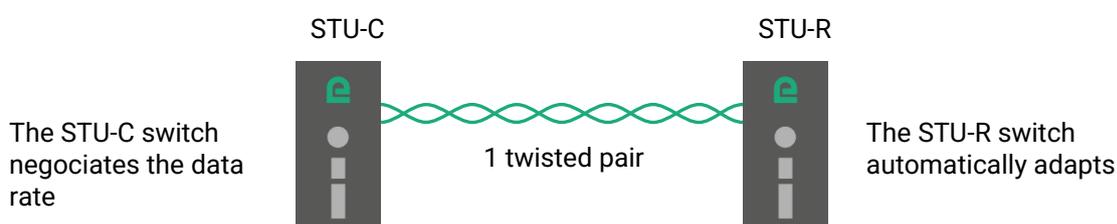
2 SHDSL connection set up overview

2.1 Principle of operation

When two XS switches are connected by a twisted pair, one switch initiates the connection while the other responds and adapts automatically its data rate.

The switch that initiates the connection is called STU-C.
The switch that responds and adapts is called STU-R.

Thus a line is always connected on one side to a switch acting as the STU-C and on the other side to a switch acting as the STU-R.



One switch is normally configured as a STU-C and the other as a STU-R. However, to make the configuration simpler, the switch configured as a STU-C is able to automatically change to STU-R mode if it detects the presence of a STU-C on the remote side. Thus, two XS configured both in STU-C will find a way to connect. One of the two will switch to STU-R.

The STU-C initiates the connection and measure the received signal level and the noise level and calculates the signal to noise ratio.

The longer the distance and the higher the noise level over the line, the smaller the SNR ratio.

A minimum SNR is required to connect two SHDSL switches through a line at a given data rate.

The difference between the SNR ratio as it is measured and the minimum required is the SNR margin.
The greater the SNR margin, the more reliable the connection at a given data rate.
One can select the SNR margin; in that way, one selects the reliability of the connection.

SETUP

2.2 Connection profiles

A connection profile includes all the technical parameters of an SHDSL connection. To make the connection process as simple as possible, five profiles are available. To set an SHDSL connection, one of these profiles has to be assigned to each SHDSL port.

STU-R, Auto

This profile has to be assigned to an SHDSL port when it has to wait for the connection (see the drawing above).

STU-C, Standard

The SHDSL port configured with this profile initiates the connection but is able to switch to STU-R mode if it detects the presence of an STU-C at the other end.

The connection is established at a data rate compliant to the EFM standard up to 5.6 Mb/s.

The SNR ratio margin is medium; the data rate is medium and the risk of disconnection is reasonable in case of any disturbance.

The duration to establish the connection is typically 45 seconds and may take up to 1 minute 30.

This profile is suitable for most situations, i.e. with no or moderate noise and using usual twisted pair transmission cables.

STU-C, Endurance

The SHDSL port configured with this profile initiates the connection but is able to switch to STU-R mode if it detects the presence of an STU-C at the other end.

The connection is established at a data rate compliant to the EFM standard up to 5.6 Mb/s.

The SNR ratio margin is high; the data rate is low and the risk of disconnection is low in case of any disturbance.

The duration to establish the connection is longer, typically 3 minutes and may take up to 5 minutes.

This profile is suitable for medium to very noisy lines or on cables not dedicated to the transmission such as cables with a large diameter or electrical cables.

STU-C, Performance

The SHDSL port configured with this profile initiates the connection but is able to switch to STU-R mode if it detects the presence of an STU-C at the other end.

The connection is established at a data rate compliant to the EFM standard up to 15,2 Mb/s.

The SNR ratio margin is low; the data rate is high and the risk of disconnection is high in case of any disturbance.

The duration to establish the connection is longer, typically 3 minutes and may take up to 5 minutes.

This profile is suitable for slightly noisy lines. The highest data rates are obtained on short distances.

STU-C, Fixed datarate

The SHDSL port configured with this profile initiates the connection.

This profile is not usable directly; It must be edited to select the desired data rate ("Copy and change").

See Advanced setting up of an SHDSL link

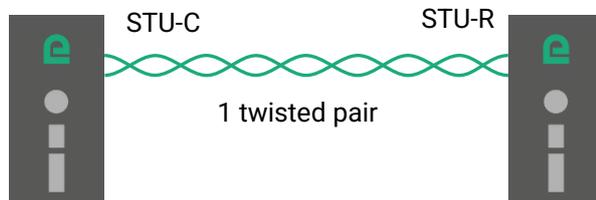
The duration to establish the connection is the fastest, typically 30 seconds.

However, it requires the user to perform tests by changing the data rate until getting a connection with the expected SNR ratio margin.

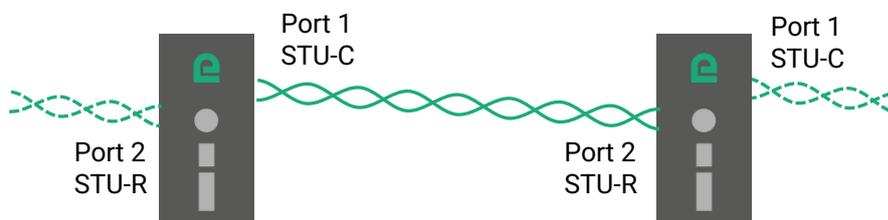
3 Setting up a link using one twisted pair

This section describes the implementation of a point to point link on a twisted pair.

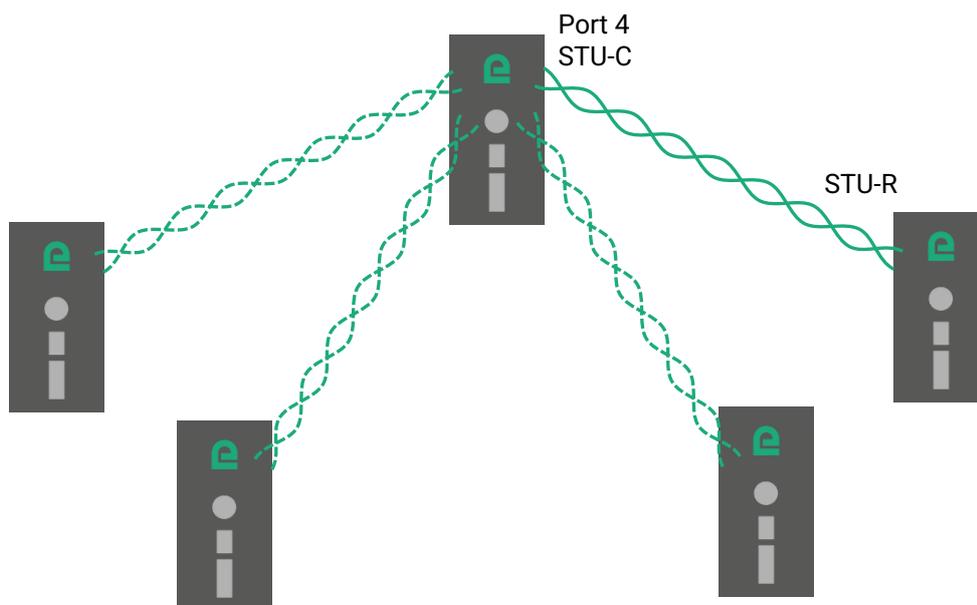
Either between two XS as in the diagram below.



Or between two XS in case of a daisy chain or a ring network, as in the diagram below.



Or between an XS used as a concentrator and several single port XS as in the diagram below.



SETUP

3.1 Set up steps

Step 1 : SHDSL connection set up

Assign the **STU-R, Auto** profile to the SHDSL port of the first XS.

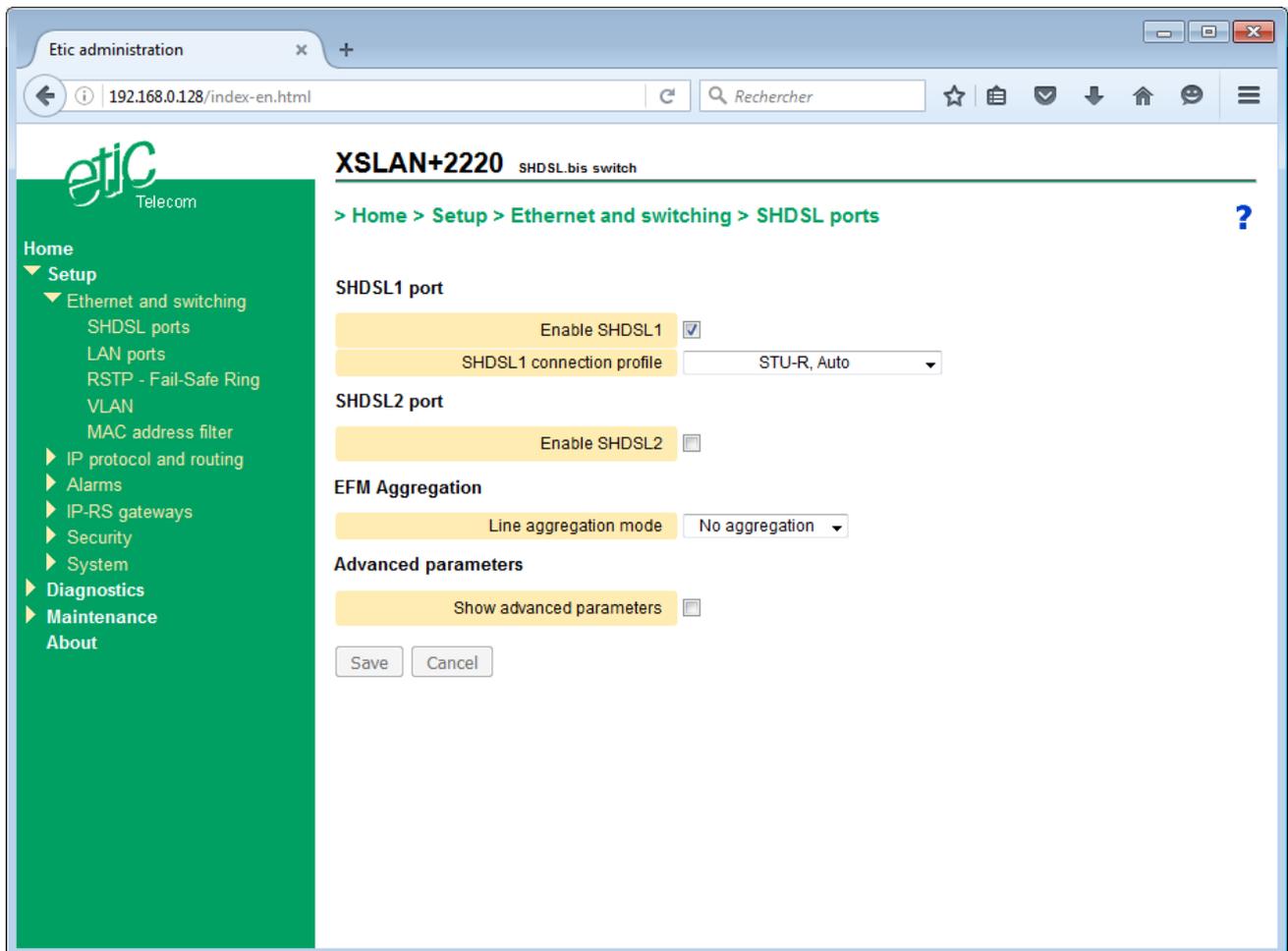
Assign a connection profile to the other XS (**STU-C, Standard** or **STU-C, Endurance** or **STU-C, Performance**).

Step 2 : SHDSL test and set up adjustment

3.2 Step 1 : SHDSL connection setup

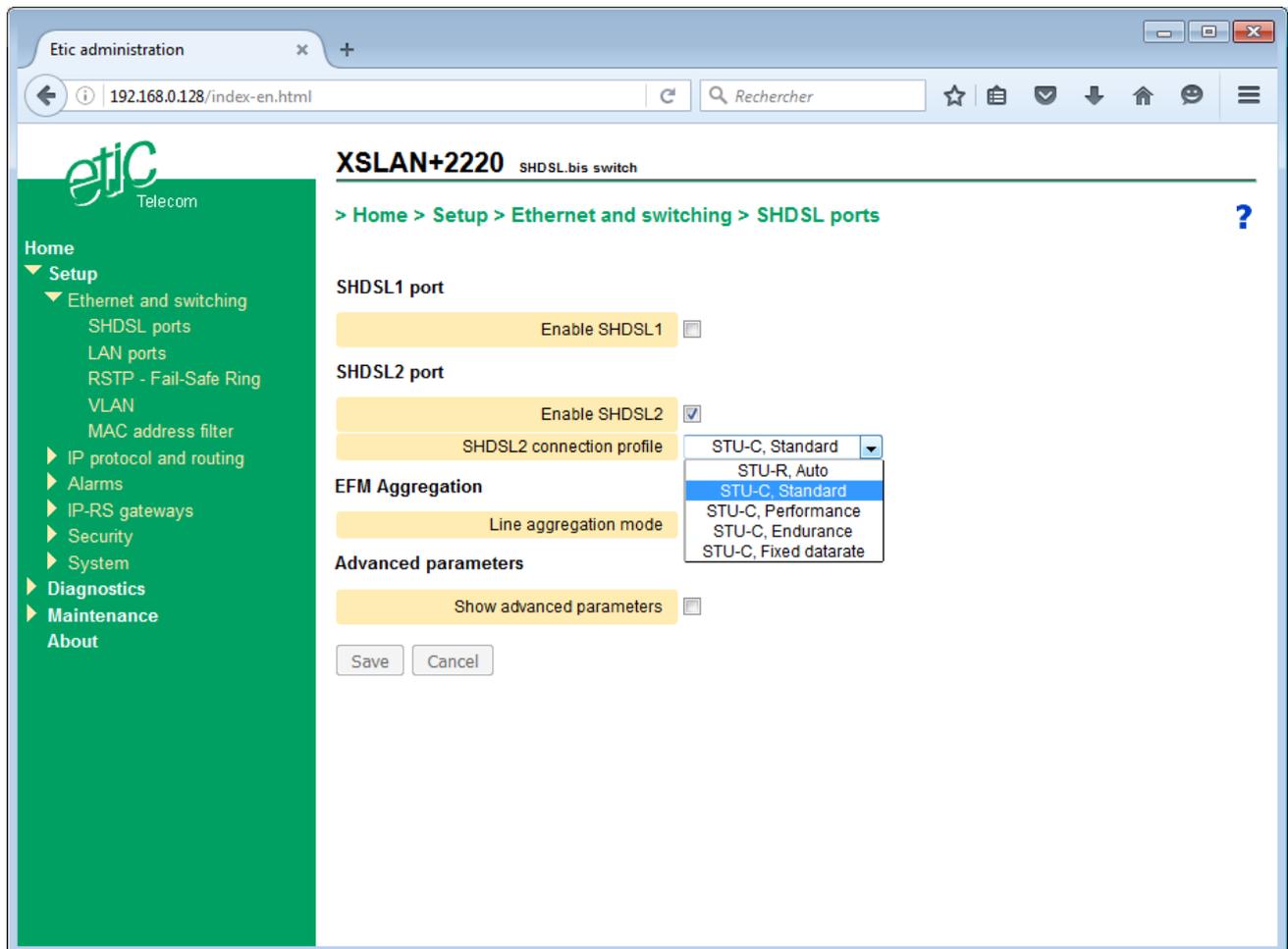
Setting up the first XS :

- In the menu, choose **Setup > Ethernet & switching > SHDSL ports**.
- Tick the **Enable SHDSL1** (or 2 or 3 or 4 depending on the case) checkbox.
- Assign the **STU-R, Auto** profile.
- Click **Save**.



Setting up the other XS :

- In the menu, choose **Setup > Ethernet & switching > SHDSL ports**.
- Tick the **Enable SHDSL1** (or 2 or 3 or 4 depending on the case) checkbox.
- Assign the **STU-C, Standard** or **STU-C Performance** or **STU-C Endurance** profile.
- Click **Save**.



SETUP

3.3 Step 2 : SHDSL test and set up adjustment

- Connect the XS to the twisted pairs. The wires of the same twisted pair can be reversed.
- Power on the XS.
- The connection takes about 45 s to establish with the « standard » profile and may takes a longer time with other profiles.
- The SHDSLx LEDs attached to each port displays the state of the connection as described in the table below.

State of the connection	SHDSL LED
The other XSLAN was not detected (for example when the line is not connected)	Blinking 0,1 s ON / 2 s OFF
Data rate negotiation	Blinking 0,3 s ON / 0,3 s OFF
Connected	Steady on
Traffic on the link	Flashing

- Once connected, choose **Diagnostics > Network status > Interfaces** in the menu to check the SHDSL link quality.

The screenshot shows the 'Etic administration' web interface for a switch. The breadcrumb trail is 'Home > Diagnostics > Network status > Interfaces'. The page title is 'XSLAN+2220 SHDSL.bis switch'. The left sidebar contains a menu with 'Home', 'Setup', 'Diagnostics', 'Log', 'Network status', 'Interfaces', 'RSTP status', 'Loop VPN', 'Routes', 'Statistics', 'Tools', 'Gateway status', 'Hardware', 'Advanced diagnostic', 'Maintenance', and 'About'. The main content area displays the 'SHDSL ports state' section, which includes a table with columns for Port name, SHDSL link state, Bitrate, Signal to noise ratio margin, Line attenuation, Last hour erroneous seconds, and Last 24 hours link losses. Below the table are buttons for 'Show', 'Reset SHDSL connections', and 'Refresh'.

Port name	SHDSL link state	Bitrate	Signal to noise ratio margin	Line attenuation	Last hour erroneous seconds	Last 24 hours link losses
SHDSL1	Connected	5696 kbits/sec	18 dB (4/4)	1 dB	0	0
SHDSL2	Connected	5696 kbits/sec	19 dB (4/4)	1 dB	0	0

- Check the quality of each SHDSL port.
The SNR ratio margin must be at least 2/4.
The number of erroneous seconds during the last hour must be close to 0.
The number of link losses during the last 24 hours must be 0 or a few ones.
- If the SNR ratio margin is only 1/4d e 1/4, with the **STU-C standard** profile, assign the **STU-C Endurance** profile and check again the connection.
- Once all the SHDSL connection run correctly, send periodically a PING from a PC to a remote XS or device to check that no error occurs.

Remark : one can use the PING tool included in the XS (**Diagnostics > Tools > PING**).

- If, despite these changes, the quality is insufficient, or if disconnections occur, or if the connection is not established, check the line :
Check that each conductor of the line is correctly connected.
Disconnect and by-pass the surge protectors to check if they are the cause of the dysfunction.
Check that the cable shield if any, is correctly connected to the ground.

SETUP

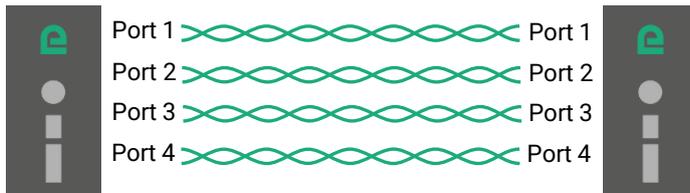
4 Setting up a link using 2, 3 or 4 twisted pairs

This chapter describes how to set up a multiplexed point to point connection.

A multiplexed connection is a link between two XS that uses two or three or four twisted pairs to multiply the total throughput. The overall data rate is approximately the sum of the rates obtained on each twisted pair.

An XS with two SHDSL ports can establish a multiplexed link with two pairs; the data rate is approximately doubled, up to 11 Mb/s or even 20 Mb/s up to 1 Km.

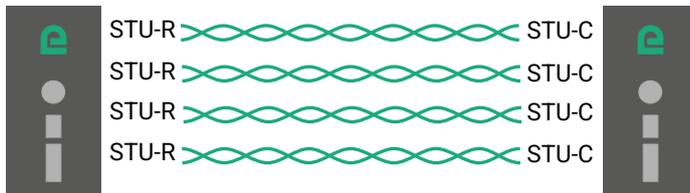
An XS with four SHDSL ports can establish a multiplexed link with up to four pairs; the data rate is approximately quadrupled, up to 22 Mb/s or even 40 Mb/s up to 1 Km.



Setting up :

The parameters are set in the same way as for Setting up a link using one twisted pair :

- Assign the **STU-R, Auto** profile to all SHDSL port of the first XS.
- Assign a connection profile to all SHDSL port of the other XS (**STU-C Standard** or **STU-C Endurance** or **STU-C Performance**).
- Aggregate the lines.



Line aggregation mode

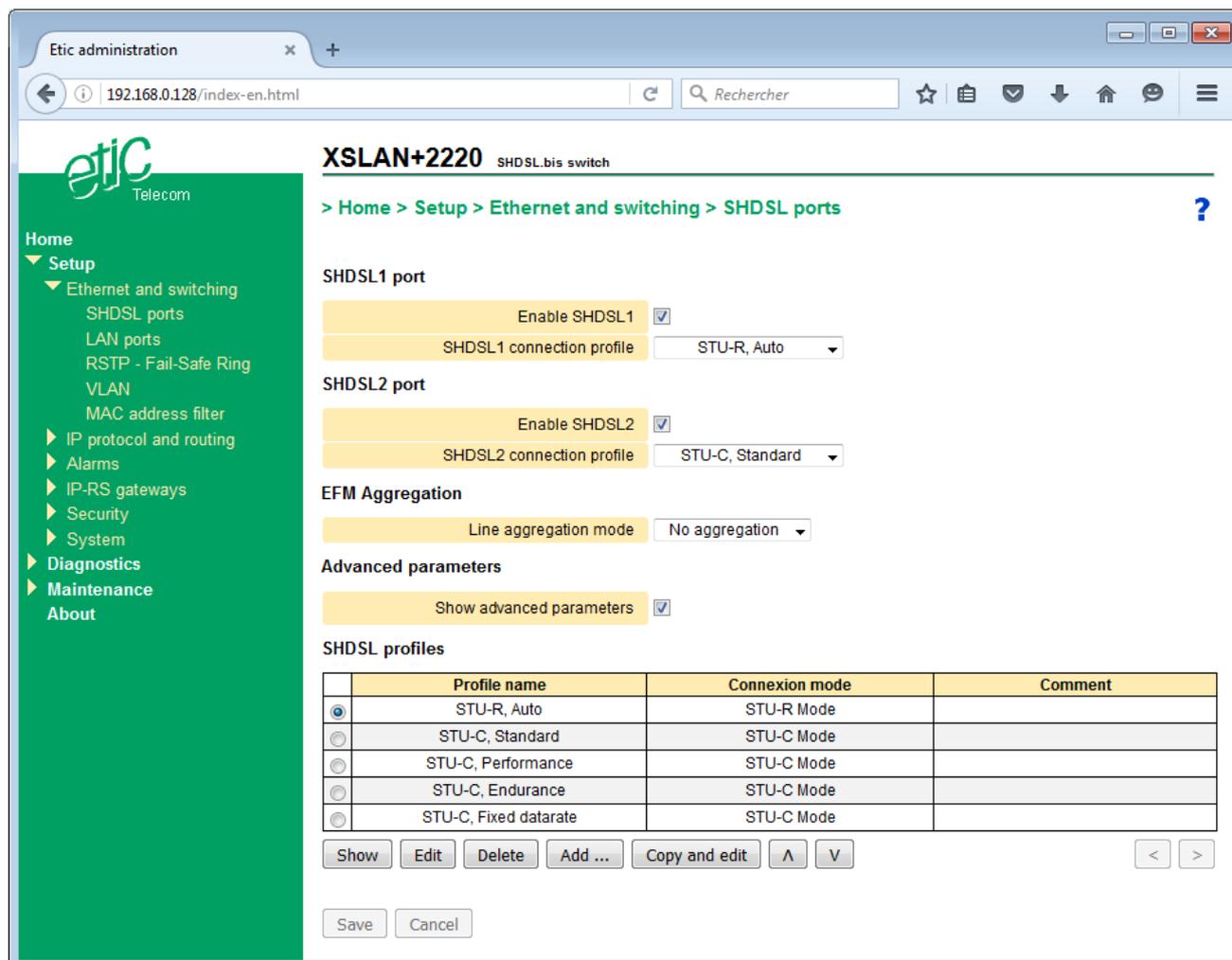
Possible values :
No aggregation
1 group of 2 lines (XS with 2 SHDSL ports)
2 groups of 2 lines (1-3) and (2-4) (XS with 4 SHDSL ports)
1 group of 4 lines (XS with 4 SHDSL ports)

5 Advanced setting up of an SHDSL link

In special cases, it may be useful to change any of the existing connection profiles, for example, to change the SNR ratio margin or to force the modulation. The modified profile is added to the five profiles.

To add a new connection profile,

- In the menu, choose **Setup > Ethernet & commutation > SHDSL ports**.
- Tick the **Show advanced parameters** checkbox.

