TELINDUS®

Telindus 1420 SHDSL Router

Telindus 1420 SHDSL Router

USER AND REFERENCE MANUAL

Version: 1.2 181363

Telindus Technical Publications – Geldenaaksebaan 335 - B-3001 Leuven - Belgium – Tel. +32 16 382011

Document properties

Subject	Telindus 1420 SHDSL Router
Manual type	User and reference manual
Version	1.2
Code	181363
Modification date	22 October 2002 ©Telindus

Copyright notice

This equipment, for safety and hygiene purposes, complies with the specific provisions contained in ARAB/RGPT 54 quater 3.1 (RD 20 06 1975, Art.1, Section X, Accident Prevention Policy).

Safety requirements

The interfaces of the Telindus 1420 SHDSL Router should only be connected to the following circuit types:

Interface	Connector	Circuit type
LAN interface	RJ45	SELV
line interface	RJ12	TNV-1
management interface	subD-9	SELV

Carefully read the safety instructions at the beginning of 2 - Installing and connecting the Telindus 1420 SHDSL Router on page 17.

Statements

http://www.telindus.com/accessproducts → Products → Choose a product → Download certificates

Hereby, Telindus declares that this Telindus 1420 SHDSL Router complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Hierbij verklaart Telindus dat deze Telindus 1420 SHDSL Router overeenstemt met de essentiële vereisten en andere relevante bepalingen van Richtlijn 1999/5/EC.

Par la présente, Telindus déclare que ce Telindus 1420 SHDSL Router est en conformité avec les exigences essentielles et autres articles applicables de la Directive 1999/5/EC.

Hiermit, Telindus erklärt daß dieser Telindus 1420 SHDSL Router in Fügsamkeit ist mit den wesentlichen Anforderungen und anderen relevanten Bereitstellungen von Direktive 1999/5/EC.

Mediante la presente, Telindus declara que el Telindus 1420 SHDSL Router cumple con los requisitos esenciales y las demás prescripciones relevantes de la Directiva 1999/5/CE.

A Telindus declara que o Telindus 1420 SHDSL Router cumpre os principais requisitos e outras disposições da Directiva 1999/5/EC.

Col presente, Telindus dichiara che questo Telindus 1420 SHDSL Router è in acquiescenza coi requisiti essenziali e stipulazioni attinenti ed altre di Direttivo 1999/5/EC.

Με το παρον, η Telindus δηλωνει οτι αυτο το Telindus 1420 SHDSL Router ειναι συμμορφουμενο με τιζ βασικεζ απαιτησειζ και με τιζ υπολοιπεζ σχετικεζ διαταξειζ τηζ οδηγιαζ 1999/5/EC.

Organisation of this manual

This manual contains the following main parts:

Part	This part …
User manual	shows you how to install and connect the Telindus 1420 SHDSL Router. It also contains the basic configuration information.
Reference manual	gives more detailed information on the Telindus 1420 SHDSL Router. It contains a complete description for look up purposes.
Annexes	gives additional information.

User manual

The following table gives an overview of the user manual:

Chapter	This chapter …
1	introduces the Telindus 1420 SHDSL Router.
2	explains how to install and connect the Telindus 1420 SHDSL Router. It also describes the front panel LED indicators.
3	shows the position of the DIP switches and straps on the Telindus 1420 SHDSL Router motherboard, and reveals their function.
4	describes how to start a Telindus Maintenance Application (TMA) session on the Telindus 1420 SHDSL Router. Further, it introduces the management attributes of the Telindus 1420 SHDSL Router.
5	teaches you the basics to configure the Telindus 1420 SHDSL Router.
6	presents some practical examples of Telindus 1420 SHDSL Router configurations.
7	can be of help in case you have trouble connecting to or configuring the Telindus 1420 SHDSL Router.

Reference manual

The following table gives an overview of the reference manual:

Chapter	This chapter …
8, 9, 10, 11	describes the configuration, status, performance and alarm attributes, respectively.
12	displays and labels the different elements of the Telindus Maintenance Application subsystem picture.
13	explains the auto install procedure. It is in this chapter that BootP, DHCP and TFTP is explained.
14	gives a firmware download procedure.
15	summarises the technical specifications of the Telindus 1420 SHDSL Router.

Annexes

The following table gives an overview of the annexes:

Chapter	This annex …
Annex A:	lists common TCP and UDP numbers.
Annex B:	shows ordering information.

Firmware version

This manual describes the features, containment tree and attributes of the Telindus 1420 SHDSL Router firmware version T2723/01500.

Typographical conventions

The following typographical conventions are used in this manual:

The format ...	indicates ...
Normal	normal text.
Italic	• new or emphasised words • application windows, buttons and fields. E.g. In the *File name* field enter ...
`Computer`	text you have to enter at the DOS or CLI prompt, computer output and code examples. E.g. `NOK,1,1,Invalid command`.