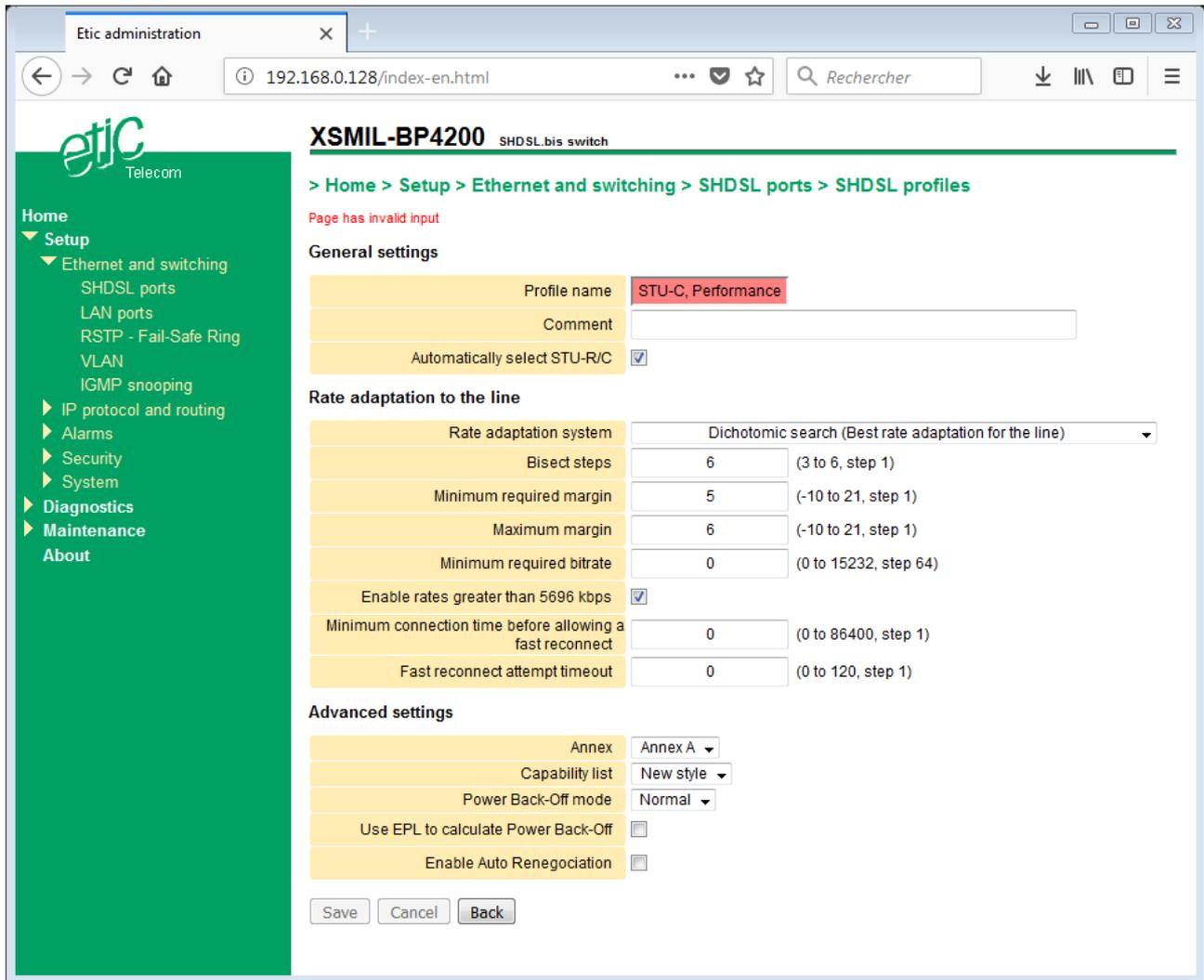


- Select one of the existing profiles,
- Click **Copy and edit**

The corresponding window is displayed ; it allows to tune the below parameters.

- Click **Save** ; the new profile is added in the profiles list and it can be selected.

SETUP



General settings:

Automatically select STU-R/C

If this checkbox is checked, the XS alternately tries to connect in STU-C and STU-R mode. Thus the connection can be established regardless the mode selected on the remote switch.

Connection mode

Possible values :
STU-C : The XS initiates the connection and negotiates the conditions.
STU-R : The wait for a connection.

Rate adaptation to the line:

Rate adaptation system

Possible values :
Line probing (Quick, adaptation is approximate)
Dichotomic search (Best adaptation for the line, but longer connection time)
Fixed data rate (Fastest connection time, but no adaptation performed)

« Line probing » mode :

The line is probed briefly to estimate the attenuation. The connection is then established at the data rate that gives the targeted signal-to-noise ratio margin.

Minimum bit rate

Minimum rate value for this connection

Possible values : 192 to 5696 kb/s step 64 Kb/s

Maximum bit rate

Maximum rate value for this connection

Possible values : 192 to 5696 kb/s step 64 Kb/s

Used margins

The SNR ratio margin may be determined either according to current conditions (CC) or according to predefined conditions considered the worst (WC)

Possible values : CC margins, WC margins, CC and WC margins, No margin

Default value : CC margins

CC SNR margin

This is the desired margin above the minimum operating threshold.

When the switch establishes the connection, it measures the signal to noise ratio and subtracts the SNR ratio margin.

If the result is greater than the minimum required, the connection is established

Possible values : -10 to 21dB

Alternate CC SNR margin

Visible when the "rate adaptation System" is set to "Line probing".

If the connection cannot be established with the specified SNR ratio margin, then the switch attempts to connect with this alternative margin. The value must be higher than the previous, which will result in a connection at a lower data rate.

Possible values : -10 to 21dB

« *Dichotomic search* » :

The XS successively performs several connections at different rates until the connection satisfies the requested criteria of bit rate and signal-to-noise ratio margin.

Bisect steps

The higher the number, the more accurate the result, but the connection setup time will be longer.

Possible values : 3 to 6

Minimum required margin

This is the minimum signal-to-noise ratio acceptable for this connection.

Possible values : -10 to 21 dB

Maximum margin

This is the maximum signal-to-noise ratio acceptable for this connection. The larger the margin range between minimum and maximum, the faster the connection setup time, but with a less accurate result.

Possible values : -10 to 21 dB

Minimum required bitrate

By defining a minimum bit rate, the connection is forbidden at a rate that is too low. This is useful in a redundant link topology where it is better to use the backup link rather than the master link when the line conditions have become bad.

Possible values : 0 to 15232 kb/s step 64 kb/s (0 means unused)

Enable rates greater than 5696 kbps

Leave this box unchecked if you know that the distance of the line does not allow a connection at higher data rates. Thus the range of tested rates will be narrower and the result will be more accurate or the connection setup time faster.

Minimum connection time before allowing a fast reconnect

SETUP

If the connection has been stable for some time and if a disconnection occurs for example because of a brief disturbance, it is likely that the conditions of the line have not changed. The XS can attempt the direct reconnection at the same rate as before which can significantly reduce the duration of unavailability of the link.

Possible values : 0 to 86400 s (0 means unused)

Fast reconnect attempt timeout

When a disconnection occurs and the XS again detects the equipment at the other end before this Timeout then it can attempt the direct reconnection at the same rate as before which significantly reduces the link downtime.

Possible values : 0 to 120 s (0 means unused)

Advanced settings :

Annex

Possible values : Annex A or Annex B

Default value : Annex A

PAM constellation

The PAM constellation defines the modulation used.

Possible values : Auto, PAM16, PAM32

Default value : Auto

Capacity list

The capacity list exchanged between the switches can be performed in an old way to interoperate with legacy switches generation (XSLAN- family).

Possible values : Auto, Old style, new style

Default value : Auto

Power-back off mode

Reduces the transmitting power when the lines are short to least disturb the surrounding lines (crosstalk).

Possible values : Normal, Forced

Default value : Normal

Use EPL to calculate Power back-off

TBD

Enable extended rates

Check this checkbox to activate the extended data rate for transmitting up to 15 Mb/s when the line is less than 1 Km.

Extended constellation

The PAM constellation defines the modulation used.

Possible values : Auto, PAM 4, PAM8, PAM16, PAM32, PAM64, PAM128

Default value : Auto

Enable Auto Renegociation

The SHDSL connection is established based on the line conditions at the connection time. For example, a noise can exist on the cable at this time and disappear thereafter. By default, the XS does not renegotiate its connection again, the SNR ratio margin will be higher than expected. If checked the switch renegotiate its link which can be established at a higher data rate.

Minimum SNR margin for renegociation (dB)

Renegotiation causes a disconnection and therefore a loss of service, during the time of recovery. This is why the renegotiation should be attempted only if the margin increased very significantly, enabling a significant increase in throughput.

Minimum duration before renegotiation (hours)

Renegotiation causes a disconnection and therefore a loss of service, during the time of recovery This is why the renegotiation should be attempted only if the margin increased very significantly, enabling a significant increase in throughput.

6.1 Overview

RSTP, standing for "Rapid Spanning Tree Protocol" is specified by the IEEE in the 802.1D-2004 document.

Loops in Ethernet networks are highly unwelcome, as they can cause broadcast storms, eating up all the available bandwidth and causing network outage. But sometimes they are necessary, in order to have backup paths in case a device or a link fails.

The goal of RSTP is to eliminate loops dynamically by calculating a spanning tree of the network. This spanning tree becomes the topology of the network and is created by disabling some ports.

The algorithm work by exchanging periodically small Ethernet frames : BPDUs (Bridge Protocol Data Unit). These frames contain information that allow the network to choose a root bridge, which is the root of the spanning tree. BPDUs originating from the root bridge are forwarded from bridge to bridge, to ensure propagation of the information in the network.

When a bridge receives BPDUs from root from 2 of its ports, meaning there is a loop in the network, it will only forward the best one, and block the port where the others were received.

When a link fails, BPDU are not received anymore by the bridge, and it will enable previously blocked ports in response.

RSTP supersedes the old STP for loop and redundancy management.

RSTP is retro-compatible with STP, but has extensions for faster recovery times :

- Ports can be put in "Edge" mode, meaning they will never be blocked.
- Ports can be put in "Peer to Peer" mode, meaning they transition quickly from "Blocked" to "Forwarding" when necessary.

This protocol can be used with devices from other manufacturers because it is interoperable.

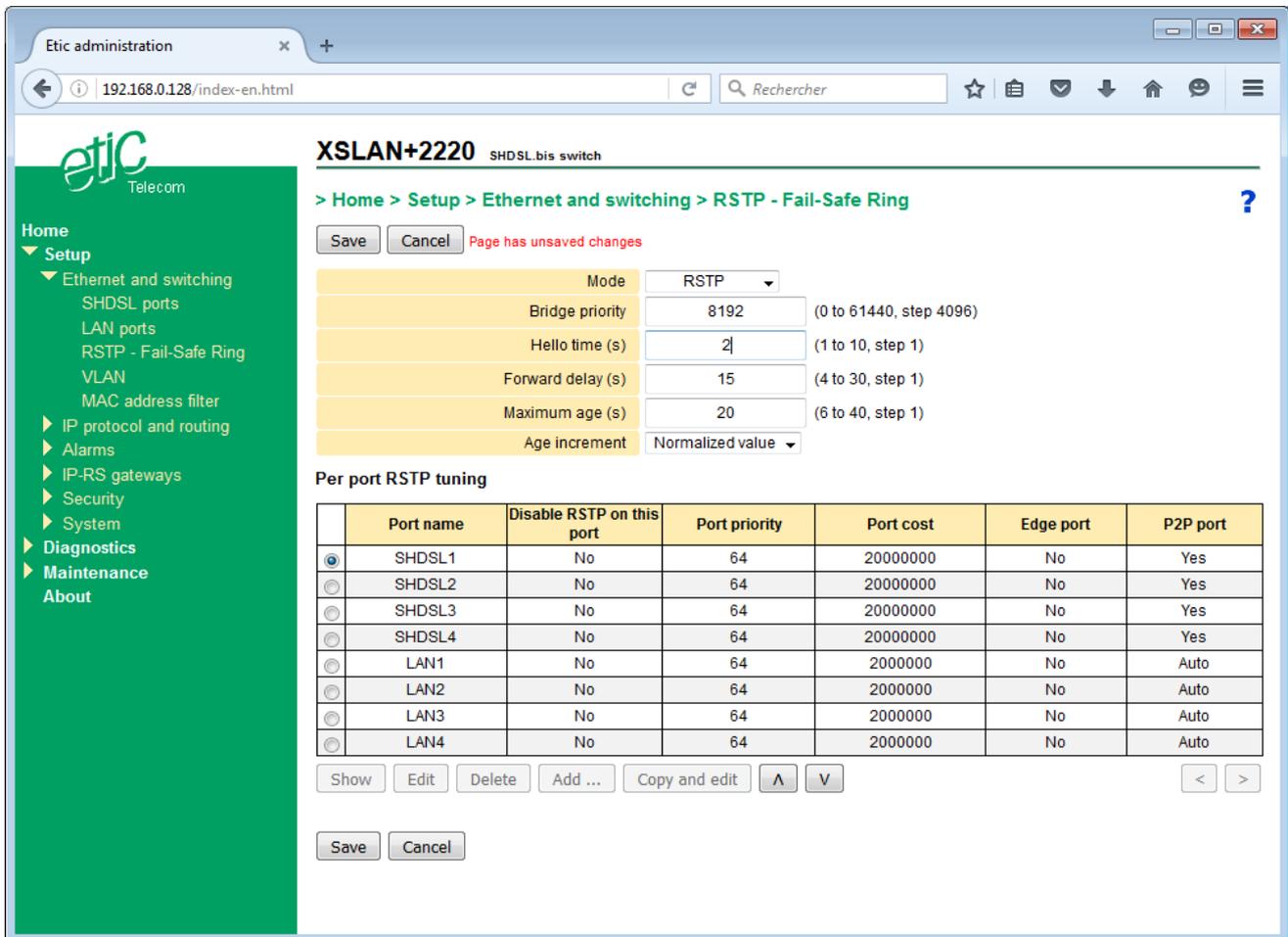
On the SHDSL side of the product, convergence is achieved in around 10 seconds.

Ports classification :

An Edge port is a port on the network edge; it connects an RSTP switch to equipments not acting as a bridge; for example, an Ethernet port that connects the XS to a PC or a PLC is an Edge Port

6.2 Set up

- In the menu, choose **Setup > Ethernet & switching > RSTP – Fail safe ring**.
- Select the **RTSP** mode.



The page is divided in two parts :

- The general parameters.
- The Ethernet & SHDSL ports parameters.

General parameters :

Bridge priority

This value is prepended to the MAC address of the bridge to form the bridge ID.

This is used by the network to choose which bridge will become the root of the spanning tree. The root is the bridge with the lowest bridge ID

Hello time

The "Hello time" is the delay between 2 consecutive BPDU sent by a bridge

It must be the same for all bridges in the network.

SETUP

Forward delay

When a port changes state following a topology change, it goes through 3 states :

- Blocked : All ingress traffic is discarded but BPDU frames (necessary for STP function)
- Listening/Learning : The port listens to the traffic but does not forward data. This is used to detect transient loops that can be created during the convergence.
- Forwarding : The port forwards data.

The forward delay is the duration of the Listening/Learning state.

Remark : Ports configured as Edge ports or P2P ports ignore this setting and skip the listening step altogether because it becomes unnecessary and increases the convergence time.

Maximum age

When the STP root transmits a BPDU, the information contained in it is forwarded from bridge to bridge. At each retransmission, a bridge adds 1 to a counter in the data. When this counter exceeds the "Max Age" value, the BPDU is not forwarded.

Note 1 : This acts like the TTL in IP packets.

Note 2 : This value must be large enough for the network. Each device must be able to receive the BPDUs from the root, even if it is located a lot of devices away. For example, for a ring with 20 devices, you must have "Max Age" greater than 20. Otherwise strange problems like erratic behavior, very long convergence time, or no convergence at all will occur.

Age increment

Increment value of age counter when going through the bridge.

Per port RSTP tuning parameters :

- Select the port to configure in the table

Port name

Select one of ports of the product (Ethernet 1 to 4 or SHDSL 1 or 2).

Disable RSTP on this port

Check this box when the port does not participate in RSTP.

Port priority

When "Port cost" is identical for two paths to the root bridge, the port priority can be used to break a tie between two ports. The less the number, the higher the priority.

Port cost

The port cost reflects the data rate of the link. It is used in the calculation of the active topology to prioritize a high data rate link versus a low data rate link. A high data rate link usually has a low cost.

Recommended values :

SHDSL port :	200 000 000
Ethernet 100 Mb/s port :	200 000

Edge port

An Edge port is a port located on the border of the network, with no bridge attached to it like, for instance, an industrial device or a PC.

BPDU are not transmitted to that kind of port; moreover, that kind of port cannot be blocked.

P2P port

Select "YES" if the port is participating in a direct link between 2 RSTP enabled switches (no unmanaged switch must be inserted on that link).

This information enables the RSTP switch to converge faster by skipping the "Learning" step, and jumping directly from "Blocked" to "Forwarding".

Moreover, a link loss is guaranteed to be detected and acted upon very quickly by both ends.

SHDSL ports must be P2P ports.

7 Fail-safe ring

Based on the STP algorithm, that proprietary redundancy solution makes possible to handle a ring structure up to 16 SHDSL switches.

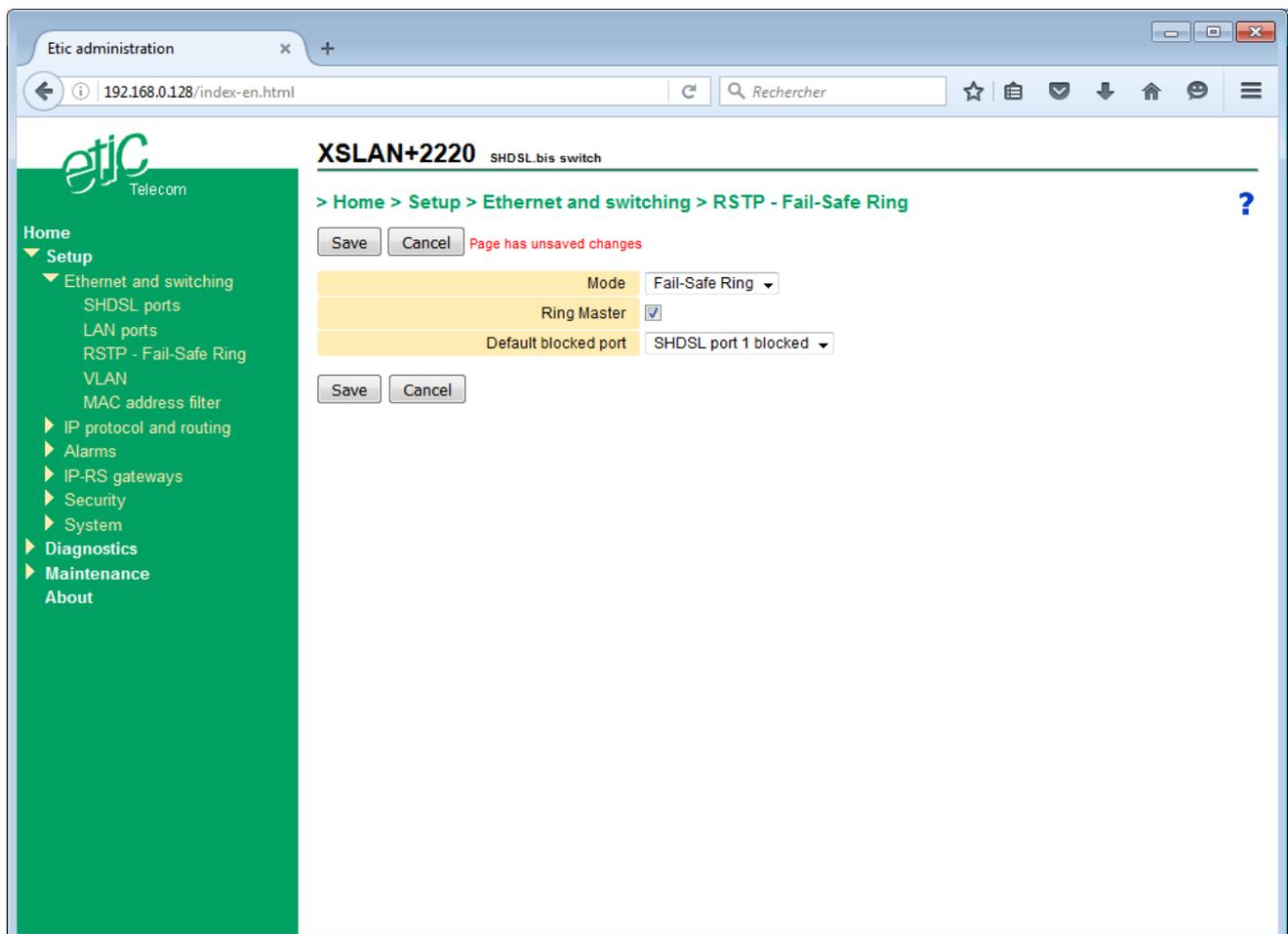
One of the switches has to be selected as the ring master ; it has a particular function : The Ring Master will block one of its ports, preventing the formation of an Ethernet loop, and leave the other in forwarding mode. When a device or a link fails in the SHDSL ring, the second port will be enabled, allowing to reach all the devices in the ring.

Remark : In this mode, LAN ports do not participate in the algorithm, only the SHDSL ports are used.

The advantages of that solution is that the failure detection delay and the recovery delay is only a few seconds (One second if the ring counts 5 SHDSL switches); moreover, it is very simple to configure.

Ring master configuration

- In the menu, choose **Setup > Ethernet & switching > RSTP – Fail-safe ring**.



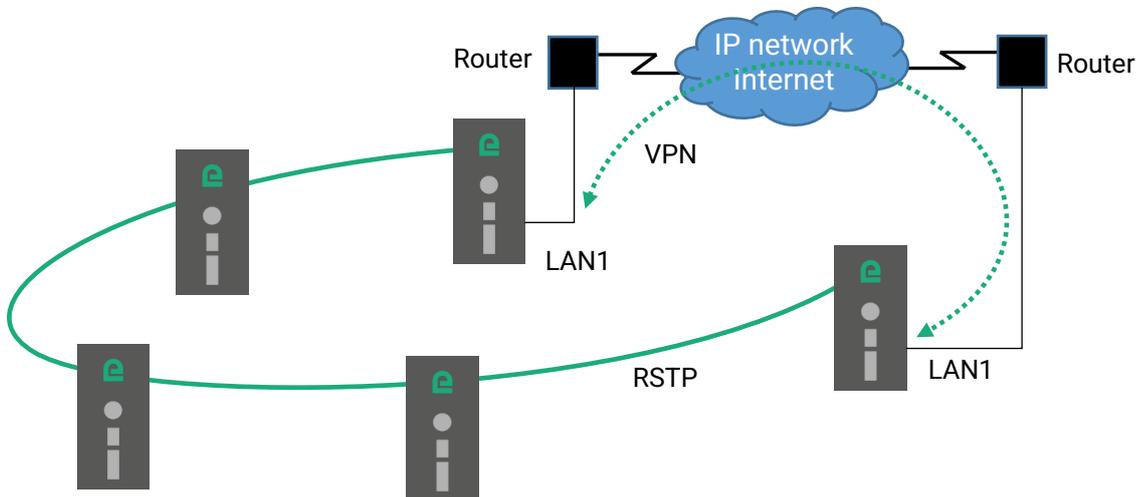
- Select the **Fail-safe ring** mode.
- Tick the **Ring master** checkbox.
- Select the default blocked port.
- Click **Save**.

Other switches configuration

- In the menu, choose **Setup > Ethernet & switching > RSTP – Fail-safe ring**.
- Select the **Fail-safe ring** mode.
- Leave the **Ring master** box unchecked.
- Click **Save**.

8 Loop VPN

When the SHDSL network forms a daisy chain (i.e. a linear topology), and when it is not possible to form a secure ring, the "loop VPN" function allows for network redundancy if a public WAN connection (Internet) or private (MPLS) is available at each end of the SHDSL network.



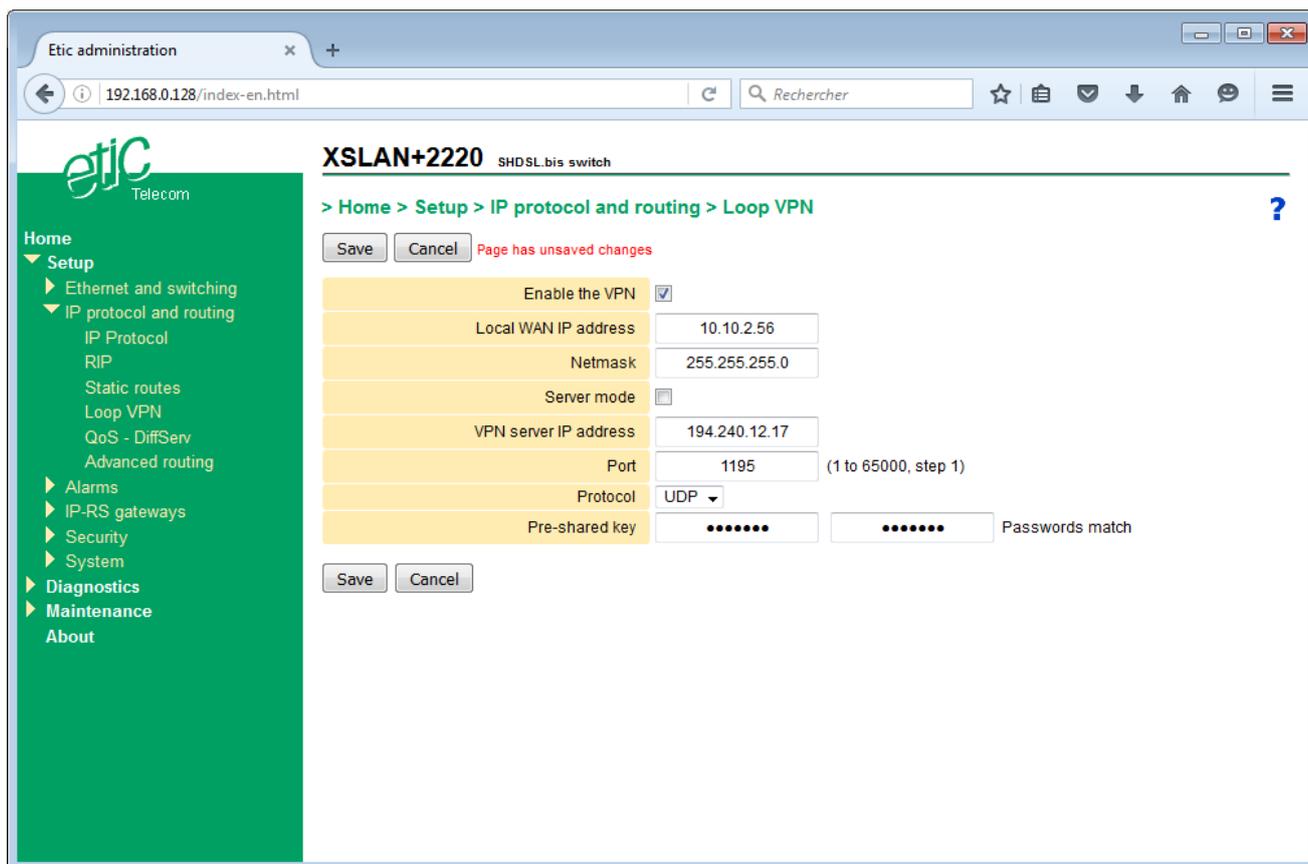
The 2 XS switches at the end of the network establish a VPN over the WAN. The VPN provides connectivity at the Ethernet level. Thus by activating the RSTP protocol redundancy may be provided thanks to that VPN.

One XS must be configured as a VPN server mode and must be accessible via a fixed IP address across the WAN. The other XS must be configured as a VPN client.

The VPN is established on the Ethernet LAN1 port of the XS switch and that port becomes a "WAN" port with its own IP address. This Ethernet port must be connected to the WAN access router and therefore cannot be used to connect other equipments which are reachable through the SHDSL link.

Setting up the VPN

- In the menu, choose **Setup > IP Protocol and routing > Loop VPN**.
- Tick the **Enable the VPN** checkbox.



Local WAN IP address

This is the IP address assigned to the LAN1 port of the XS in the IP subnet of the WAN access router. This subnet is different from the one on the other LAN ports.

Netmask

Netmask of the WAN router subnet.

Server mode

Check this box on the switch used as a VPN server. Leave the box unchecked on the one used as a VPN client.

VPN server IP address

When the XS is the VPN client, the IP address to reach the VPN server switch must be defined. This IP address is not necessarily the one assigned to the VPN server XS in the "Local WAN IP Address" parameter if the VPN goes through routers with Network Address Translation (NAT).

Port

TCP or UDP port number of the VPN.

Protocol

TCP or UDP protocol of the VPN.

Pre-shared key

The Pre-shared key is a secret character string that is used for encryption and VPN traffic authentication. It must be the same in the 2 XS that perform the VPN.

9.1 Overview

VLAN function

The VLAN technology conform to the IEEE 802.1Q norm makes possible to transmit up to 4096 Ethernet networks over the same physical Ethernet layer.

The devices belonging to the same Ethernet VLAN can exchange Ethernet frames with one another but cannot exchange frames with devices belonging to another VLAN except if a level 3 switch or an equivalent device makes possible to bridge that VLANs.

Ethernet ports

When we speak of an Ethernet port of an XS, we speak not only of 10/100 BT Ethernet ports, but also of the SHDSL ports.

All SHDSL ports are supposed to be a unique SHDSL port.

Principles of operations

A particular field of each Ethernet frame stores the VLAN identity (VID) to which the frame belongs. When that field stores the VLAN ID, one says the frame is tagged.

How are Ethernet frames tagged and untagged ?

An Ethernet frame can be tagged by the device which produces it.

Otherwise, the Ethernet frame is tagged by the switch to which the device is connected.

Reciprocally, the VLAN ID of an Ethernet frame can be removed by the Ethernet switch before being transmitted to the Ethernet device or can be transmitted tagged to the device.

The switch filters the Ethernet frames according to their VLAN ID

When they come into the switch on an Ethernet port, Ethernet frames are tagged with the VLAN ID assigned to that Ethernet port.

When it is received by the switch, a tagged Ethernet frame can only come out to an Ethernet port, if the VLAN ID assigned to that port is the same as the VLAN ID of the Ethernet frame.

Html administration server and the serial gateway

If the VLAN function is enabled, Ethernet frames produced by the html administration server and the serial gateway are tagged with a particular VLAN.

If the html administration server and the serial gateway do not belong to the same VLAN, a separate IP address must be assigned to the serial gateway

Setting up the VLAN function

The VLAN set up is divided in two parts : The Egress policy set up and the Ingress policy set up.

- **The Egress policy** consists in registering the authorized VLAN IDs and defining which Ethernet ports belong to each VLAN.
- **The Ingress policy** consists in defining which process must be applied to each Ethernet frames going into the switch : Tagging the frame with a VLAN ID or leaving the frames untagged etc ...

9.2 Set up

Warning:
 Before saving the VLAN configuration, make sure you will be able to access to the administration html server through an Ethernet port or remotely through the line.
 One Ethernet port at least belongs to the same VLAN as the administration html server of the XS.

- In the menu, choose **Setup > Ethernet & Switching > VLAN**.
- Tick the **Enable VLAN management** box.

Enable VLAN management

Administration VLAN ID: (0 to 4095, step 1)

Serial gateways VLAN ID: (0 to 4095, step 1)

VLANs : Egress policy

This table defines the egress policy of the LAN ports when VLAN management is enabled.

	VLAN name	VLAN ID	LAN1 Egress policy	LAN2 Egress policy	LAN3 Egress policy	LAN4 Egress policy	SHDSL Egress policy
<input checked="" type="radio"/>	VLAN4	4	Frames exit the port tagged	Port does not belong to this VLAN	Port does not belong to this VLAN	Port does not belong to this VLAN	Frames exit the port tagged
<input type="radio"/>	VLAN5	5	Frames exit the port tagged	Port does not belong to this VLAN	Port does not belong to this VLAN	Port does not belong to this VLAN	Frames exit the port tagged
<input type="radio"/>	VLAN12	12	Port does not belong to this VLAN	Frames exit the port untagged	Port does not belong to this VLAN	Port does not belong to this VLAN	Frames exit the port tagged

Buttons: Show, Edit, Delete, Add ..., Copy and edit, [Up], [Down], [Left], [Right]

VLANs : Ingress policy

These parameters define the ingress policy of the LAN ports when VLAN management is enabled.

LAN1 ingress policy: Refuse a frame not belonging to a VLAN associated to the port

LAN1 VLAN ID: (0 to 4095, step 1)

LAN2 ingress policy: Refuse a frame not belonging to a VLAN associated to the port

LAN2 VLAN ID: (0 to 4095, step 1)

LAN3 ingress policy: Refuse a frame not belonging to a VLAN associated to the port

LAN3 VLAN ID: (0 to 4095, step 1)

LAN4 ingress policy: Refuse a frame not belonging to a VLAN associated to the port

LAN4 VLAN ID: (0 to 4095, step 1)

SHDSL ingress policy: Refuse a frame not belonging to a configured VLAN

SHDSL VLAN ID: (0 to 4095, step 1)

Buttons: Save, Cancel

The page allows you to set the output policy, the input policy and the VLAN ID of the administration server and the serial gateways.

SETUP

9.2.1 Egress policy

That part of the page is made to register the VLAN IDs and to specify which process must be applied to exiting tagged frames with that VLAN ID.

The processes which can be applied to an outgoing frame are :

- Frames exit that port untagged.
- Frames exit that port tagged.
- Frames exit that port unmodified
- Port does not belong to that VLAN

Example :

Three VLANs are defined : 4, 5, 12.

The LAN1 port is registered on VLAN 4 and 5. The frames that belongs to the VLAN exits the switch on the LAN1 port tagged.

The LAN2 port is registered on VLAN 12. The frames that belongs to the VLAN exits the switch on the LAN2 port untagged.

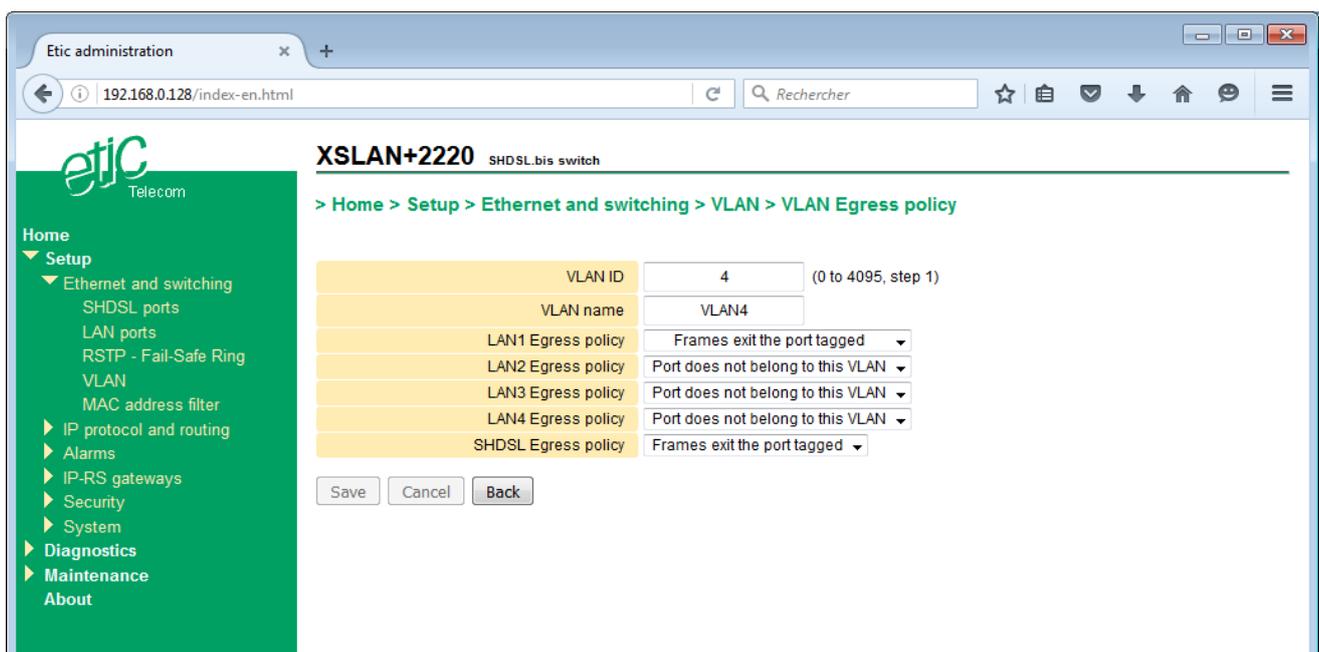
Lan3 and LAN4 ports don't belong to any VLAN (not used).

The SHDSL ports are registered to all VLANs. All frames are transmitted on the SHDSL network tagged.

Egress policy	LAN1	LAN2	LAN3	LAN4	SHDSL
VLAN 4	Yes – tagged	No	No	No	Yes – tagged
VLAN 5	Yes – tagged	No	No	No	Yes – tagged
VLAN 12	No	Yes – untagged	No	No	Yes – tagged

To set up the Egress policy,

- In the menu, choose **Setup > Ethernet & Switching > VLAN**.
- Click **Add**.
- Enter a VLAN ID and assign a name to that network.
- For each Ethernet port, define if the port belongs to that VLAN and if the frame exits the port tagged or not.



VLAN ID

Enter the VLAN ID.

VLAN name

Enter a name for this VLAN.

LAN1 Egress policy (or LAN2, or LAN3, or LAN4)**Frames exit the port tagged**

Ethernet frames belonging to this VLAN can exit on LAN1 port (or 2 or 3 or 4).
Frames exit the port tagged.

Frames exit the port untagged

Ethernet frames belonging to this VLAN can exit on LAN1 port (or 2 or 3 or 4).
Frames exit the port untagged.

Frames exit the port unmodified

Ethernet frames belonging to this VLAN can exit on LAN1 port (or 2 or 3 or 4).
Frames exit the port unmodified (tagged or untagged).

Port does not belong to this VLAN

Ethernet frames belonging to this VLAN can not exit on LAN1 port (or 2 or 3 or 4).

SHDSL Egress policy**Frames exit the port tagged**

Ethernet frames belonging to this VLAN can exit on SHDSL ports.
Frames exit the port tagged.

Note : SHDSL ports should belong to all VLAN so that Ethernet frames coming from all the devices locally connected to the XS be transmitted to the SHDSL line.

SETUP

9.2.2 Ingress policy

That part of the page is made to register which process must be applied to the Ethernet frames when they enter a given port of the switch or when they are received from the line.

One defines

- which already tagged frames can enter the switch;
- which VLAN ID will be assigned to untagged frames coming into the switch.

Example :

Let us go on with the example given at the previous paragraph; we have defined the Egress policy :

Egress policy	LAN1	LAN2	LAN3	LAN4	SHDSL
VLAN 4	Yes – tagged	No	No	No	Yes – tagged
VLAN 5	Yes – tagged	No	No	No	Yes – tagged
VLAN 12	No	Yes –untagged	No	No	Yes – tagged

The table hereafter, defines the ingress policy :

	LAN1	LAN2	LAN3	LAN4	SHDSL
VLAN ID	4	12	0	0	12
Accept all frames					
Refuse a frame not belonging to a configured VLAN					X
Refuse a frame not belonging to a VLAN associated to the port	X	X	X	X	

LAN1

Only frames tagged with ID 4 or 5 can enter through this port.

Untagged frames are assigned to VLAN 4 and can enter through this port.

LAN2

Only frames tagged with VLAN ID 12 can enter through this port.

Untagged frames are assigned to VLAN 12 and can enter through this port.

LAN3 et LAN4

Frames cannot enter through these ports.

SHDSL

Only frames tagged with ID 4 or 5 or 12 can enter through these ports.

Untagged frames are assigned to VLAN 12 and can enter through this port.

To set up the Ingress policy,

- In the menu, choose **Setup > Ethernet & Switching > VLAN**
- For each Ethernet port and for the SHDSL ports, select the Ingress policy and the VLAN ID which must be applied to the untagged frames.

LAN1 ingress policy (or LAN2 or LAN3 or LAN4 or SHDSL)

Accept all frames

All frames entering the Ethernet ports are accepted whatever they are tagged or not.
 An untagged frame entering the Ethernet port will belong to the VLAN of this port.
 A tagged frame entering the Ethernet port will keep its VLAN ID.

Refuse a frame not belonging to a configured VLAN

An untagged frame entering the Ethernet port will belong to the VLAN of this port.
 Tagged frames entering the Ethernet port are only accepted if their VLAN ID is one of the previously configured VLAN (see Egress policy).
 Frames tagged with another VLAN ID are denied.

Refuse a frame not belonging to a VLAN associated to the port

An untagged frame entering the Ethernet port will belong to the VLAN of this port.
 Tagged frames entering the Ethernet port are only accepted if their VLAN ID is one of the registered VLAN or that port (see Egress policy).
 Frames tagged with another VLAN ID are denied.

LAN1 VLAN ID (or LAN2 or LAN3 or LAN4 or SHDSL)

This is the VLAN ID assigned to an untagged frame entering to this port.

9.3 Administration server and serial gateways

When VLAN management is enabled, the administration web server and the serial gateway must belong to a VLAN.

Administration VLAN ID

Enter the VLAN ID to which the administration server belongs.

Serial gateways VLAN ID

Enter the VLAN ID to which the serial gateways belong.

Remark :

If the serial gateway does not belong to the same VLAN as the html administration server, a particular IP address must be assigned to serial gateways.

- In the menu, choose **Setup > IP protocol and routing > IP protocol**.
- Tick the **Use a different address for the serial gateways** checkbox.
- Enter the IP and the netmask for the serial gateways

10 MACSec

10.1 Overview

Media Access Control security (MACsec) is defined by IEEE standard 802.1AE and provides point-to-point security on SHDSL links

MACsec operates at the medium access control layer and defines connectionless data confidentiality and integrity for media access independent protocols.

MACSec allows frames egressing an Ethernet interface to be enciphered and signed. Frames ingressing the Ethernet interface will be deciphered and authenticated.

The system has two parts :

- The datapath virtual interface, encrypts, decrypts, signs, verifies frames,
- The MACSec Key Agreement (MKA), responsible for installing keys in the virtual interface.

10.1.1 Virtual interface

The virtual interface uses a single 256bit key for authentication and encryption (the SAK).

The virtual interface uses the AES-256 in GCM mode.

The virtual interface uses a dedicated EtherType for MACSec frames (it processes ingress frames with this EtherType, and generates egress frames with the EtherType)

10.1.2 MKA

MKA generates, distributes and installs the SAK in the virtual interface.

It requires two variables :

- The CKN which identifies a group of devices that must establish a common SAK,
- The CAK which is a PSK

Its high level operation is as follows :

1. The participant with the lowest MAC address will be elected key server,
2. The key server randomly chooses an SAK, using a CSPRNG and various sources of entropy,
3. The key server encrypts the SAK with the CAK using AES-keywrap and signs it with the CAK,
4. The key server distributes the encrypted SAK to the other participants
5. The participants verify, decrypt and install the SAK in the virtual interface.

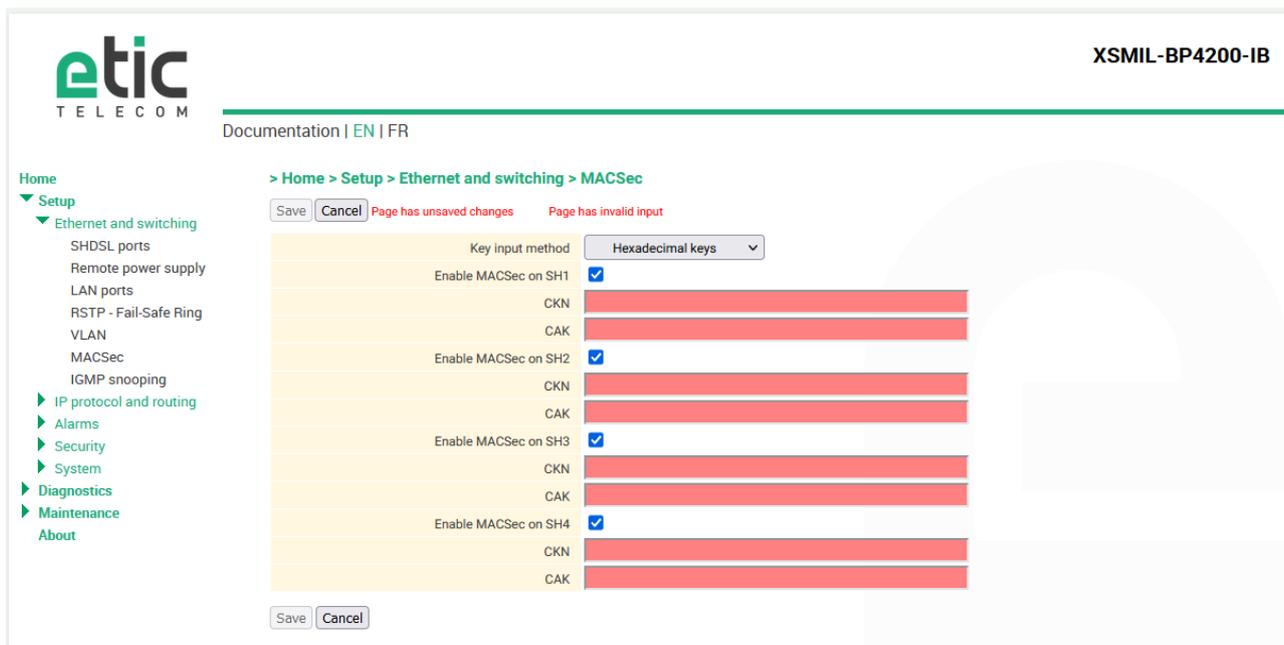
Each time a participant is added or removed, the process restarts.

MKA uses 802.1X PDUs to exchange data (MKPDUs).

The destination address of these is 01:80:C2:00:00:03. This address is link-local and is not forwarded by bridges. As a result older firmware versions of the XS do not forward these frames.

10.2 Setting up MACSec

- In the menu, choose **Setup > Ethernet and switching > MACSec**.
- Enable MACSec on the SHDSL ports
- Enter the CKN (32 hexadecimal characters) and the CAK (64 hexadecimal characters)



10.3 Password mode

A « Password mode » is added in the XS and is not part of the standard. Its operation is as follows :

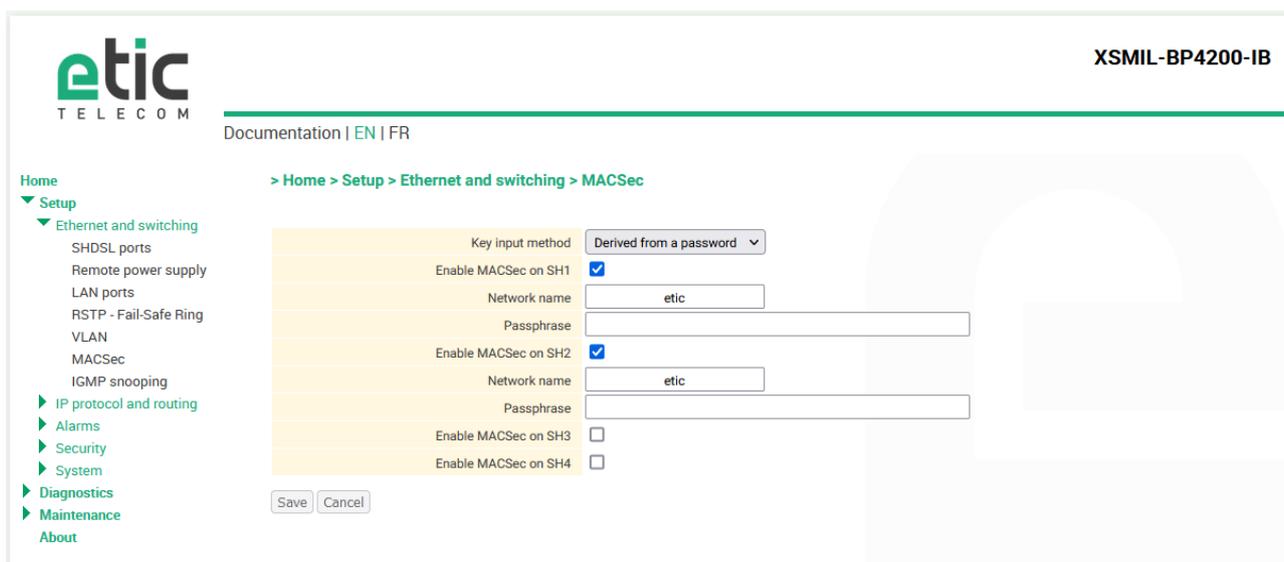
A network name and a password are input by the user.

The CKN is calculated as follows :

$$CKN = \text{sha256}(\text{network_name})$$

The CAK is calculated as follows :

$$CAK = \text{pbkdf2_sha512}(\text{password} = \text{password}, \text{salt} = \text{network_name}, \text{iterations} = 30000, \text{len} = 32\text{bytes})$$



SETUP

10.4 MACSec state

To verify the MACSec state :

- In the menu, choose **Diagnostics > Network status > Interfaces**.

MACSec status

SHDSL1 MACSec status	Frames are authenticated and enciphered
SHDSL2 MACSec status	Not secured
SHDSL3 MACSec status	Disabled
SHDSL4 MACSec status	Disabled

Refresh

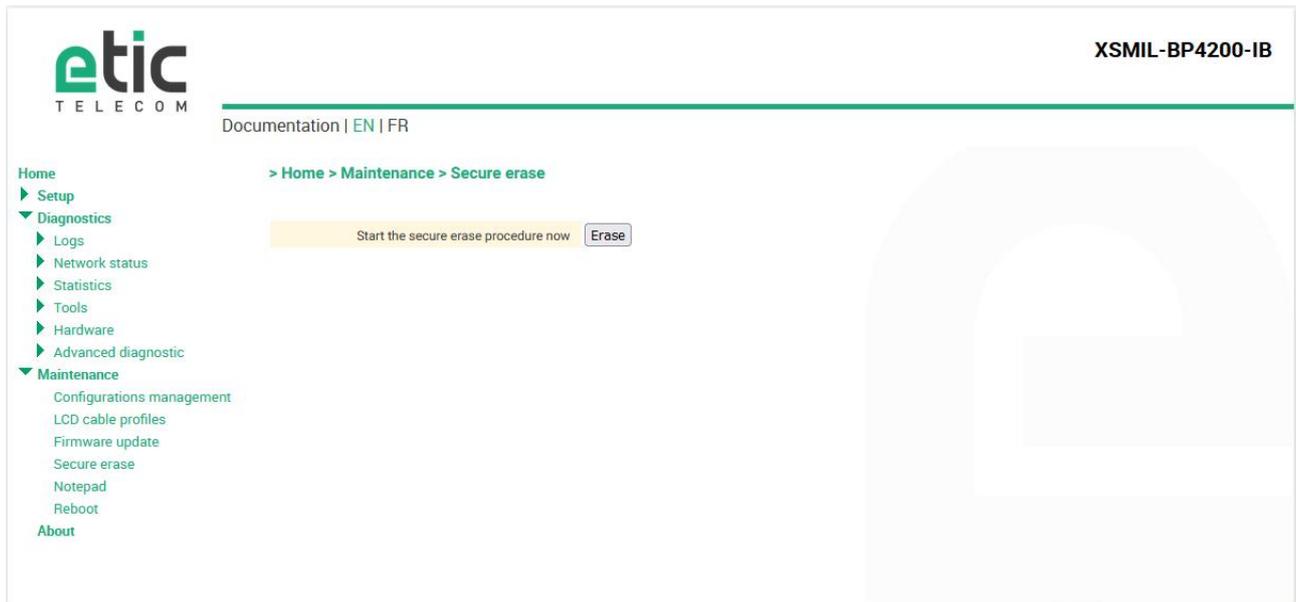
10.5 Key management and secure erase

The keys for MACSec are stored in a separate storage area, separated from the configuration. A new web page in Maintenance/Secure Erase allows to start a secure erase process.

This process erases the copies of the MACSec keys from the RAM, erases the separate storage area and cuts off the power of the CPU/RAM for a brief instant, causing loss of the contents of the DDR3-SDRAM.

To perform a Secure erase :

- In the menu, choose **Maintenance > Secure erase**.
- Click **Erase**.



10.6 MTU considerations

The MTU of the L2 interface with the management IP address and web server is now as follows:

1500 with MACSec disabled

1468 if MACSec is enabled

1464 if VLANs and MACSec are enabled.

This allows the web page to work in all cases, the TCP MSS is set correctly.

The MTU of an SHDSL link with MACSec is 1468 bytes, 32 bytes are taken by the MACSec header.

The MTU of an SHDSL link with MACSec and VLANs is 1464 bytes, 4 additional bytes are taken by the VLAN tag header.

11 IGMP snooping

11.1 Overview

By default, a switch floods all multicast frames to all its ports. In heavy traffic scenarios, this can cause saturation of the links, especially on slower SHDSL connections. To avoid this and take informed bridging decisions, a switch can inspect the IGMP traffic that peers doing multicast exchange.

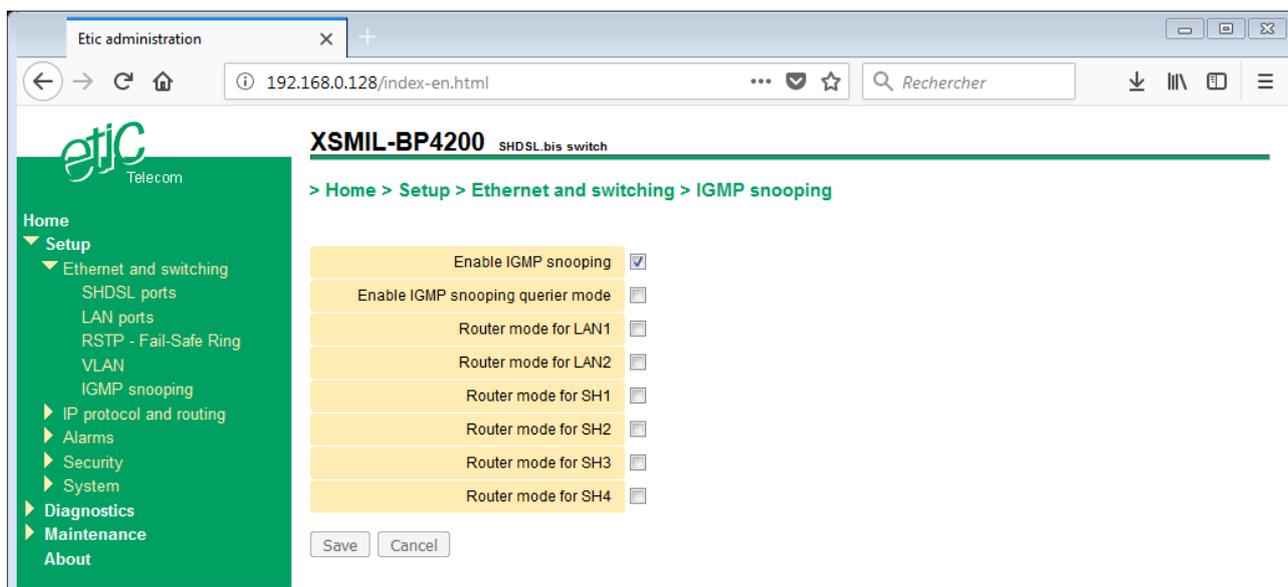
In a typical multicast enabled network, there is a multicast router. This device queries periodically using IGMP the other hosts to know which peers want to receive what multicast traffic.

The switch, when forwarding the frames, will check whether or not it should forward or block a given traffic on a given port.

When there is no multicast router to query the network, one of the IGMP snooping enabled switch can do the queries. The device with the lowest IP address is elected as the querier for the network.

11.2 Setting up the IGMP snooping function

- In the menu, choose **Setup > Ethernet and switching > IGMP snooping**.
- Tick the **Enable IGMP snooping** checkbox.



Enable IGMP snooping

Enable the filtering/forwarding of IP multicast packets based on IGMP traffic.

Enable IGMP snooping querier mode

Enable the XS to be elected querier if there is no router on the network.

Router mode for LAN1

Router mode for LAN2

Router mode for SH1

Router mode for SH2

Router mode for SH3

Router mode for SH4

Accept all multicast traffic from this port.

12 SNMP

12.1 Overview

The XS supports SNMP V2 and V3 protocols.

The XS supports the following MIBs :

- RFC1213-MIB (MIB-2)
- HDLSL2-SHDSL-LINE-MIB
- HOST-RESOURCES-MIB
- IF-MIB
- IP-MIB
- BRIDGE-MIB
- RSTP-MIB

See Annex for a detailed description.

The SNMP manager can acquire, in particular, the following informations :

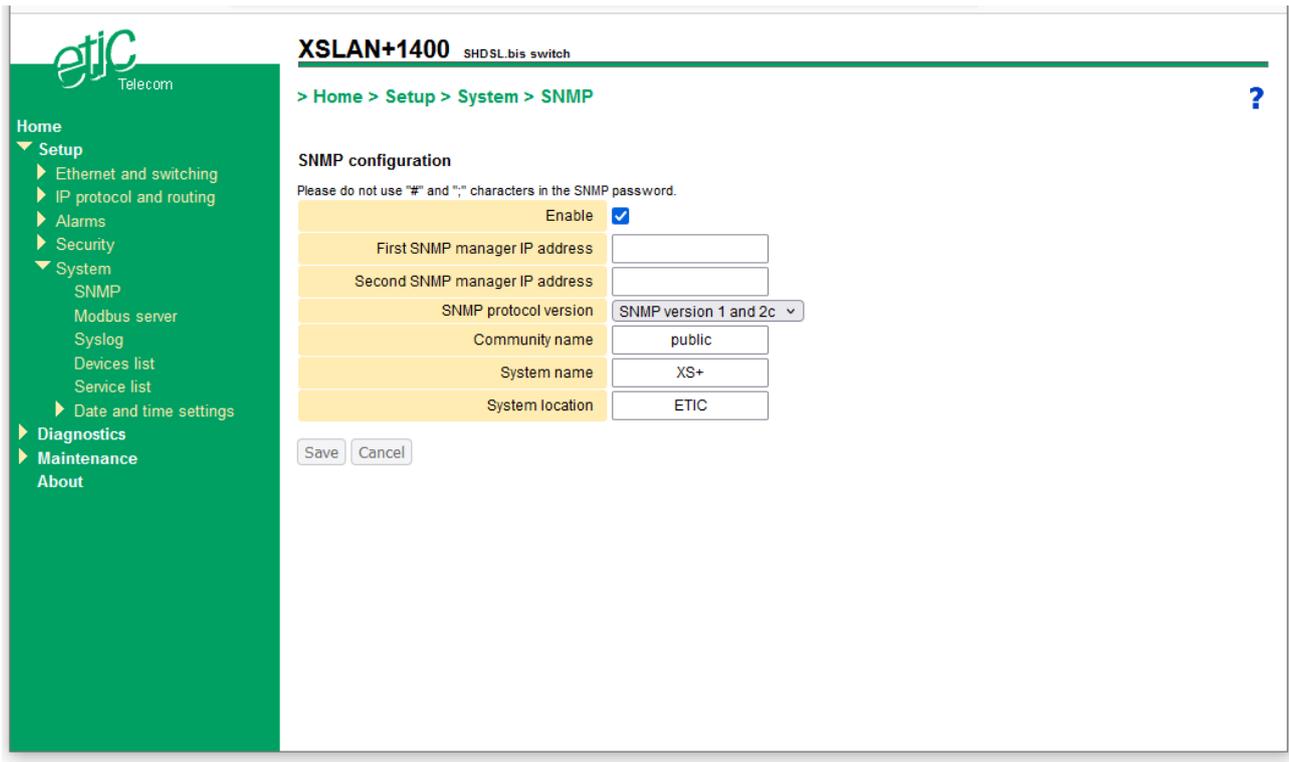
Ethernet 10/100 BT ports status : Up / down
SHDSL links status : connected or not
SHDSL links bit rate
SHDSL links SNR ratio margin
SHDSL links Number of erroneous seconds during the last quarter of hour
SHDSL links Number of erroneous seconds during the last 24 hours
RSTP ports status (blocked / learning / forwarding)
RSTP bridge parameters (bridge ID, priority, MAC, root)
MAC addresses data base

The XS is also able to send SNMP traps when the following events occur :

Ethernet 10/100 BT port connection
Ethernet 10/100 BT port disconnection
SHDSL connection established for each SHDSL port
SHDSL connection disconnected for each SHDSL port
Failsafe ring established
Failsafe ring failure
Product restart

12.2 Setting up the SNMP function

- In the menu, choose **Setup > System > SNMP**.
- Tick the **Enable** checkbox.



First SNMP manager IP address

Enter the IP address of the first SNMP manager where to send SNMP traps.

Second SNMP manager IP address

Enter the IP address of the second SNMP manager where to send SNMP traps.

Community name

Enter the name of the community to which the product belongs.

System name

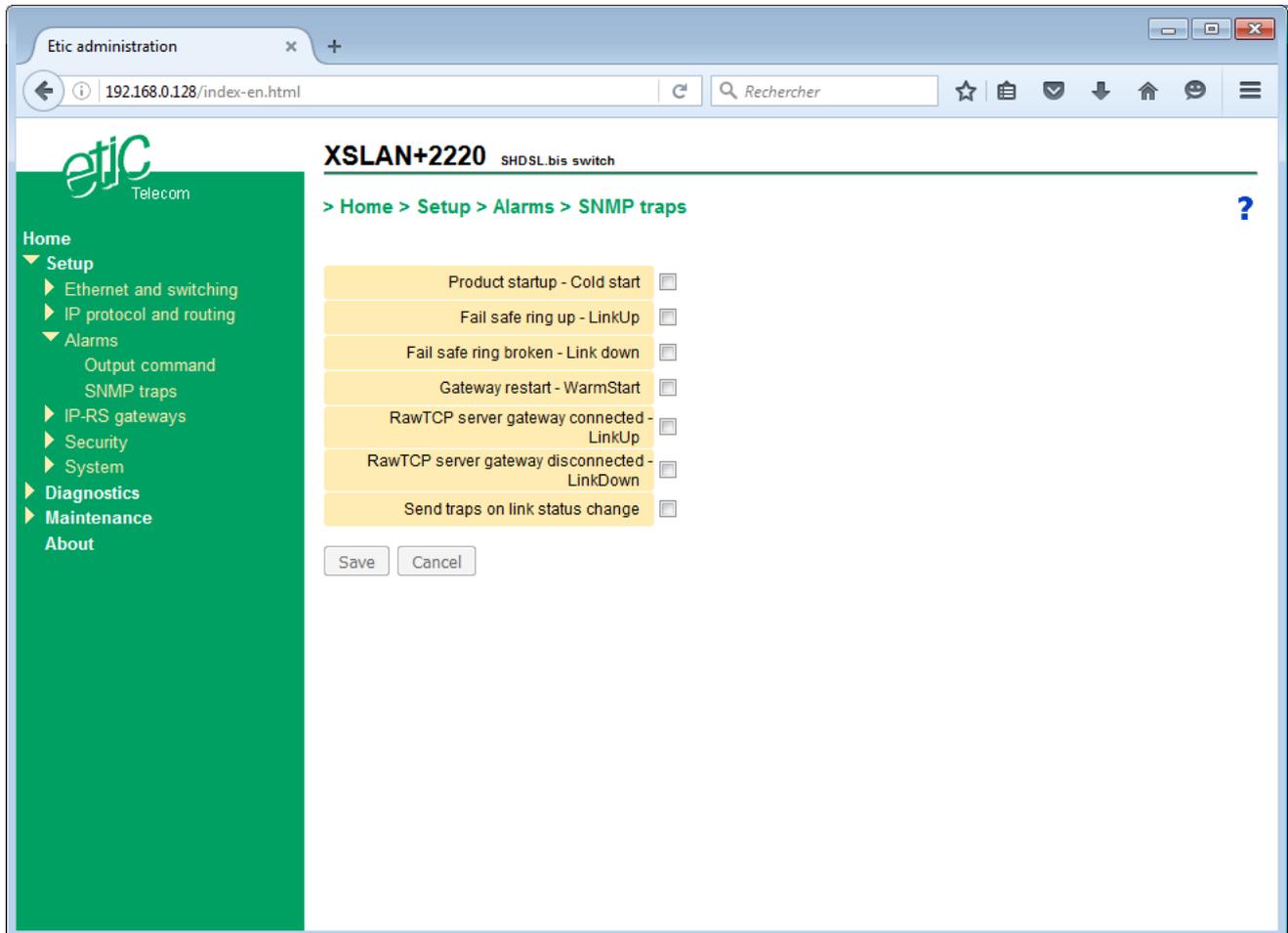
The system name is the name of the product. (XSLAN+2400 for example).

System location

Enter a string which identifies the location where the product is installed.

12.3 Setting up the SNMP traps

- In the menu, choose **Setup > Alarms > SNMP traps**.
- Select the traps which must be transmitted by the product.



Product startup – Cold start

Fail safe ring up – LinkUp

Fail safe ring broken – LinkDown

Gateway restarted – WarmStart

RawTCP server gateway connected – LinkUp

RawTCP server gateway disconnected – LinkDown

Link status change

SETUP

13 NTP

13.1 Overview

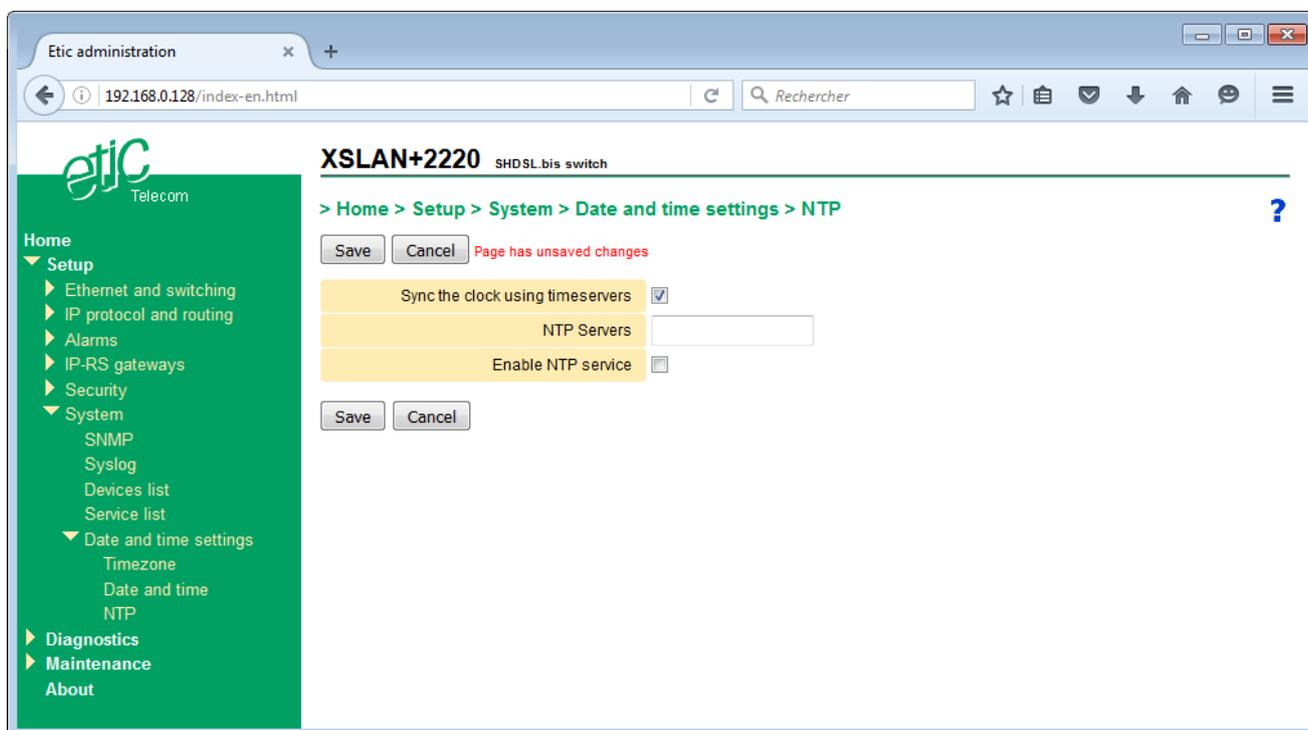
The FTP protocol is used to synchronize the time of a device on a reference server

The XS supports this protocol and can get the time on one or more time servers.

The XS can also act as a time server and deliver time for secondary equipments. This solution is interesting in the case of a low throughput SHDSL link. Only the XS queries a time server at the other end of the link. Equipments connected to the LAN ports of the XS are synchronized locally. This allows not to overload the low data rate SHDSL link by many NTP requests.

13.2 Setting up the NTP client

- In the menu, choose **Setup > System > Date and time settings > NTP**.
- Tick the **Sync the clock using timeservers** checkbox.



NTP Servers

Enter the IP address of the NTP time server. If there are several servers, enter the different IP address with a coma separator « , » .

13.3 Setting up the NTP server

- In the menu, choose **Setup > System > Date and time settings > NTP**.
- Tick the **Enable NTP service** checkbox.

14 Quality of service (Qos) - DiffServ

14.1 Overview

The IP protocol can multiplex different services on the same media (video, command and control, html ...). The advantages are well known; However, if a service transmits an excessive IP traffic, the network is congested and the latency becomes important.

By default, each SHDSL port has a transmit FIFO buffer of 10 packets (this value can be modified). When activating the "Quality of Service" (QoS), the FIFO is replaced by a SFQ buffer (Stochastic Fairness Queuing). SFQ automatically classifies incoming frames into streams according to their addresses and their source and destination ports. Each stream alternately send a frame. This method limits the latency and reserve a bandwidth for each traffic. This method is sufficient in most cases and requires no further setting.

If the result is not satisfactory, it is possible to manually classify and prioritize different traffics using the DiffServ algorithm that will mark each IP frame in the DSCP field.

Principle of operation :

A traffic is the couple formed by an IP address and a service (ftp, html, Modbus etc ...).
 Moreover, the bandwidth available is shared into 5 parts called "classes"
 Each traffic defined is assigned to one of the first 4 classes: Platinum, Gold, Silver, Bronze. .
 The undefined traffic is assigned to the class « Default ».

The "Platinum" class has the highest priority; That traffic is routed first whatever the traffic in the other classes. Classes "Gold, Silver, Bronze" share the available bandwidth:

Exemple	Minimum bandwidth	Maximum bandwidth
	% of the whole bandwidth	% of the whole bandwidth
Gold	50 %	80 %
Silver	30 %	80 %
Bronze	15 %	80 %
Default	5 %	Unlimited
Total	60 %	

Once the traffic of one of these 4 classes fills the minimum band allocated, the additional traffic of this class can take more bandwidth provided that some unused band by other classes is available. The attribution rule of that unused band depends of the class priority: Additional traffic of the Gold class has the highest priority and the one of the Default class has the lowest priority.

Care should be taken not to affect too much traffic to the "Platinum" class. Indeed, the traffic of this class has the highest priority; if it is too large it prevents traffic from other classes to flow.
 "Platinum" class should be reserved for example, to "Control and Command" traffic.

The DiffServ classification is effective in the area of SHDSL links. Within this domain IP frames keep their DSCP classification mark. By cons, IP frames that exit the Ethernet LAN port lose their classification (DSCP 0). Sometimes it is useful to extend the DiffServ domain to Ethernet LAN, for instance, to communicate with another XS on the Ethernet LAN. In this case IP frames that exit the Ethernet LAN port keep their classification, the DSCP field is not set to 0.

SETUP

Corresponding DSCP value for each class :

Olympic classes	DiffServ classes assigned by the XS	DSCP value	DiffServ classes supported by the XS
Platinum	EF	46	EF
Gold	AF11	10	CS1, AF11, AF12, AF13
Silver	AF21	18	CS2, AF21, AF22, AF23
Bronze	AF31	26	CS3, AF31, AF32, AF33
Default	BE	0	BE

14.2 Basic configuration

- In the menu, choose **Setup > IP protocol and routing > QoS – DiffServ**.
- Tick the **Enable QoS** checkbox.

The screenshot shows the Etic administration web interface for the XSLAN+2220 SHDSL.bis switch. The breadcrumb trail is: Home > Setup > IP protocol and routing > QoS - DiffServ. The configuration options are:

- Enable QoS:
- Enable domain extensions:

The **Classes** section shows the following bandwidth settings:

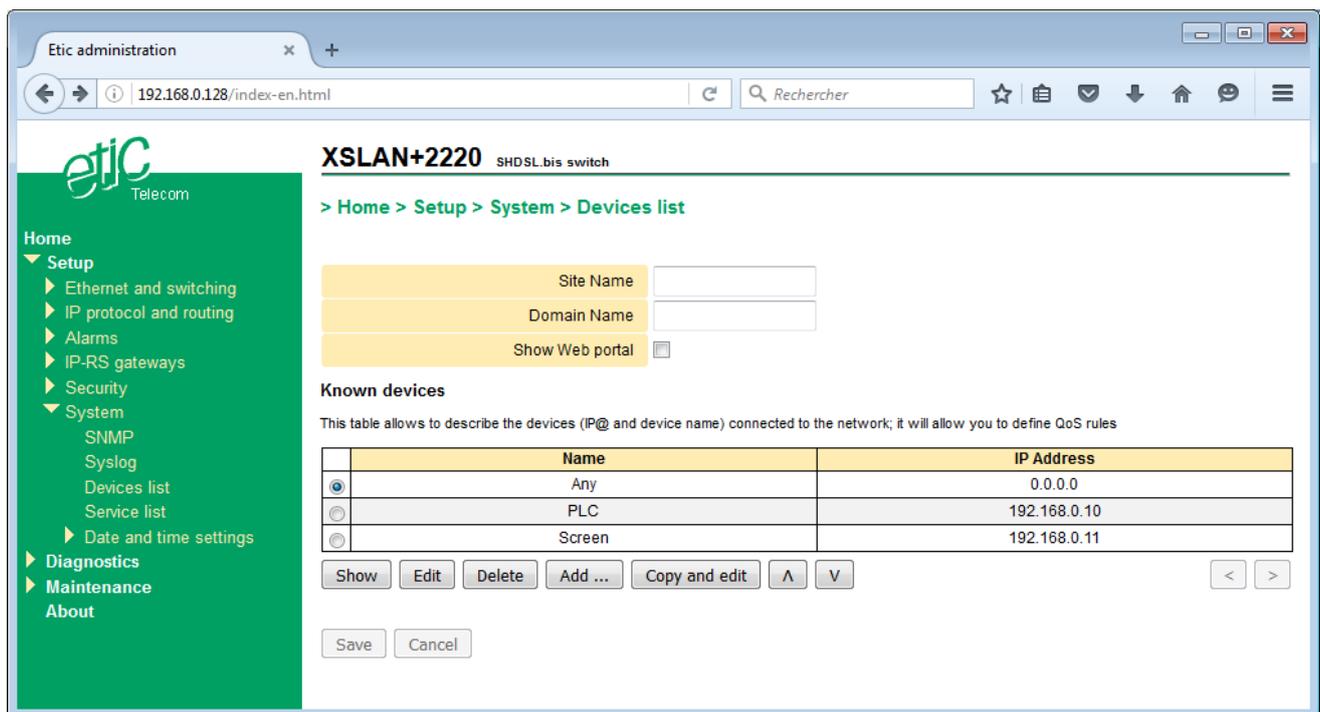
Class	Minimum bandwidth reserved	Maximum bandwidth allowed
Gold	50 (0 to 95, step 5)	100 (0 to 100, step 5)
Silver	30 (0 to 95, step 5)	100 (0 to 100, step 5)
Bronze	15 (0 to 95, step 5)	100 (0 to 100, step 5)

The **Traffic classification** section shows a table with columns for Machine, Service, and Class. Below the table are buttons for Show, Edit, Delete, Add ..., Copy and edit, and navigation arrows. At the bottom are Save and Cancel buttons.

14.3 Advanced configuration

Step 1 : Define the devices addresses

- In the menu, choose **Setup > System > Device list**.
- Click **Add**
- Give a name for this device or this group of devices.
- Enter an IP address to specify a single host (for instance 192.168.10.12) or a range of IP addresses and a netmask (for instance 192.168.10.0/255.255.255.0).
- Click **Save**.



Step 2 : Optionally set other services

- In the menu, choose **Setup > System > Service list**.
- Click **Add**
- Give a name for this service.
- Define a protocol and a port number for that service.
- Click **Save**.

SETUP

The screenshot shows a web browser window with the URL `192.168.0.128/index-en.html`. The page title is "XSLAN+2220 SHDSL.bis switch". The breadcrumb navigation is `> Home > Setup > System > Service list`. The left sidebar contains a menu with options: Home, Setup (expanded), Ethernet and switching, IP protocol and routing, Alarms, IP-RS gateways, Security, System (expanded), SNMP, Syslog, Devices list, Service list (selected), Date and time settings, Diagnostics, Maintenance, and About. The main content area is titled "Service list" and includes a descriptive paragraph: "A service consists of a couple (port, protocol), eg. web/http service : (80, tcp). The table below includes the list of the usual services. You may have to use them to build the firewall. You may add any service to the list." Below this is a table with columns for Name, Protocol, and Port. The table lists various services such as Any, Http, Ftp, Telnet, Dns, Pop3, Sntp, Tftp, Ping, Snmp, Netbios, SMB MS-ds, Modbus TCP, Schneider UNI-TE, Rockwell EtherNet/IP-CIP, Omron FINS, and Siemens S7 ISO on TCP. At the bottom of the table are buttons for Show, Edit, Delete, Add ..., Copy and edit, and navigation arrows.

	Name	Protocol	Port
<input checked="" type="radio"/>	Any	All	0:65535
<input type="radio"/>	Http	TCP	80
<input type="radio"/>	Ftp	TCP	21
<input type="radio"/>	Telnet	TCP	23
<input type="radio"/>	Dns	UDP	53
<input type="radio"/>	Pop3	TCP	110
<input type="radio"/>	Sntp	TCP	25
<input type="radio"/>	Tftp	UDP	69
<input type="radio"/>	Ping	ICMP	8
<input type="radio"/>	Snmp	UDP	161,162
<input type="radio"/>	Netbios	TCP	137:139
<input type="radio"/>	SMB MS-ds	TCP	445
<input type="radio"/>	Modbus TCP	TCP	502
<input type="radio"/>	Schneider UNI-TE	TCP	502
<input type="radio"/>	Rockwell EtherNet/IP-CIP	TCP	44818
<input type="radio"/>	Omron FINS	UDP	9600
<input type="radio"/>	Siemens S7 ISO on TCP	TCP	102

Step 3 : Configure the traffic classes

- In the menu, choose **Setup > IP protocol and routing > QoS – DiffServ**.
- Tick the **Enable QoS** checkbox.
- Assign a minimum and a maximum bandwidth to each class (Gold, Silver, Bronze).
- Click **Save**.

Step 4 : Classify the traffic

- Under the traffic classification table, click **Add**
- Assign a device and a service to a class (Platinum, Gold, Silver, Bronze).
- Click **Save**.

The screenshot shows the Etic administration web interface for a switch named XSLAN+2220. The browser address bar shows the URL 192.168.0.128/index-en.html. The left sidebar contains a navigation menu with categories like Home, Setup, Alarms, IP-RS gateways, Security, System, Diagnostics, and Maintenance. The main content area is titled 'QoS - DiffServ' and includes the following configuration options:

- Enable QoS:**
- Enable domain extensions:**

Classes configuration:

Class	Minimum bandwidth reserved	Maximum bandwidth allowed
Gold class	50 (0 to 95, step 5)	100 (0 to 100, step 5)
Silver class	30 (0 to 95, step 5)	100 (0 to 100, step 5)
Bronze class	15 (0 to 95, step 5)	100 (0 to 100, step 5)

Traffic classification table:

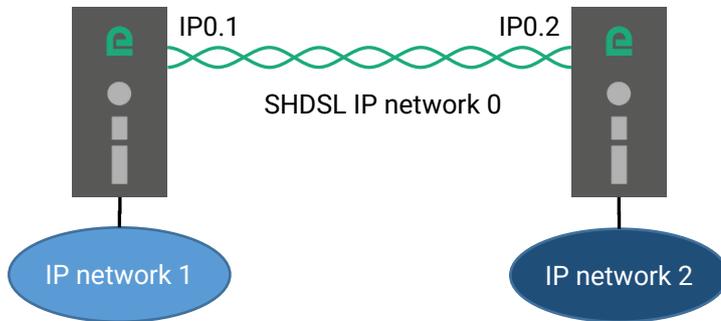
Machine	Service	Class
<input checked="" type="radio"/> PLC	Modbus TCP	Platinum
<input type="radio"/> PLC	Telnet	Silver
<input type="radio"/> Screen	Http	Gold

Below the table are buttons for Show, Edit, Delete, Add ..., Copy and edit, and navigation arrows. At the bottom are Save and Cancel buttons.

15 IP Routing

15.1 Overview

The XS can perform basic IP routing functions between its local interface consisting of 2 to 4 Ethernet ports and the SHDSL interface, consisting of 1 to 4 SHDSL ports.



See chapter « IP addresses setting »

To access devices located in a different IP network, the XS usually send the IP frames to its default gateway. However, for more complex situation, it is possible to create static routes or use a routing protocol.

15.2 Static routes

To create a static route,

- In the menu, choose **Setup > IP protocol and routing > Static routes**.
- Click **Add ...**.
- Enter the destination IP address, the netmask, the gateway address used for this destination and the cost of the route.

The screenshot shows the web interface for an XSLAN+2220 SHDSL bis switch. The breadcrumb navigation is: Home > Setup > IP protocol and routing > Static routes. The page title is "XSLAN+2220 SHDSL bis switch". The main content area is titled "Static routes table" and includes the text "This list defines accessible networks through routers". Below this is a table with the following data:

	Active	Route name	IP address	Netmask	Gateway IP address	Interface	Metric (0-32000)
<input checked="" type="radio"/>	Yes	Scada	192.168.38.2	255.255.255.0	192.168.0.1		10

Below the table are several buttons: Show, Edit, Delete, Add ..., Copy and edit, and two arrow buttons. A left sidebar contains a navigation menu with categories like Home, Setup, Ethernet and switching, IP protocol and routing, Alarms, IP-RS gateways, Security, System, Diagnostics, Maintenance, and About.

15.3 RIP protocol

RIP (Routing Information Protocol) is an IP routing protocol that allows each router or a network equipment to know the route to another network.

Principle of operation :

Routing table broadcasting

Each router transmits to neighboring routers and neighboring RIP listeners, its routing table.

Routing table update

Each router updates its own table using the information received from the other.

RIP prevents to declare static routes in each router.

To enable RIP,

- In the menu, choose **Setup > IP protocol and routing > RIP**.
- Tick the **Enable RIP** checkbox.

When enabled, RIP runs on all Ethernet ports, LAN or SHDSL, regardless whether the router mode is enabled or not.

15.4 OSPF protocol

The OSPF protocol performs the same function as RIP but is used on more complex network configuration.

The XS supports OSPF but the configuration is done via SSH command line. This is an advanced operating mode which allows the XS to behave as a very flexible and sophisticated router. For example, it is possible to bridge any Ethernet port with any SHDSL port and assign different IP addresses for each port.

To enable OSPF,

- In the menu, choose **Setup > IP protocol and routing > RIP > Advanced routing**.
- Tick the **Enable advanced routing mode (SSH CLI)** checkbox.
- In the **Bridge configuration** table, click **Add**
- Enter the list of interfaces that belong to that bridge.

For each bridges an IP address and a subnet mask will be assigned later.

The rest of the configuration is done via SSH on port 22.

For more information, refer to Quagga reference manual.

16 Advanced NAT

16.1 Overview

The IP address translation function consists of modifying the source and/or destination addresses as well as the port number of the IP frames passing through the XS.

It applies to any IP frame received by the XS both on its LAN interface and on its SHDSL interface.

One brings out the DNAT function which consists in replacing the IP address and the destination port, the SNAT function which consists of replacing the source IP address.

Because the DNAT and SNAT functions modify the IP addresses of the IP packets processed by the XS and because the firewall filters that frames, it is very important to understand in which order that different functions are carried out.

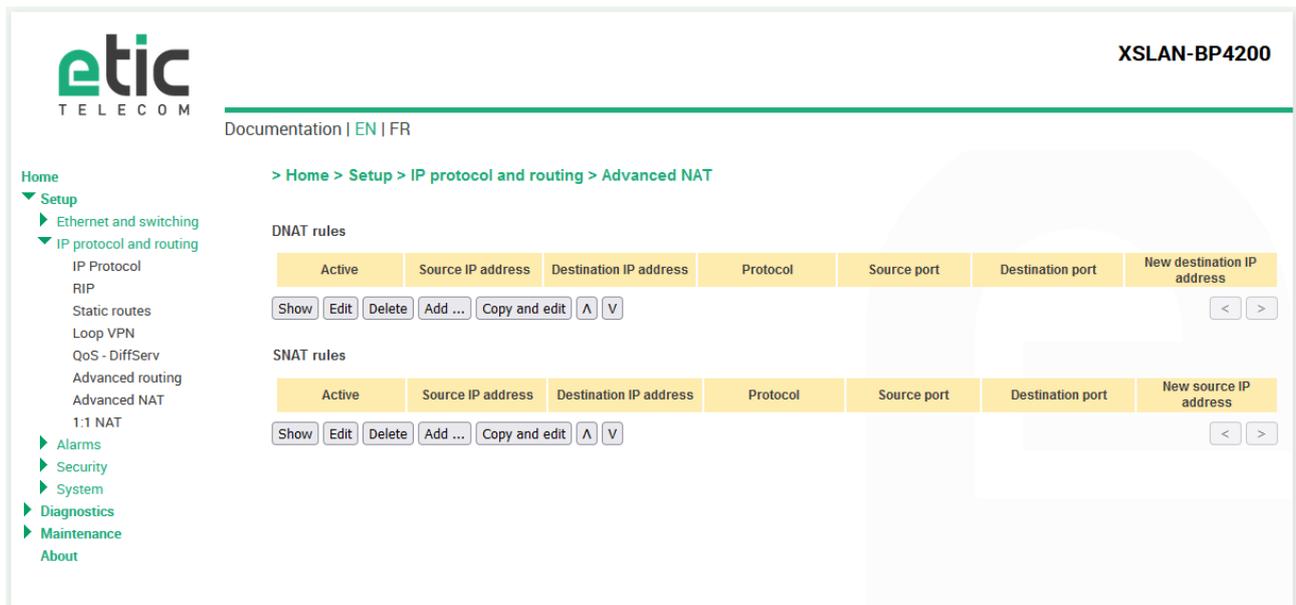
The order in which the substitution is made changes the way the firewall filter rules are configured. Substitution treatments are carried out as follows:

Direction	
SHDSL to LAN	SHDSL -> DNAT -> Firewall -> SNAT -> LAN
LAN to SHDSL	LAN -> DNAT -> Firewall -> SNAT -> SHDSL

16.2 Set up

To set the advanced address translation function,

- In the menu, choose **Setup > IP protocol and routing > Advanced NAT**.



To create a new DNAT rule,

- Click **Add** in the DNAT table
- The DNAT rule window is displayed
- Click **Active** to make the rule active.
- Enter the characteristics of the IP frames which must be modified by the DNAT rule.
 - Source IP address & Destination IP address.
 - Protocol (TCP, UDP, ...)
 - Source port & Destination port
- Enter the new destination port number and IP address.

To create a new SNAT rule,

- Click **Add** in the SNAT table
- The SNAT rule window is displayed
- Click **Active** to make the rule active.
- Enter the characteristics of the IP frames which must be modified by the SNAT rule :
 - Source & Destination IP address and transport protocol (TCP, UDP)
 - Source & Destination port
- Enter the new source IP address.

17 Firewall

17.1 Overview

The firewall filters IP frames between the LAN interface and the SHDSL interface to protect devices connected to the LAN network.

It consists of a set of filtering rules that authorize or deny a type of IP frames.

The firewall is a SPI type (Stateful Packet inspection). Filter rules only apply on request frames. Answer frames do not have to be specified, they are automatically accepted if they relate to accepted requests.

17.2 Setting up the firewall

To enable the firewall,

- In the menu, choose **Setup > Security > Firewall**.
- Click **Enable Firewall**.

The screenshot shows the 'Firewall' configuration page in the etic XSLAN-BP4200 web interface. The page title is '> Firewall'. Under 'SHDSL-LAN traffic rules:', there are several settings:

- 'Enable Firewall' is checked with a blue checkbox.
- 'Default policy LAN->SHDSL' is set to 'Allow' via a dropdown menu.
- 'Default policy SHDSL->LAN' is set to 'Allow' via a dropdown menu.
- 'Default policy LAN->Intern' is set to 'Allow' via a dropdown menu.
- 'Default policy SHDSL->Intern' is set to 'Allow' via a dropdown menu.

A warning message reads: 'WARNING: If both "Intern" traffics are denied, You won't be able to open this web administration interface anymore.'

Below the policies is a table with the following columns: Direction, Action, Protocole, Source IP address, Source port, Destination IP address, and Destination port. Below the table are buttons for 'Show', 'Edit', 'Delete', 'Add ...', 'Copy and edit', and a small icon. At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

- **Default policy**

The default policy is the decision which will be applied if a packet does not match any of the rules of the filter.

A distinction is made between traffic going through the XS (LAN-SHDSL) and traffic destined for the XS for, among other things, web administration (LAN/SHDSL to intern).

The SHDSL to LAN and the LAN to SHDSL traffic are regarded separately because the decision can be opposite for a packet coming from the SHDSL or coming from the LAN.

- **Filter rules table**

Each row is a filter rule.

Each rule of the filter is composed a several fields which defines an action (Allow or Deny) and a particular data flow:

- Direction (« SHDSL to LAN » or « LAN to SHDSL » or « LAN to Intern » « SHDSL to Intern »),
- Protocol (TCP, UDP...),
- IP@ & port number, source & destination.

Here is an example of a filter which authorizes two devices of the SHDSL network (192.168.2.X) to access a particular device of the LAN network. Any other flow from SHDSL to the LAN is prohibited.

Default policy : LAN -> SHDSL : Accept - SHDSL -> LAN : Deny						
Direction	Action	Protocol	Source IP @	Source port	Destination IP @	Dest. port
SHDSL->LAN	Allow	any	192.168.2.1	any	192.168.1.12	any
SHDSL->LAN	Allow	TCP	192.168.2.2	any	192.168.1.12	502

- **Operation**

When the firewall receives an IP frame, it successively checks compliance with the filtering rules.

If the frame does not conform to the first rule, it is submitted to the next one and so on.

As soon as it complies with a rule in the table, the firewall applies the associated action to it (allow or deny).

If the frame does not comply with any rule, the default policy is applied to it (allow or deny).

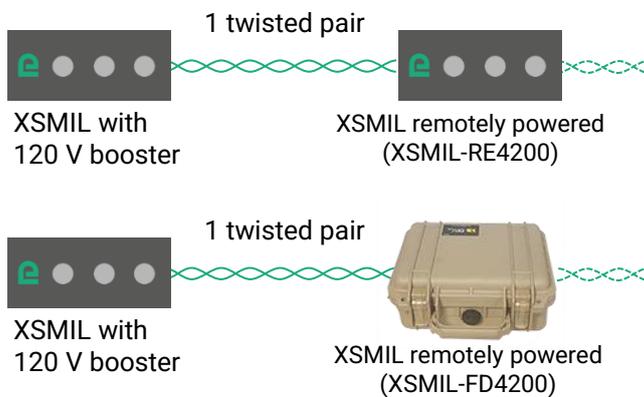
18 Remote power feeding

18.1 Overview

The XSMIL-FD4200 (not described here) or the XSMIL-RE4200 can be powered through the SHDSL lines. A 120 V DC voltage, provided by the XSMIL equipped with an internal 120 V booster (XSMIL-BP4200IB), is injected on the line with the signal. This applies on the SHDSL port 1. This voltage powers the remote XSMIL-FD4200 (or XSMIL-RE4200). No local power is needed at this side.

This feature is particularly useful when it is necessary to repeat the SHDSL signal to reach a long distance but there is no local power available where the repeater is installed.

The maximum distance to remotely power an XSMIL-FD4200 (or XSMIL-RE4200) depends on the quality of the cable (4 km on a D10 cable).



SHDSL ports 1 and 2 of an XSMIL-FD4200 (or XSMIL-RE4200) support the remote power feeding. If powered from both sides, the maximum distance is doubled.



18.2 Safety aspects

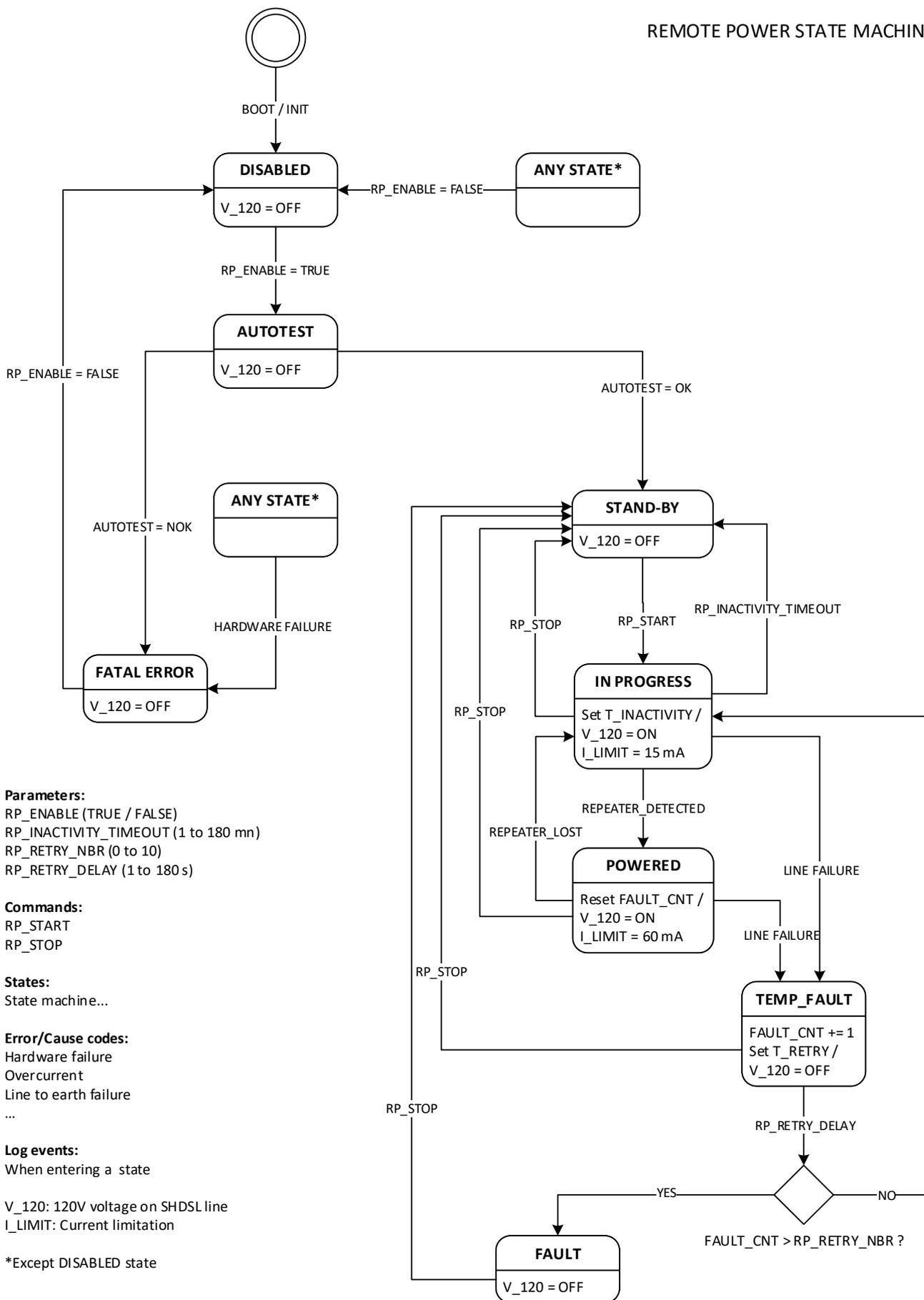
The remote power function complies with IEC 62368-3: Safety aspects for DC power transfer through communication cables and ports.

Several safety improvements are provided for field case:

- Current limitation to #15mA (rather than 60 mA) until a repeater is detected
- Remote power must be activated manually by the user when needed
- Inactivity time out to avoid a permanent high voltage on a cable, configurable up to a few hours

18.3 State machine

REMOTE POWER STATE MACHINE



Parameters:

- RP_ENABLE (TRUE / FALSE)
- RP_INACTIVITY_TIMEOUT (1 to 180 mn)
- RP_RETRY_NBR (0 to 10)
- RP_RETRY_DELAY (1 to 180 s)

Commands:

- RP_START
- RP_STOP

States:

State machine...

Error/Cause codes:

- Hardware failure
- Overcurrent
- Line to earth failure
- ...

Log events:

When entering a state

V_120: 120V voltage on SHDSL line
I_LIMIT: Current limitation

*Except DISABLED state

SETUP

18.4 Details

18.4.1 Repeater detection

When the repeater receives the remote power, it starts to draw a sequence of low current cycles to signal itself to the D10 modem. The current cycle consists of: 1s at 2 mA and 1s at 6 mA. The cycle is repeated at least 5 times. At the D10 modem side, the measurement of 5 consecutive cycles triggers the REPEATER_DETECTED event.

18.4.2 Loss of Repeater

A current drop below 10 mA for at least 1s triggers the REPEATER_LOST event.

18.4.3 Line failures

Overcurrent:

When the current drawn reaches the current limitation for more than 200 ms.

Line to earth fault:

When one conductor is accidentally earthed for more than 200 ms.

18.4.4 Error/Cause codes

These codes depend on the actual state of the remote power and are not relevant in DISABLED, AUTOTEST and POWERED states.

FATAL_ERROR state:

Hardware failure - Current limitation
Hardware failure - Voltage limitation
Hardware failure – Unspecified

STAND-BY state:

Normal – Autotest OK
Normal – Stopped by user
Inactivity time-out

IN PROGRESS state:

Normal – Started
Repeater lost
Retry after line failure

TEMP_FAULT state:

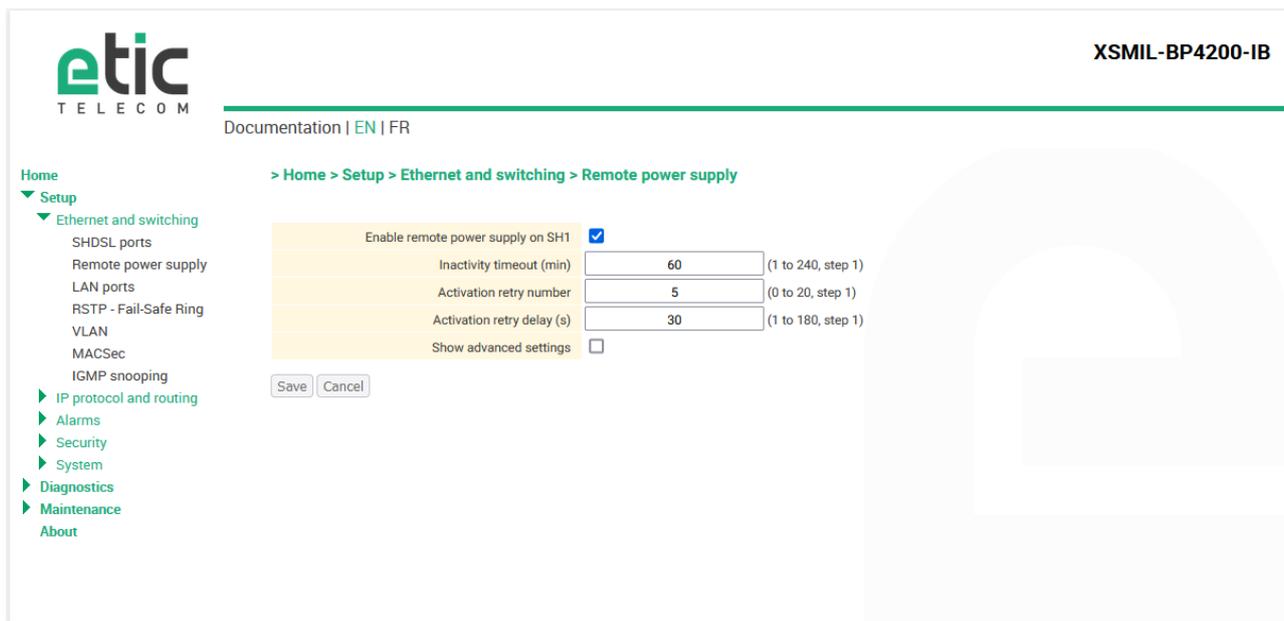
Line failure – Overcurrent
Line to earth failure

FAULT state:

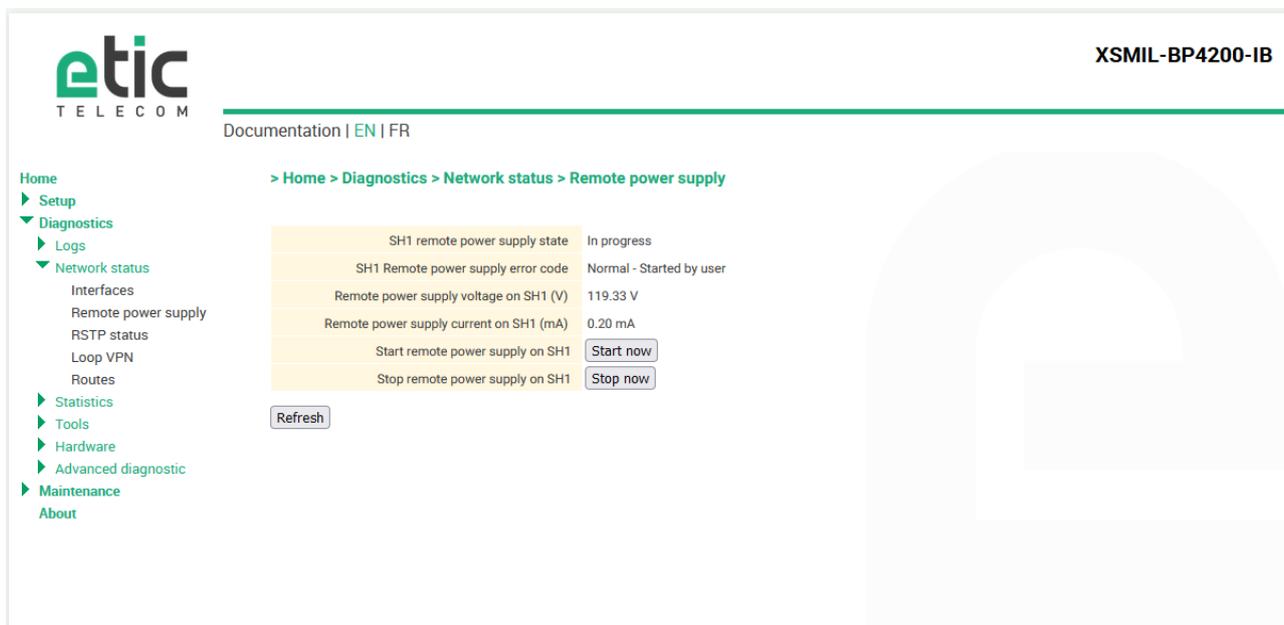
Line failure – Overcurrent
Line to earth failure

18.5 Setting up the Remote power supply

- In the menu, choose [Setup > Ethernet and switching > Remote power supply](#).
- Tick the [Enable remote power supply on SH1](#) checkbox.



- In the menu, choose **Diagnostics > Network status > Remote power supply**.
- Click **Start** to activate the power supply on SHDSL port 1.
- Check the Remote power state (see state machine above)
- Click **Stop** to deactivate the power supply.



19 Alarms

19.1 SNMP Alarms

See SNMP chapter.

19.2 Digital output

The digital output can switch OFF in case of one of these events :

Port SHDSL 1 disconnected

Port SHDSL 2 disconnected *

Port SHDSL 1or 2 disconnected *

Fail safe ring broken *

*Only available on XS with more than one SHDSL port

20 Serial to IP gateways

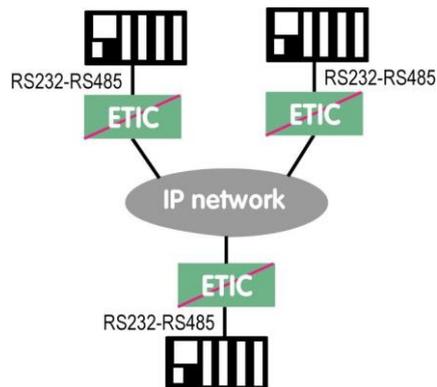
20.1 Overview

Depending on the model, the XS provides 2 serial ports : 2 RS232, or 1 RS232 and 1 RS485, or 1 RS422 isolated or 1 RS485 isolated.

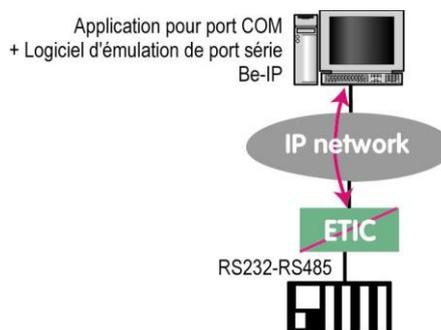
A gateway can be assigned to each serial port.

A serial gateway makes possible to use the IP network to transport serial data between two or several serial devices or directly with devices connected to the Ethernet network.

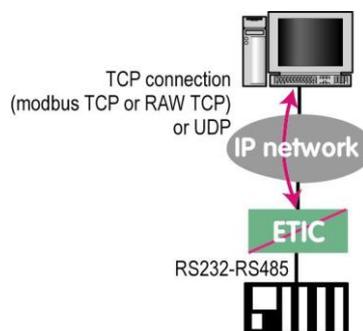
- Communication between serial devices



- Communication between a serial device and a PC via a COM port emulation software



- Communication between serial devices and a PC software application able to encapsulate the serial data into UDP or TCP (like a Modbus TCP software application for instance).



To perform the functions described above, several types of gateways are available.

SETUP

20.2 Modbus gateway

The Modbus gateway allows to connect serial RS232-RS485 master or slaves devices to one or several Modbus TCP devices connected to the IP network

20.2.1 Glossary

A Modbus TCP client is a device connected to the Ethernet network and able to transmit Modbus requests to a Modbus TCP server device which will reply.

Several Modbus clients can send requests to the same Modbus TCP server.

A Modbus TCP server is a device connected to the Ethernet network and able to reply to Modbus requests to a coming from Modbus TCP client devices.

A TCP server can reply to several TCP clients.

A Modbus master device is a device connected to a serial asynchronous link and able to send requests to a Modbus slave device connected to the same serial network.

A Modbus slave device is a device connected to a serial asynchronous link and able to reply to Modbus requests connected to the same serial network.

Modbus address : An address between 0 and 254 assigned to each participant to a Modbus network.

Remark the Modbus address must not be confused with the IP address of a Modbus device

.

20.2.2 Selecting a Modbus client or a Modbus server gateway

Select the Modbus Server gateway to connect serial slave devices to the serial port of the product.

Select the Modbus Client gateway to connect a serial Master device to the serial port of the product.

20.2.3 Assigning a Modbus gateway to a serial port

The Modbus client gateway (respectively server) can be assigned to the serial port COM1 or COM2.

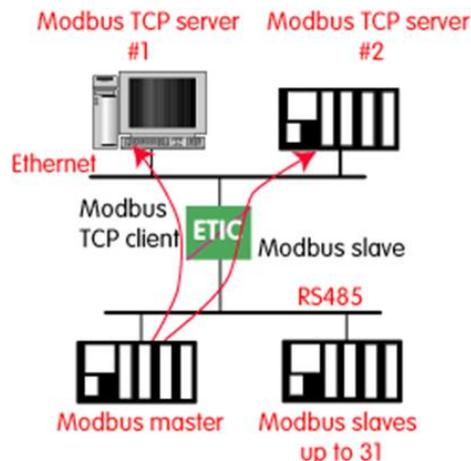
The Modbus client gateway can be assigned to a serial port (COM1 for ex.) while the Modbus server gateway is assigned to the other port (COM2 for ex.).

20.2.4 Modbus client gateway

This gateway allows to connect a serial modbus master to the serial interface of the product.

The gateway can be connected to several Modbus TCP servers on the IP network

Other slaves can be connected to the serial link.

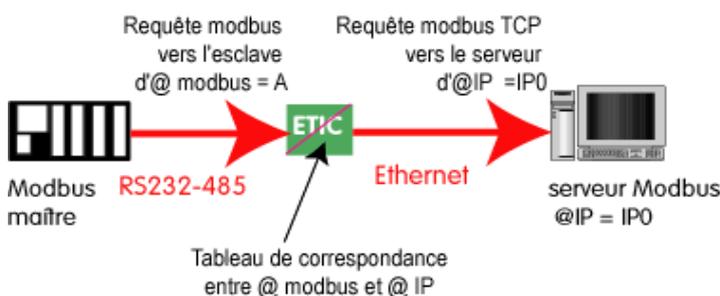


How the Modbus Client Gateway works :

In order to access a Modbus TCP server on the IP network, a mapping table between a Modbus slave address and an IP address is set ; so when the Modbus master sends a request to the Modbus slave at address A, the mapping table allow to transmit the request to the corresponding IP address.

In addition, the Modbus address field of the Modbus TCP frame is set to A.

The mapping table can contain 32 lines allowing a Modbus master to address 32 servers on the IP network.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Modbus > Modbus client**.
- Tick the **Enable Modbus client** checkbox.
- Configure the following parameters.

COM port

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Modbus protocol

Select RTU (hexa) or ASCII.

Inter-character time

Set up the maximum delay the gateway will have to wait between a received character of a Modbus answer packet and the following character of the same packet.

TCP idle Timeout

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

SETUP

TCP port

Set the port number the gateway has to use. The default Modbus TCP port is 502.

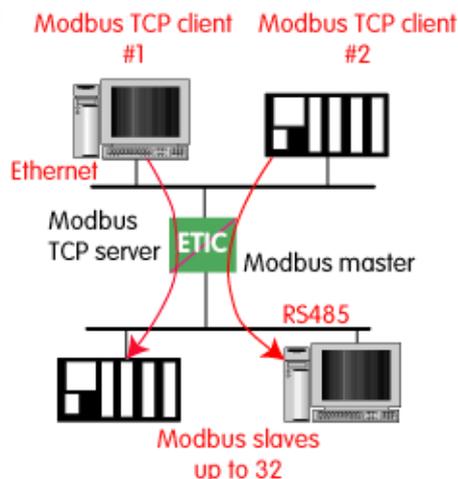
Modbus slaves

The table allow the mapping of a Modbus slave address to an IP address.

20.2.5 Modbus server gateway

This gateway allows to connect serial modbus slaves to the serial interface of the product.

Up to 32 slaves, can be connected to the RS485 port.



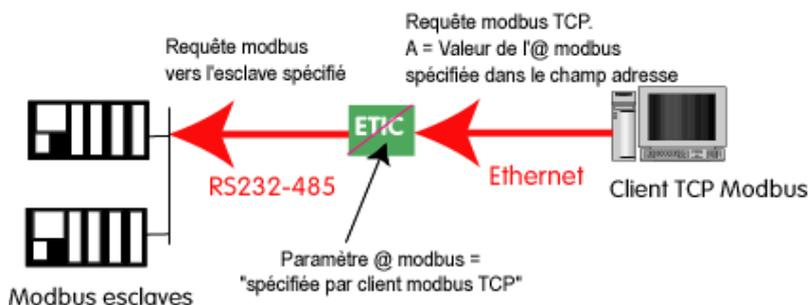
How the Modbus server Gateway works :

A Modbus TCP client send a Modbus TCP client to the gateway.

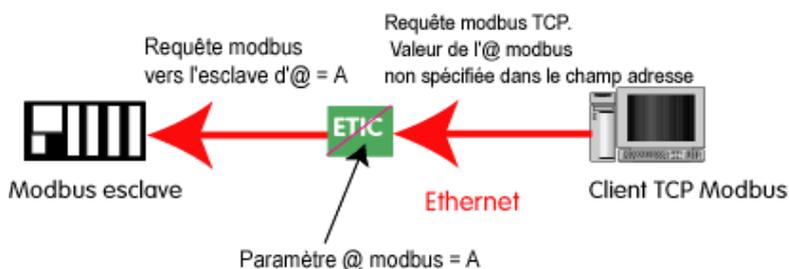
The gateway behave as a master on the serial link. It transcode and transmit the request on the serial link.

The Modbus slave address of the request is :

- Either the address contained in the Modbus TCP address field ; in this case, several slaves can be addressed on the serial link.



- Or a fixed address configured in the gateway (see below); in this case, only one slave can be addressed on the serial link.



Warning : Several TCP Modbus client can send requests to the slaves on the serial link. Nevertheless, care must be taken not to saturate the serial link since its flow rate is much lower than the Ethernet one.

To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Modbus > Modbus server**.
- Tick the **Enable Modbus server** checkbox.

SETUP

- Configure the following parameters.

COM port

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link..

Modbus protocol

Select RTU (hexa) or ASCII.

Enable proxy/cache function

If this function is active, a request is only sent to a slave if the same query has not been sent since the time set by the "cache refresh" parameter.

Cache refresh

Sets the minimum time between two identical requests to the same slave.

Inter-character time

Set up the maximum delay the gateway will have to wait between a received character of a Modbus answer packet and the following character of the same packet.

Modbus slave address

If the value "0" is selected, the gateway uses the Modbus address specified by the Modbus TCP client to address the Modbus slave on the serial link ; up to 32 slaves can be addressed on the serial link.

If a particular value is selected (1 to 255), the gateway sends all requests to the selected slave ; only one slave can be addressed on the serial link.

TCP idle Timeout

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

Slave response timeout

Set the time the gateway will wait for a response from the slave.

TCP port

Set the port number the gateway has to use. The default Modbus TCP port is 502.

Local reiteration count

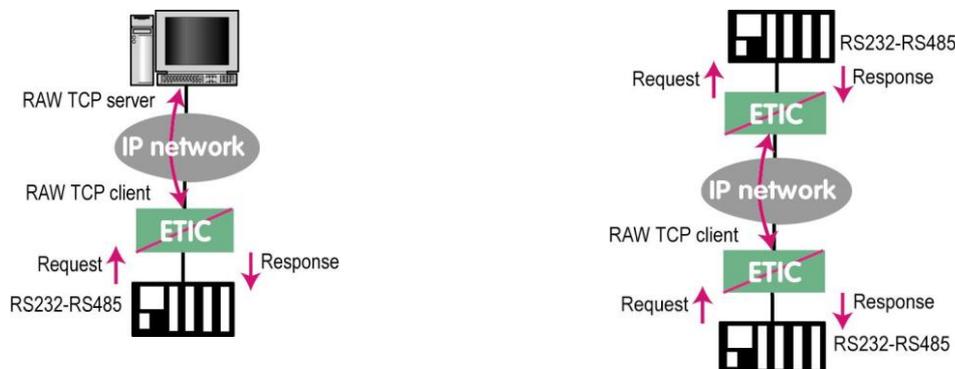
Set up the number of times the gateway will repeat a request in case of no response from the slave.

20.3 Raw TCP gateway

20.3.1 Raw TCP client

The Raw client gateway can be used if a serial “master” device has to send requests to one slave device (also called server) located on the IP network.

The server can be either an ETIC gateway or a PC including a software TCP server.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Transparent > Raw client COMx**
- Tick the **Enable** checkbox.
- Configure the following parameters.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Receive buffer size

Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

RS end frame timeout

Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.

Once declared complete, the gateway will transmit the string to the IP network.

TCP idle Timeout

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

TCP port

Set the port number the gateway has to use.

Warning : If two gateways of the same type are active on the two serial ports, they can not use the same TCP port number.

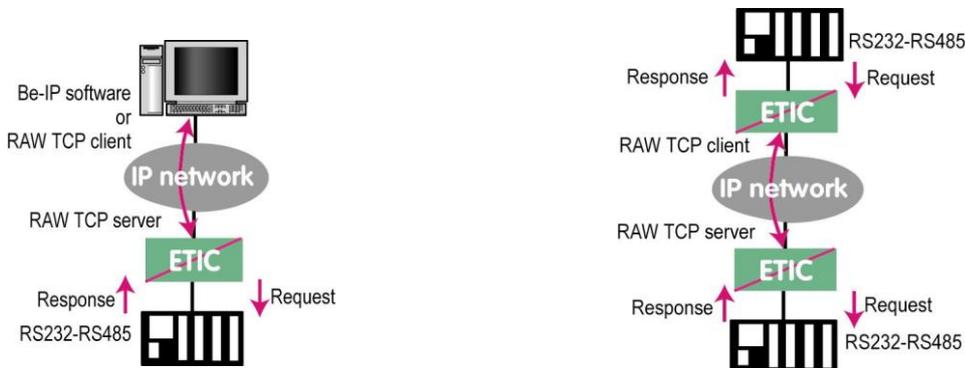
Server IP address

Set the IP address of the Raw server. The gateway will connect to that server and send it the data received on the serial link.

SETUP

20.3.2 Raw server gateway

That gateway can be used if a serial slave device has to answer requests coming from devices located on the IP network and acting like a master (also called TCP client).



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Transparent > Raw server COMx**
- Tick the **Enable** checkbox.
- Configure the following parameters.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Receive buffer size

Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

RS end frame timeout

Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.

Once declared complete, the gateway will transmit the string to the IP network.

TCP idle Timeout

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

TCP port

Set the port number the gateway has to use.

Warning : If two gateways of the same type are active on the two serial ports, they can not use the same TCP port number.

20.4 Raw UDP gateway

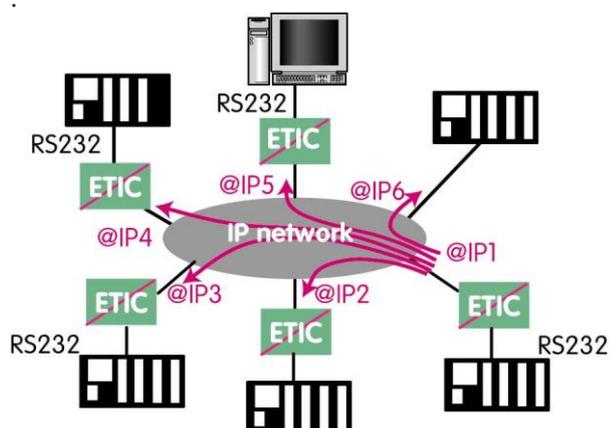
The RAW UDP gateway allows to connect together a group of serial or IP devices through an IP network. The group can include IP devices if they have the software pieces able to receive or transmit serial data inside UDP.

Serial data transmitted by each device is transmitted to all other serial devices through the IP network.

A table of IP addresses define the list of the devices belonging to the group.

The serial data is encapsulated in the UDP protocol.

The UDP datagram is sent to each destination IP address stored in the table.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Transparent > Raw UDP COMx**
- Tick the **Enable** checkbox.
- Configure the following parameters.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Receive buffer size

Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

RS end frame timeout

Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.

Once declared complete, the gateway will transmit the string to the IP network.

UDP port

Set the port number the gateway has to use.

Warning : If two gateways of the same type are active on the two serial ports, they can not use the same UDP port number.

Destination

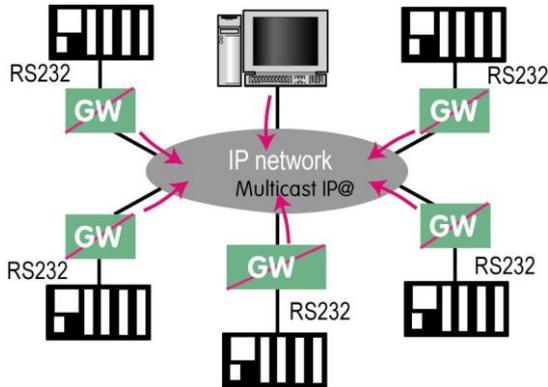
This table stores the IP addresses of the gateways to which the serial data, encapsulated inside UDP, have to be sent. A different UDP port number can be entered for each destination IP address.

SETUP

20.5 Raw multicast gateway

This gateway is designed to connect a serial device to several devices on an IP network.

It uses the "multicast" protocol that can simultaneously deliver an IP frame to many devices without increasing the traffic: The RS232 data are transmitted in an IP frame with a particular IP address called multicast address; all subscribers to this address can receive the frame.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Transparent > Raw Multicast COMx**
- Tick the **Enable** checkbox.
- Configure the following parameters.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Receive buffer size

Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

RS end frame timeout

Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.

Once declared complete, the gateway will transmit the string to the IP network.

UDP port

Set the port number the gateway has to use.

Warning : If two gateways of the same type are active on the two serial ports, they can not use the same UDP port number.

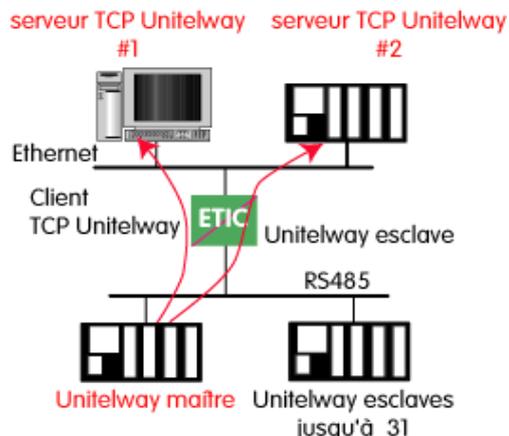
Multicast group IP address

Set the IP address assigned to the multicast group in conformance with the IANA rules.

20.6 Unitelway gateway

The Unitelway gateway is used to connect a Unitelway master PLC to an IP network.

In particular it is used to perform the remote maintenance of a Schneider Electric RS485 PLCs via an IP network.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Unitelway**
- Tick the **Enable** checkbox.
- Configure the following parameters.

COM port

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link..

Xway address

Gateway address in the Xway network.

TCP idle Timeout

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

Unitelway slaves

Mapping between the address of each Unitelway slave emulated by the gateway and the IP and XWAY addresses of the device on Ethernet.

SETUP

20.7 Telnet gateway

This gateway allows a PC running a Telnet client software to connect to an equipment connected to the serial link of the XS.

The data rate and the format of the characters on the serial link can be controlled according to the RFC2217 standard.

To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Telnet**
- Tick the **Enable** checkbox.
- Configure the following parameters.

COM port

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

TCP idle Timeout

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

TCP port

Set the port number the gateway has to use.

DIAGNOSTICS AND MAINTENANCE

1 Visual diagnostic

At power up, the RUN LED  is red for about 20 seconds during the initialization of the product.

Then the LED turns green and blinks for 30 seconds then becomes steady green when the product is ready.

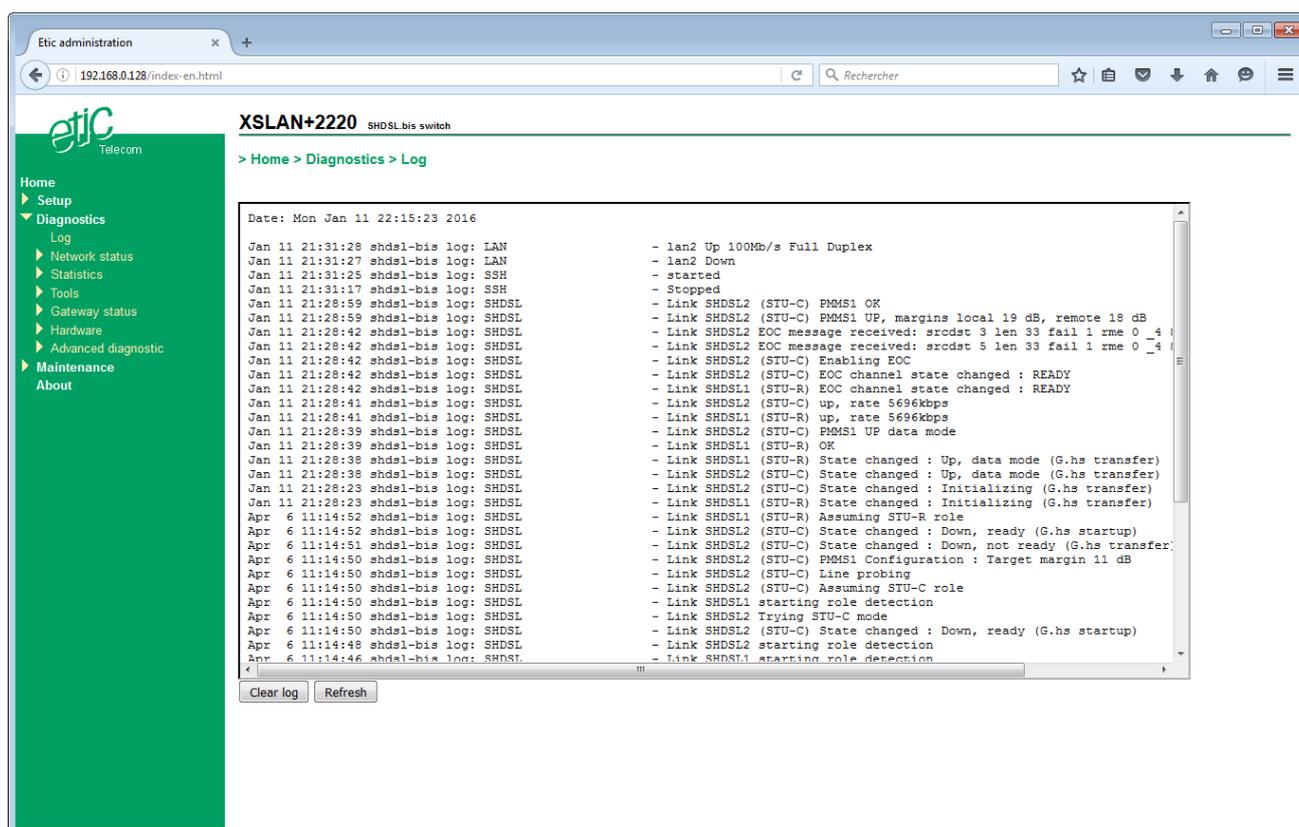
If the LED remains red after that delay, the product is probably faulty ; please contact the hotline.

2 Log

The log displays the last three hundred time-stamped events including the SHDSL connections and disconnections.

To access the log,

- In the menu, choose **Diagnostic > Log**.



The screenshot shows the Etic administration web interface for the device XSLAN+2220 SHDSL bis switch. The breadcrumb navigation is Home > Diagnostics > Log. The log content is as follows:

```

Date: Mon Jan 11 22:15:23 2016
Jan 11 21:31:28 shdsl-bis log: LAN - lan2 Up 100Mb/s Full Duplex
Jan 11 21:31:27 shdsl-bis log: LAN - lan2 Down
Jan 11 21:31:25 shdsl-bis log: SSH - started
Jan 11 21:31:17 shdsl-bis log: SSH - Stopped
Jan 11 21:28:59 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) PMMS1 OK
Jan 11 21:28:59 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) PMMS1 UP, margins local 19 dB, remote 18 dB
Jan 11 21:28:42 shdsl-bis log: SHDSL - Link SHDSL2 EOC message received: srodst 3 len 33 fail 1 rme 0 _4
Jan 11 21:28:42 shdsl-bis log: SHDSL - Link SHDSL2 EOC message received: srodst 5 len 33 fail 1 rme 0 _4
Jan 11 21:28:42 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) Enabling EOC
Jan 11 21:28:42 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) EOC channel state changed : READY
Jan 11 21:28:42 shdsl-bis log: SHDSL - Link SHDSL1 (STU-R) EOC channel state changed : READY
Jan 11 21:28:41 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) up, rate 5696kbps
Jan 11 21:28:41 shdsl-bis log: SHDSL - Link SHDSL1 (STU-R) up, rate 5696kbps
Jan 11 21:28:39 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) PMMS1 UP data mode
Jan 11 21:28:39 shdsl-bis log: SHDSL - Link SHDSL1 (STU-R) OK
Jan 11 21:28:38 shdsl-bis log: SHDSL - Link SHDSL1 (STU-R) State changed : Up, data mode (G.hs transfer)
Jan 11 21:28:38 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) State changed : Up, data mode (G.hs transfer)
Jan 11 21:28:23 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) State changed : Initializing (G.hs transfer)
Jan 11 21:28:23 shdsl-bis log: SHDSL - Link SHDSL1 (STU-R) State changed : Initializing (G.hs transfer)
Apr 6 11:14:52 shdsl-bis log: SHDSL - Link SHDSL1 (STU-R) Assuming STU-R role
Apr 6 11:14:52 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) State changed : Down, ready (G.hs startup)
Apr 6 11:14:51 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) State changed : Down, not ready (G.hs transfer)
Apr 6 11:14:50 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) PMMS1 Configuration : Target margin 11 dB
Apr 6 11:14:50 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) Line probing
Apr 6 11:14:50 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) Assuming STU-C role
Apr 6 11:14:50 shdsl-bis log: SHDSL - Link SHDSL1 starting role detection
Apr 6 11:14:50 shdsl-bis log: SHDSL - Link SHDSL2 Trying STU-C mode
Apr 6 11:14:50 shdsl-bis log: SHDSL - Link SHDSL2 (STU-C) State changed : Down, ready (G.hs startup)
Apr 6 11:14:48 shdsl-bis log: SHDSL - Link SHDSL2 starting role detection
Apr 6 11:14:46 shdsl-bis log: SHDSL - Link SHDSL1 starting role detection
  
```

At the bottom of the log window, there are buttons for "Clear log" and "Refresh".

3 Link quality measurement

The quality of the connection can be verified using the following endpoints :

1 : The signal to noise ratio (SNR) margin

This is the difference between the measured SNR and the minimum SNR needed to have an established connection.

The lower the value, the higher the risk to get transmission errors or disconnection in case of noise disturbances on the line.

2 : The link loss number

The number of disconnections is a good indicator of the quality of the link.

On a link that works fine disconnections must be very rare and should only happen during a thunderstorm or an electromagnetic disturbance.

3 : Error rate of the link

The number of errored seconds gives the error rate of the link.

When a link is working well, the number of erroneous seconds must be very low.

A few erroneous seconds may occur time by time, for instance during a thunderstorm or an electromagnetic disturbance.

To verify the link quality :

- In the menu, choose **Diagnostics > Network status > Interfaces**.

The screenshot shows the Etic administration web interface. The browser address bar displays '192.168.0.128/index-en.html'. The page title is 'XSLAN+2220 SHDSL.bis switch'. The breadcrumb navigation is '> Home > Diagnostics > Network status > Interfaces'. The left sidebar contains a menu with options: Home, Setup, Diagnostics (expanded), Log, Network status (expanded), Interfaces, RSTP status, Loop VPN, Routes, Statistics, Tools, Gateway status, Hardware, Advanced diagnostic, Maintenance, and About. The main content area shows the following information:

- MAC address:** MAC Address 00:0a:b4:00:4e:f7
- LAN ports state:** LAN1 state Down, LAN2 state Up 100Mb/s Full Duplex
- SHDSL ports state:** A table with 8 columns: Port name, SHDSL link state, Bitrate, Signal to noise ratio margin, Line attenuation, Last hour erroneous seconds, and Last 24 hours link losses.

	Port name	SHDSL link state	Bitrate	Signal to noise ratio margin	Line attenuation	Last hour erroneous seconds	Last 24 hours link losses
<input checked="" type="radio"/>	SHDSL1	Connected	5696 kbits/sec	18 dB (4/4)	1 dB	0	0
<input type="radio"/>	SHDSL2	Connected	5696 kbits/sec	18 dB (4/4)	1 dB	1	0

Below the table are buttons for 'Show', 'Reset SHDSL connections', and 'Refresh'.

The summary table shows for each SHDSL line:

- If it is connected or not
- The data rate
- The line attenuation
- The SNR margin
- The number of erroneous seconds
- The number of disconnections

To diagnose a malfunction of an SHDSL link,

- Select the SHDSL link
- Click **Show**.

The detailed status of the link is displayed.

The screenshot shows the Etic administration web interface. The browser address bar displays '192.168.0.128/index-en.html'. The page title is 'XSLAN+2220 SHDSL.bis switch'. The breadcrumb trail is '> Home > Diagnostics > Network status > Interfaces > SHDSL link details'. The left sidebar contains a navigation menu with categories: Home, Setup, Diagnostics (expanded), Network status (expanded), Statistics, Tools, Gateway status, Hardware, Advanced diagnostic, Maintenance, and About. The main content area shows the following details for port SHDSL1:

SHDSL link state	
SHDSL link state	Connected
Bitrate	5696 kbits/sec
Signal to noise ratio margin	18 dB (4/4)
Line attenuation	1 dB
Negotiated constellation	PAM-32
Power Back-off value	5

SHDSL counters	
Code violation errors	0
Loss of sync words seconds	0
Erroneous seconds	0
Severely erroneous seconds	0
Unavailable seconds	0
Link losses count	1

At the bottom of the main content area, there are 'Back' and 'Refresh' buttons.

DIAGNOSTICS AND MAINTENANCE

4 SHDSL statistics

SHDSL statistics allow a comprehensive view of the quality of the link by taking into account a long period of operation.

This is a set of counters indicating the link quality for every second, similarly to the G821 standard. Furthermore, an hour by hour history of these counters can be used to correlate transmission defects with other events, such as starting a motor and this to a depth of 15 days.

To access the SHDSL statistics,

- In the menu, choose **Diagnostics > Statistics > SHDSL counters**.

The screenshot shows the Etic administration web interface. The browser address bar displays '192.168.0.128/index-en.html'. The page title is 'XSLAN+2220 SHDSL.bis switch'. The breadcrumb trail is '> Home > Diagnostics > Statistics > SHDSL counters'. The main content area is titled 'SHDSL counters' and contains a table with the following data:

	Port name	Error free seconds	Erroneous seconds	Severely erroneous seconds	Unavailable seconds	Not connected seconds
<input checked="" type="radio"/>	SHDSL1	4168	0	0	0	52
<input type="radio"/>	SHDSL2	4167	1	1	0	52

Below the table is a button labeled 'Reset SHDSL G.821 counters'. The 'SHDSL counters history' section has tabs for 'Line 1' and 'Line 2'. The 'Line 1' tab is active, showing a scrollable log with the following data:

```
Date: Mon Jan 4 23:29:22 2016

EFS : Error free seconds
ES : Erroneous seconds
SES : Severely erroneous seconds
US : Unavailable seconds
NCS : Not connected seconds

Line ID : 1

Datetime          EFS   ES   SES   US   NCS
2016-01-04 23:00:01 3604  0   0   0   0
2016-01-04 22:00:00 3600  0   0   0   0
2016-01-04 21:00:00 3600  0   0   0   0
2016-01-04 20:00:00 3061  1   1   3  172
2016-01-04 19:00:03  0   0   0   0  112
2016-01-04 18:00:02  0   0   0   0  3600
2016-01-04 17:00:02  0   0   0   0  3600
2016-01-04 16:00:02  0   0   0   0  3600
2016-01-04 15:00:02  0   0   0   0  3600
2016-01-04 14:00:02  0   0   0   0  3600
2016-01-04 13:00:02  0   0   0   0  3600
2016-01-04 12:00:02  0   0   0   0  3600
2016-01-04 11:00:02  0   0   0   0  3600
2016-01-04 10:00:02  0   0   0   0  3600
2016-01-04 09:00:02  0   0   0   0  3600
2016-01-04 08:00:02  0   0   0   0  3600
2016-01-04 07:00:02  0   0   0   0  3600
2016-01-04 06:00:02  0   0   0   0  3600
2016-01-04 05:00:02  0   0   0   0  3600
2016-01-04 04:00:02  0   0   0   0  3600
```

A 'Refresh' button is located at the bottom of the history section.

5 Gateways status

To access the status of the gateways,

- In the menu, choose **Diagnostics > Gateways status**.

This page displays the current settings of the gateways, the number of bytes transmitted and the number of erroneous frames.

The screenshot shows the Etic administration web interface for a device named XSLAN+2220 (SHDSL.bis switch). The breadcrumb navigation is > Home > Diagnostics > Gateway status. A link for Serial data visualisation is visible. The page is divided into two sections: COM 1 gateway and COM 2 gateway. Each section lists various settings and statistics.

COM 1 gateway	
Enable gateway	Modbus Server
Serial port setup	9600-8-N-1
Characters sent on serial port	0
Characters received on serial port	0
Network frames sent	0
Received network frames	0
CRC/LRC errors	N/A
Slave timeout expired	0
Active connections count	0

COM 2 gateway	
Enable gateway	
Serial port setup	
Characters sent on serial port	N/A
Characters received on serial port	N/A
Network frames sent	N/A
Received network frames	N/A
CRC/LRC errors	N/A
Slave timeout expired	N/A
Active connections count	N/A

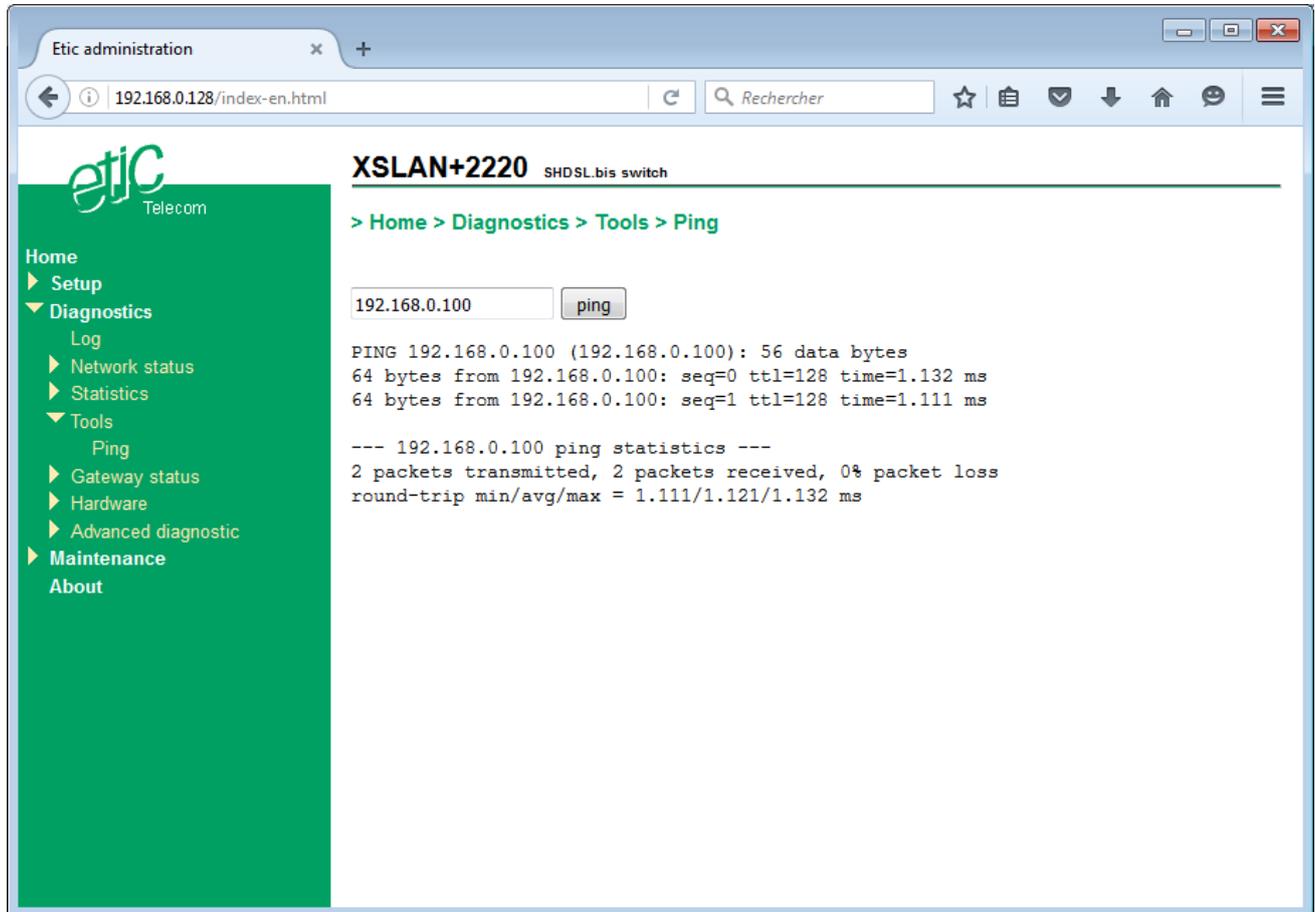
A Refresh button is located at the bottom of the page.

To analyze the RX and TX traffic on the serial link,

- Click **Serial data visualization**.

6 PING tool

This tool is used to send a "PING" frame from the product to a device on the network.



7 Line Cut Detection (LCD)

7.1 Overview

The XSMIL provides a built-in tool that can locate a cut of the cable and that will be very easy to use for a non-technical people.

This tool is based on a built-in feature of the SHDSL modem which is capable to measure the reflections on the copper line in order to tune the “echo canceler” function. This test cannot be performed when the SHDSL connection is established. The remote end should be disconnected, but this is actually the case when the cable is broken.

This tool is intended to detect a simple defect of the cable like a full cut or a full short circuit. Some over defects like a bad contact in a connector or a wire which is just half cut may not be detected. In this case, a TDR tester may be useful, with the help of a telecom specialist.

The accuracy will depend on the type of cable. A calibration will be necessary before using the LCD. If several types of cables are used on the same line, the accuracy will be reduced.

Using the LCD when the line is not cut will give unexpected result.

7.2 Launching the LCD tool

- In the menu, choose **Diagnostics > Tools > Line cut detection**.

The screenshot shows the XSMIL-FD4200 web interface. The top right corner displays 'XSMIL-FD4200'. The left sidebar contains a navigation menu with categories: Home, Setup (Ethernet and switching, IP protocol and routing, Alarms, Security, System), Diagnostics (Logs, Network status, Statistics, Tools), Hardware, Advanced diagnostic, Maintenance, and About. The 'Tools' sub-menu is expanded, showing 'Line cut detection' as the selected option. The main content area shows a breadcrumb trail: '> Home > Diagnostics > Tools > Line cut detection'. Below this, there is a horizontal menu with tabs for SH1, SH2, SH3, and SH4, with SH4 selected. The page title is 'SH4'. A diagram shows two modem icons connected by a line with a large blue question mark in the center, indicating a measurement. Below the diagram, the text 'no measure' is displayed. A dropdown menu shows 'cable: D10 Permanent' and a green 'start measure' button is located below it.

- Select the SH port and the type of cable
- Click **start measurement**

DIAGNOSTICS AND MAINTENANCE

The screenshot shows the etic TELECOM XSMIL-FD4200 web interface. The breadcrumb trail is > Home > Diagnostics > Tools > Line cut detection. The left sidebar contains a navigation menu with categories: Home, Setup, Diagnostics (Logs, Network status, Statistics, Tools), Hardware, Advanced diagnostic, Maintenance, and About. The 'Tools' sub-menu is expanded, showing Ping, Line cut detection, and Repeater discovery. The main content area displays 'SH2' and a diagram of two fiber optic cables connected by a line. A magnifying glass icon is positioned over the connection point. Below the diagram is a progress bar that is partially filled with green. The text 'measurement in progress...' is centered below the progress bar, and a green 'start measure' button is located at the bottom.

- Wait until the measurement is done (1m 30s)

The screenshot shows the etic TELECOM XSMIL-FD4200 web interface displaying the results of the 'Line cut detection' tool. The breadcrumb trail is > Home > Diagnostics > Tools > Line cut detection. The left sidebar is the same as in the previous screenshot. The main content area displays 'SH2' and a diagram of two fiber optic cables connected by a line. A large red 'X' is positioned over the connection point. Below the diagram, the text 'Defect at 592m' is displayed. A dropdown menu shows 'cable: D10 Permanent' and a green 'start measure' button is located at the bottom. A '> Expert' link is visible in the bottom left corner of the main content area.

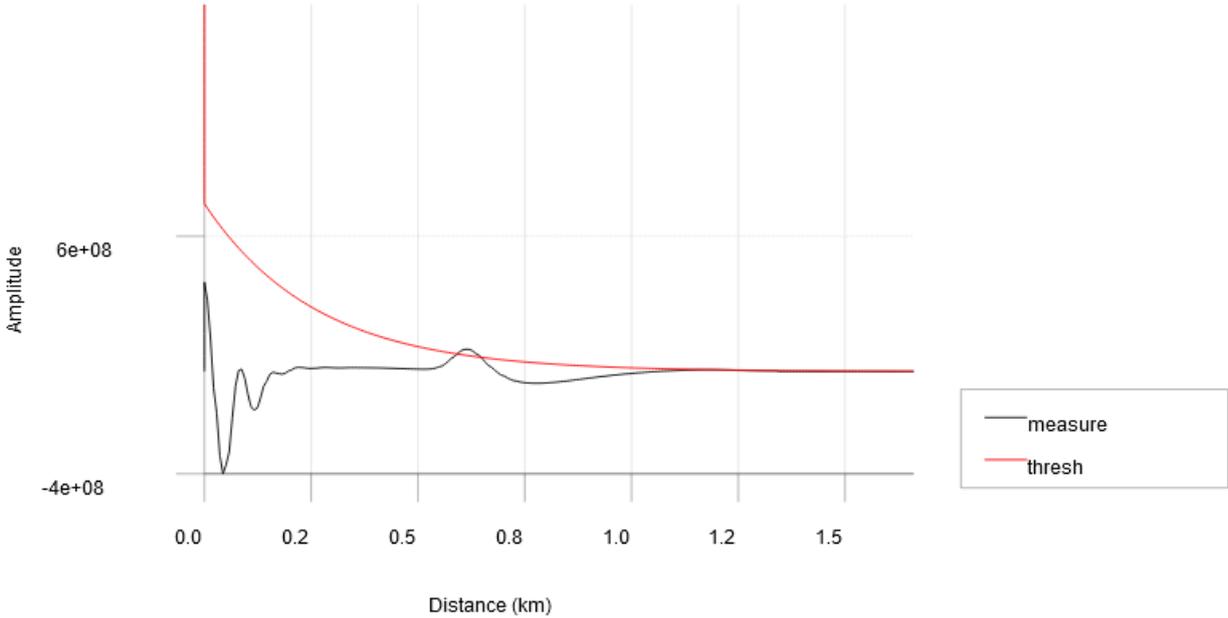
7.3 Advanced results

- Click **Expert**.

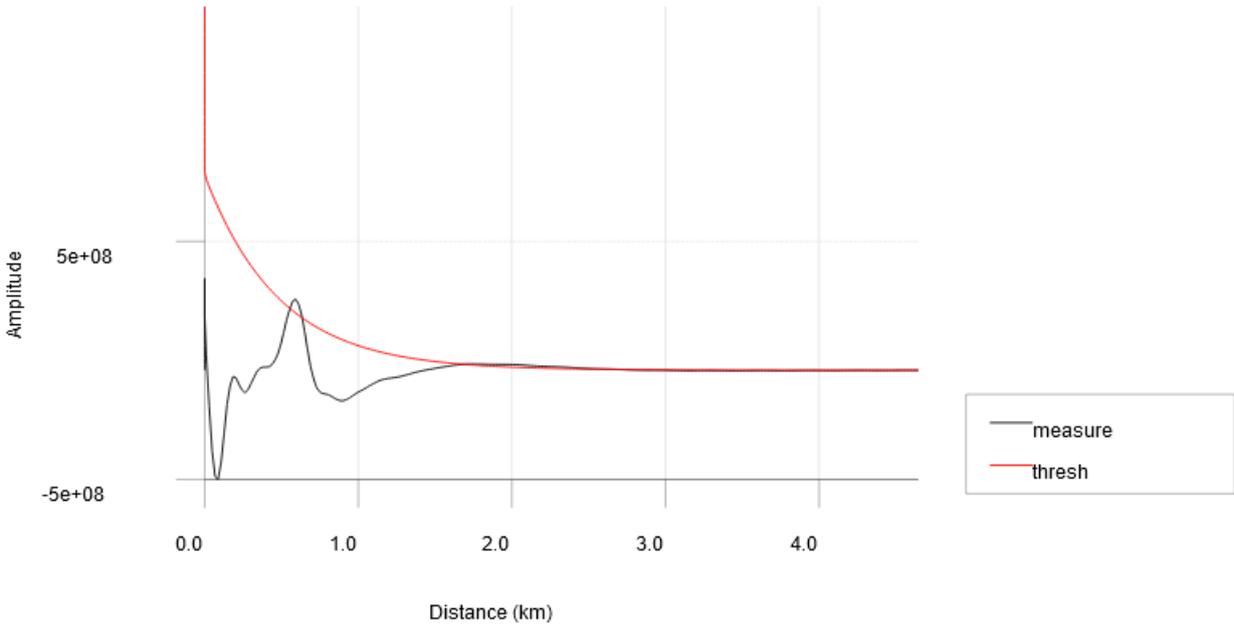
3 curves are displayed corresponding to the 3 measurements at different meter ranges.

These curves are intended for specialist people with knowledge of TDR (Time Domain Reflectometer) techniques.

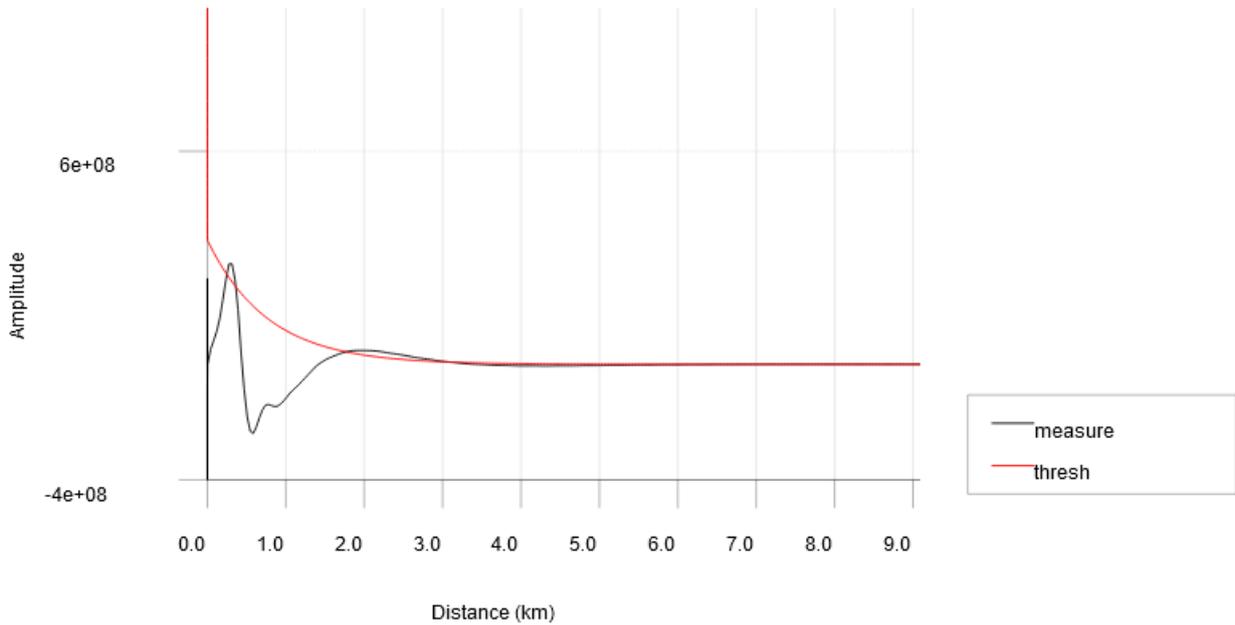
0-1.5km



0-2km



0-8km



7.4 Cable profile management

A cable profile consists of a file containing several parameters which were defined by a calibration process on real cable lengths. This calibration is performed by the technical ETIC team.

- In the menu, choose **Maintenance > LCD cable profiles**.

The screenshot shows the ETIC Telecom web interface. The top left corner features the ETIC TELECOM logo. The top right corner displays the device model 'XSMIL-FD4200'. Below the logo, there are links for 'Documentation | EN | FR'. The main navigation menu on the left includes 'Home', 'Setup', 'Diagnostics', and 'Maintenance'. The 'Maintenance' menu is expanded, showing options like 'Configurations management', 'LCD cable profiles', 'Firmware update', 'Secure erase', 'Notepad', 'Reboot', and 'About'. The main content area shows the breadcrumb navigation '> Home > Maintenance > LCD cable profiles'. Below this, there is a section titled 'Available profiles' containing a table with two columns: 'Profile name' and 'Comment'. The table lists two profiles: 'D10 BrandRex type' and 'D10 Permanent'. The 'D10 Permanent' profile has a comment 'HUZHOU PERMANENT CABLE CO. LTD'. Below the table, there are buttons for 'Show', 'Edit', 'Delete', 'Add ...', and a refresh icon. There are also navigation arrows on the right side of the table.

To add a cable profile from a PC,

- Click **Add...** .
- Then click **Browse** and then select the file provided by ETIC.
- Give a name and a comment to this cable profile and click **Save**.

8 Repeater Discovery (RD)

The aim of this feature is to provide a means to detect which part of the cable is broken (i.e. between which repeaters). This is useful when there are several repeaters in a daisy chain topology. This option works only in Repeater Mode.

A discovering protocol runs in background on each XSMIL-FD or XSMIL of a branch. The result is remotely displayed on a web page of the unit.

This option combined with the above Line Cut Detection feature (LCD) gives the capability to detect a cut in the cable whatever the number of repeaters installed (max 8).

To launch the Repeater Discovery tool,

- In the menu, choose **Diagnostics > Tools > Repeater Discovery**.
- Select the SH port and wait a few seconds until the result is displayed.

The screenshot displays the ETIC Telecom web interface. The top left features the ETIC TELECOM logo. The top right shows the unit identifier 'XSMIL-BP4200-IB'. Below the logo, there are links for 'Documentation | EN | FR'. A navigation menu on the left includes sections for 'Home', 'Setup', 'Diagnostics', 'Tools', 'Hardware', 'Advanced diagnostic', 'Maintenance', and 'About'. The main content area shows a breadcrumb trail: '> Home > Diagnostics > Tools > Repeater discovery'. Below this, there is a row of four buttons labeled 'SH1', 'SH2', 'SH3', and 'SH4', with 'SH1' selected. The results for 'SH1' are displayed as follows:

Port	Device	IP	MAC
SH1	XSMIL-BP4200-IB	192.168.0.128	00:0a:b4:00:86:b6
	XSMIL-FD4200	192.168.0.127	00:0A:B4:00:89:5E

DIAGNOSTICS AND MAINTENANCE

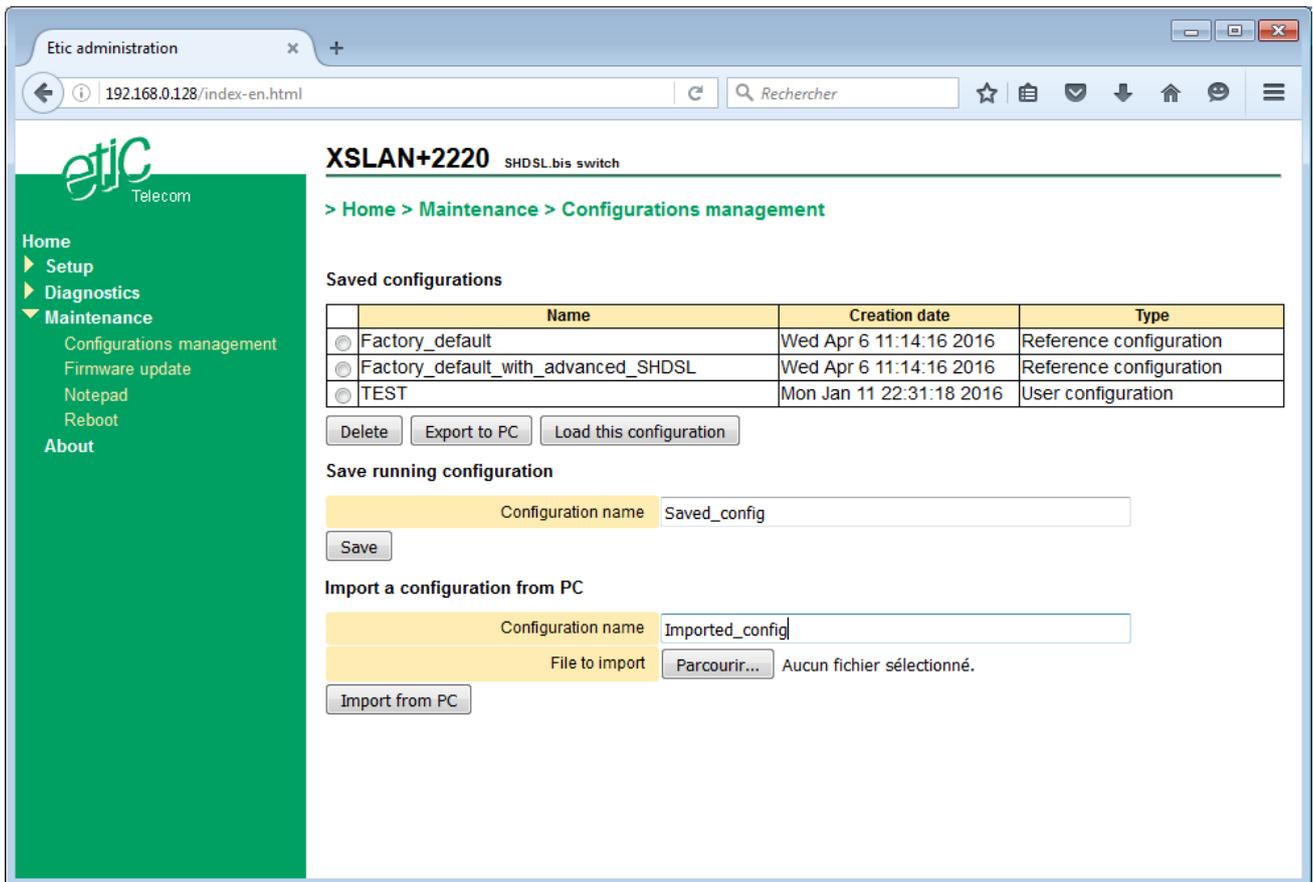
9 Saving and loading a configuration file

In each configuration page, the "Save" button is used to save the new settings. The configuration is saved in memory and takes effect immediately. If the XS switch reboot, the configuration is not lost ; This is the running configuration.

It is possible to save the running configuration to a file into the XS switch, or export it to a PC as an editable file.

Conversely, it is possible to load a configuration from the set of configurations stored in the XS switch or to import a configuration file stored in a PC.

- In the menu, choose **Maintenance > Configurations management**.



To save the running configuration to a file into the XS switch,

- In **Configuration name**, type a name for that configuration.
- Click on **Save**.

The configuration is added to the table **Saved configurations**.

To load a configuration from the list as the running configuration,

- Select the configuration in the list and click **Load this configuration**.

To export the running configuration to a file (.txt) into a PC ,

- First save the running configuration to a file in the XS switch as previously stated.
- Then select in the list the configuration to export and click **Export to a PC**.

To import a configuration file from a PC,

- Click on « **Browse** » then select the file (XXX.txt) to import.
- Optionally change the name of the configuration and click **Import from PC**. This configuration appears in the **Configurations saved** list.
- Select this configuration in the list and click on **Load this configuration** ; it becomes the running configuration.

Warning : A configuration file can only be downloaded to an XS switch having the same firmware version.

10 Updating the firmware

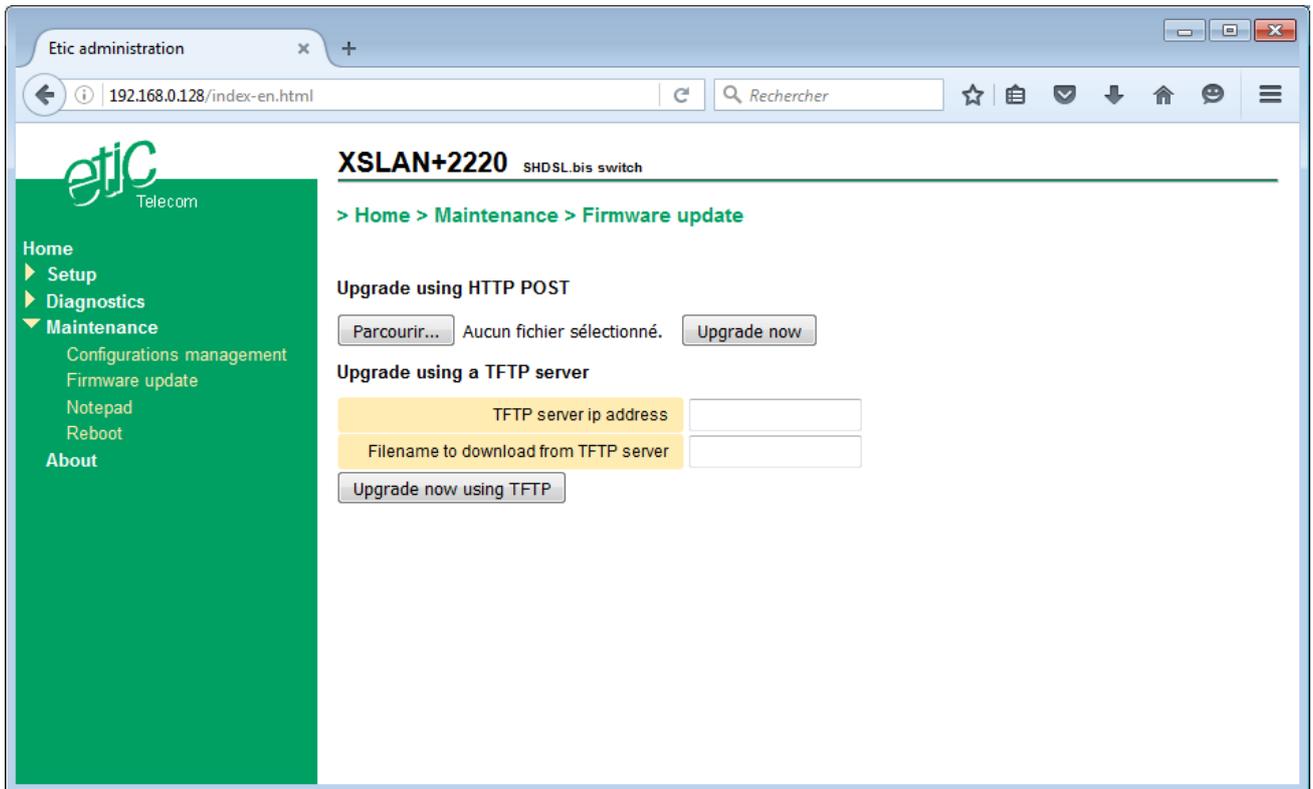
It is usually performed via the Ethernet port or remotely, via the SHDSL link. The update does not change the setting of the XS switch.

If the update is done remotely, verify that the new firmware version is compatible with the current setting to insure that the SHDSL link will go up automatically after the update.

The update can be done in two ways :

If the updated firmware file is accessible from the user's PC, it can be done directly with the browser using HTTP POST.

The update can also be done via a TFTP server there the updated firmware file has to be previously loaded.



To perform the firmware update using HTTP POST,

- In the menu, choose **Maintenance > Firmware update**.
- Select the new firmware file.
- Click **Update now**.

After a few seconds, the RUN LED  blinks red.

Wait about 5 minutes and then check that the update is done (**About** item in the menu).

ANNEX 1 : SNMP MIB

1 Purpose of the document

This document describes the MIBs and the OIDs supported by the XS devices manufactured by ETIC Telecom.

2 Accessible OIDs and MIBs

2.1 Supported MIBs

The OIDs used are standard and located under iso.org.dod.internet.mgmt.mib-2.

It is only possible to read information, not to write it. The SET command is not supported.

The SNMP agent functionality in the XS device is provided by the Net-SNMP software package (<http://www.net-snmp.org>). A lot of common MIBs are implemented by this package. In addition to these MIBs, a few more specific MIBs are supported.

The common MIBs supported include the following :

- RFC1213-MIB (MIB-2)
- HOST-RESOURCES-MIB
- IF-MIB
- IP-MIB

These will not be documented here unless there is something specific in the implementation in the XS devices.

The specific MIBs are :

- HDLSL2-SHDSL-LINE-MIB
- BRIDGE-MIB
- RSTP-MIB

These will be described in detail because they are not implemented by default in Net-SNMP.

ANNEX 1

2.2 Network interface indexes

All the SNNP tables that deal with network interfaces are indexed with the network interface index. In the XS software versions greater or equal to 2.0.0, the indexes are :

Interface name	Internal name	Index
LAN1	lan1	11
LAN2	lan2	10
LAN3	lan3	9
LAN4	lan4	8
SHDSL1	sh1	15
SHDSL2	sh2	12
SHDSL3	sh3	14
SHDSL4	sh4	13

The interface index will not change for a given software version even after configuration changes and reboots. However, they are subject to change after changing the firmware.

2.3 Querying the MIB

To query the MIB of the device and see what OID can be useful, the tools from the Net-SNMP project can be used. They can be installed on an Unix like operating system such as Linux or a BSD variant. They can also be installed on Windows using Cygwin.

To use them, start a shell in a terminal window and test these commands :

This command will return all OIDs supported by the device.

```
mc@ubuntu:~$ snmpwalk -v1 -c public 192.168.0.128
SNMPv2-MIB::sysDescr.0 = STRING: ETIC Telecom XSLAN+4400 SHDSL switch, firmware
version v2.1.0-b2
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (26205510) 3 days, 0:47:35.10
SNMPv2-MIB::sysContact.0 = STRING: www.etictelecom.com
SNMPv2-MIB::sysName.0 = STRING: XS+
...
```

This command queries one OID.

```
mc@ubuntu:~$ snmpget -v1 -c public 192.168.0.201 IF-MIB::ifName.8
IF-MIB::ifName.8 = STRING: lan4
```

This command translates the name of an OID to its numeric representation.

Note that the MIB file must be installed somewhere where Net-SNMP can find it.

```
mc@ubuntu:~$ snmptranslate IF-MIB::ifName.8 -On
.1.3.6.1.2.1.31.1.1.1.1.8
```

Table display : SNMP tables can be displayed with this command :

```
mc@ubuntu:~$ snmptable -v1 -c public 192.168.0.201 IF-MIB::ifTable
SNMP table: IF-MIB::ifTable
...
```

3 Description of the supported OIDs

3.1 Sysdesc, Syslocation, SysName

- OID SNMPv2-MIB::sysDescr.0 : Type of product and firmware version
- OID SNMPv2-MIB::sysLocation.0 : Parameter "syslocation" in the web page
- OID SNMPv2-MIB::sysName.0 : Parameter "sysname" in the web page

3.1.1 Example

```
mc@ubuntu:~$ snmpget -v1 -c public 192.168.0.201 SNMPv2-MIB::sysName.0
SNMPv2-MIB::sysName.0 = STRING: XS+
mc@ubuntu:~$ snmpget -v1 -c public 192.168.0.201 SNMPv2-MIB::sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: ETIC Telecom XSLAN+4400 SHDSL switch, firmware
version v2.1.0-b2
```

3.2 Network interfaces table (IF-MIB::ifTable)

List of the network interfaces of the device.

The XS can have up to 8 Ethernet interfaces :

- 4 10/100BASE-T Ethernet ports,
- 4 SHDSL 2BASE-TL ports.

The interfaces are named :

- lan1, lan2, lan3, lan4 for the 10/100BASE-T interfaces (from 1 to 4)
- sh1, sh2, sh3, sh4 for the SHDSL interfaces (from 1 to 4).
- The br_lan and br_sh interfaces are Linux bridge interfaces. They allow Ethernet bridging between the ports of the device.

In this table there are a few particularities :

- OID IF-MIB::ifAdminStatus : Display the administrative state of the interface.
- Warning : For the SHDSL ports, the value ifAdminStatus is « up » when the connection is established, and « down » otherwise.
- OID IF-MIB::ifOperStatus : Is « up » when a connection is established, or « down » when there is no connection. This is true for the SHDSL and LAN ports.
- OID ifIndex : Index of the interface, used in many tables of the product.
- OID ifSpeed : Data rate of the interface. Note: for the SHDSL ports, this value is always 100Mb/s.

3.2.1 Example

```
mc@ubuntu:~$ snmptable -v1 -c public 192.168.0.201 IF-MIB::ifTable
SNMP table: IF-MIB::ifTable
...
```

ANNEX 1

3.3 SHDSL MIB (HDSL2-SHDSL-LINE-MIB)

This MIB contains information relative to the SHDSL connections. It is published by the IETF in RFC4319.

3.3.1 Table HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrTable :

This table contains information about how the line is working.
At least the Attenuation and SNR margin should be monitored.

The attenuation gives an indication about the length of the line and the insertion losses of the connectors.
The SNR margin tells how much noise the receiving modem can bear without causing transmission errors or disconnects.

The number of erroneous seconds should also be monitored. It indicates the availability of the line. A number near zero indicates a noise free operation. A high number indicates noise or signal distortion somewhere on the line. Usual causes include crosstalk, inadequate surge protectors and EMI disturbances caused by other equipment.

- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn: Line attenuation
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrSnrMgn: SNR margin
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointrrActivationState: Line status, connected or not (Warning, the other fields are invalid when this parameter value is not « data »)
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCRCAnomalies: CRC errors on the line
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointLOSWS: Seconds with one or more synchronization loss
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointES: Erroneous seconds. A second is « erroneous » if there are one or several CRC errors or synchronization loss
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointSES: Severely erroneous seconds . A second is « severely erroneous » if there are at least 50 CRC errors or one or several synchronization loss.
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointUAS: Unavailable seconds. A second is « unavailable » after 10 consecutive severely erroneous seconds. It is necessary to have 10 seconds with no « severely erroneous » seconds to leave this state.

For more information, refer to ITU-T standard G.991.2 (G.SHDSL.bis).

The other fields are not supported.

Example

```
mc@ubuntu:~$ snmpwalk -v1 -c public 192.168.0.201 HDSL2-SHDSL-LINE-
MIB::hds12ShdslEndPointCurrTable
HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn.12.0.networkSide.wirePair1 =
INTEGER: 0 dB
HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn.13.0.networkSide.wirePair1 =
INTEGER: 0 dB
HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn.14.0.networkSide.wirePair1 =
INTEGER: 0 dB
HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn.15.0.networkSide.wirePair1 =
INTEGER: 0 dB
...
```

Numeric OIDs

Replace “ifindex” with the SHDSL interface index in the table below.

hdl2ShdslEndpointCurrAtn	.1.3.6.1.2.1.10.48.1.5.1.1.ifindex.0.1.1
hdl2ShdslEndpointCurrSnrMgn	.1.3.6.1.2.1.10.48.1.5.1.2.ifindex.0.1.1
hdl2ShdslEndpointCurrStatus	.1.3.6.1.2.1.10.48.1.5.1.3.ifindex.0.1.1
hdl2ShdslEndpointES	.1.3.6.1.2.1.10.48.1.5.1.4.ifindex.0.1.1
hdl2ShdslEndpointSES	.1.3.6.1.2.1.10.48.1.5.1.5.ifindex.0.1.1
hdl2ShdslEndpointCRCAnomalies	.1.3.6.1.2.1.10.48.1.5.1.6.ifindex.0.1.1
hdl2ShdslEndpointLOSWS	.1.3.6.1.2.1.10.48.1.5.1.7.ifindex.0.1.1
hdl2ShdslEndpointUAS	.1.3.6.1.2.1.10.48.1.5.1.8.ifindex.0.1.1

3.3.2 Table HDSL2-SHDSL-LINE-MIB::SpanStatusTable

- OID hdl2ShdslStatusActualLineRate (.1.3.6.1.2.1.10.48.1.2.1.3.ifindex) : data rate of the SHDSL line. It is recommended to monitor this OID, if the chosen profile for the line is not a fixed datarate profile.

The other fields are not supported and are set to 0.

3.3.3 Table HDSL2-SHDSL-LINE-MIB::SpanConfProfileTable

This table gives the list of the profiles defined for the SHDSL links configuration. These informations are the same as the ones in the web page « SHDSL ports »

3.3.4 Table HDSL2-SHDSL-LINE-MIB::SpanConfTable

This table gives the SHDSL profile associated with each SHDSL port.

3.4 MIB : BRIDGE-MIB::dot1dBridge

Information about the Ethernet bridge are gathered under this OID. This MIB is published by the IETF under RFC4188.

3.4.1 OID BRIDGE-MIB::dot1dBase

The following information is displayed :

- OID BRIDGE-MIB::dot1dBaseBridgeAddress : Bridge MAC address
- OID BRIDGE-MIB::dot1dBaseNumPorts : Number of ports in the bridge
- OID BRIDGE-MIB::dot1dBaseType : Type of bridge (Tranparent-only)

ANNEX 1

3.4.2 Table BRIDGE-MIB::dot1dBasePortTable :

This table provides details of the bridge ports. Throughout the BRIDGE-MIB, ports are referenced by number. This table associates a bridge port number with ifIndex (network interface number).

- OID dot1dBasePort : Port number
- OID dot1dBasePortIfIndex : Port index in the ifTable table
- OID dot1dBasePortCircuit : Always 0
- OID dot1dBasePortDelayExceededDiscards : Not supported
- OID dot1dBasePortMtuExceededDiscards : Not supported

3.4.3 OID BRIDGE-MIB::dot1dTp

This oid gathers information on transparent bridges (= Ethernet switches).

3.4.4 Table BRIDGE-MIB::dot1dTpFdbTable

This table contains the MAC address table learned by the product.

- OID dot1dFdbAddress : MAC address learned by the switch
- OID dot1dFdbPort : Which port to send a frame with the destination MAC address above.
- OID dot1dFdbStatus : the state of the entry in the table: learned or fixed.

This table allows you to draw a "map" of the network and equipment connected to it.

3.4.5 RSTP and STP

The RSTP and STP system can be polled with the standard MIBs BRIDGE-MIB and RSTP-MIB. The RSTP-MIB is published by the IETF in RFC4318.

ANNEX 2 : SHDSL data rate versus distance

The table below shows the data rate which is possible to get on a SHDSL link depending on the wire diameter and the distance.

These values are indicative in noise free environment.

Data rate	192Kb/s	1,2Mb/s	2,3Mb/s	5,7 Mb/s	6.7 Mb/s	10 Mb/s	12 Mb/s	15 Mb/s
Distance (Ø 0.9 mm) *	13 km	8 km	6 km	3.7 km	2.5 km	1.5 km	1 km	0.7 km
Distance (Ø 0.4 mm) *	7 km	4 km	3 km	2 km	1.3 km	0.9 km	0.6 km	0.4 km

ANNEX 3 : XSLAN and XSLAN+ switches compatibility

This annex concerns first-generation XSLANs (2005-2012). These products conformed to the Shdsl standard at 2.3 Mb/s, while the following families conform to the Shdsl.bis standard at 5.7 Mb/s.

A XSLAN switch and a XSLAN+ switch can interwork through a twisted pair.

The firmware version of the XSLAN+ switch must be later than V1.3.2.

1/ Case 1 : XSLAN is a STU-R (NTU)

Compatibility between a XSLAN switch and a XSLAN+ switch is guaranteed unconditionally.

The XSLAN+ switch must be configured with the "STU-C, Standard" profile or with a fixed data rate profile. In this case the data rate must be less than or equal to 2304 Kb/s.

2/ Case 2 : XSLAN is a STU-C (LTU)

Compatibility between a XSLAN switch and a XSLAN+ switch is only guaranteed if the XSLAN firmware version is at or later than V2.20.

The data rate must be at least 192 kb/s.

The XSLAN+ switch must be configured with the "STU-R, Auto" profile.



405 rue Lavoisier
38330 Montbonnot Saint Martin
France

Tel : +33 (0)4 76 04 20 00
contact@etictelecom.com

www.etictelecom.com