`Computer Bold`	text you have to enter at the DOS or CLI prompt when it is part of a mix of computer input and output.
	E.g.
	`/o1003:"Edit Configuration"`
	`>`**`get sysName`**
	`  sysName = "Orchid 1003 LAN"`
	`/o1003:"Edit Configuration"`
	`>`

Narrow	containment tree objects and attributes of a device when they are mentioned in the normal text. I.e. when they are not a part of computer input or output. E.g. Use the sysName attribute in order to ...
Blue	references to other parts in the manual. E.g. For more information, refer to Chapter xx - Technical specifications.
Blue underline	a hyperlink to a web site. E.g. http://www.telindus.com

Graphical conventions

The following icons are used in this manual:

Icon	Name	This icon indicates …
	Remark	remarks or useful tips.
	Caution	text to be read carefully in order to avoid damage to the device.
	Warning	text to be read carefully in order to avoid injury.
	DIP switch	a DIP switch or strap table.
	Basic attribute	a basic attribute in the containment tree of the Telindus 1420 SHDSL Router.
	Advanced attribute	an advanced attribute in the containment tree of the Telindus 1420 SHDSL Router.
	Action	an action in the containment tree of the Telindus 1420 SHDSL Router.

Audience

This manual is intended for computer-literate people, who have a working knowledge of computing and networking principles.

Your feedback

Your satisfaction about this purchase is an extremely important priority to all of us at Telindus. Accordingly, all electronic, functional and cosmetic aspects of this new unit have been carefully and thoroughly tested and inspected. If any fault is found with this unit or should you have any other quality-related comment concerning this delivery, please submit the Quality Comment Form on our web page http://www.telindus.com/accessproducts.

Table of contents

User manual

1 Introducing the Telindus 1420 SHDSL Router

This chapter gives an introduction to the Telindus 1420 SHDSL Router. The following gives an overview of this chapter:

1.1 The Telindus 1420 SHDSL Router

The Telindus 1420 SHDSL Router is an S-HDSL baseband modem with a built-in IP router.

Power requirements

The Telindus 1420 SHDSL Router requires 9 Vdc as input voltage. Using different power adapters, the Telindus 1420 SHDSL Router can be powered with -48 Vdc, 115 Vac or 230 Vac.

Physical interfaces

The Telindus 1420 SHDSL Router has three physical interfaces:

- a LAN interface (LAN). This is a 10 Mbps TPI Ethernet interface.
- a line interface (LINE). The S-HDSL line interface supports speeds up to 2.3 Mbps.
- an auxiliary interface (AUX). This interface can be used to serially connect TMA, or using any terminal emulation program also ATWIN and CLI. For (serial) firmware downloads, TML is used.

Self-test

The Telindus 1420 SHDSL Router does a complete self-test during power-up.

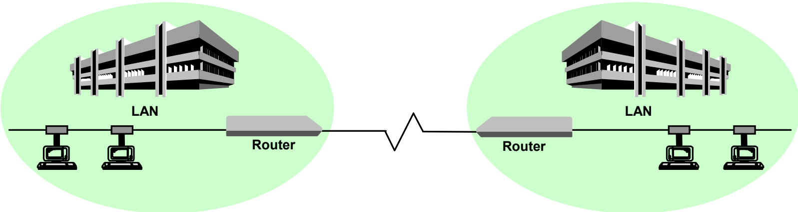
1.2 Telindus 1420 SHDSL Router applications

The Telindus 1420 SHDSL Router allows the direct connection of 10-BaseT Ethernet LANs via a WAN. It routes IP traffic and encapsulates it in PPP, Frame Relay, HDLC on the WAN link.

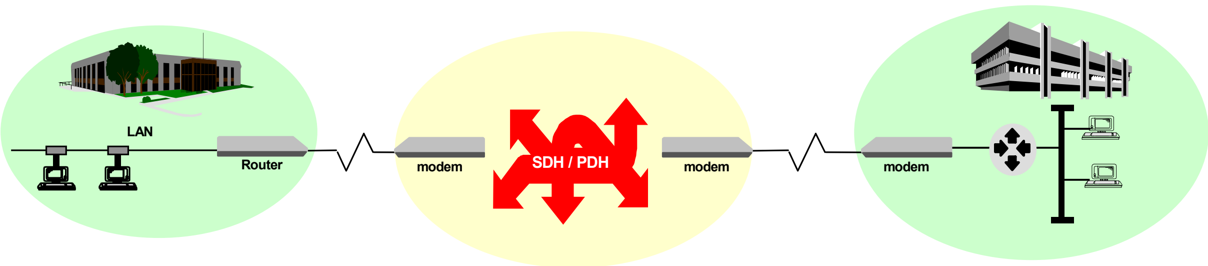
The product can be used to implement:

- LAN to LAN connection over a galvanic copper line or fibre line,
- LAN extension over a PDH or SDH backbone,
- LAN extension over a Frame Relay network,
- LAN to Internet connection.

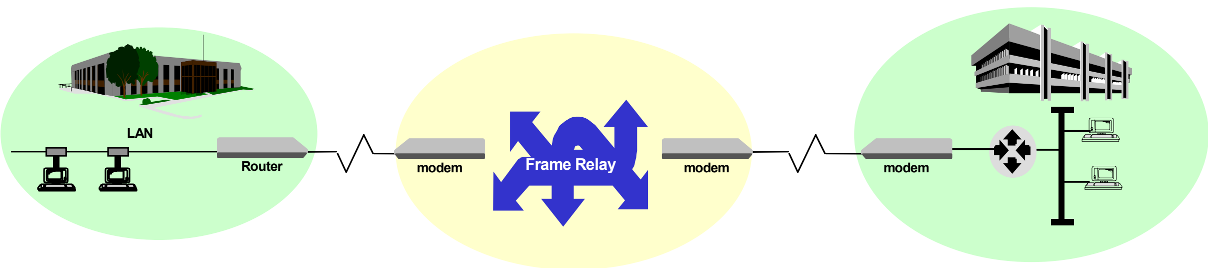
Point-to-point LAN interconnection



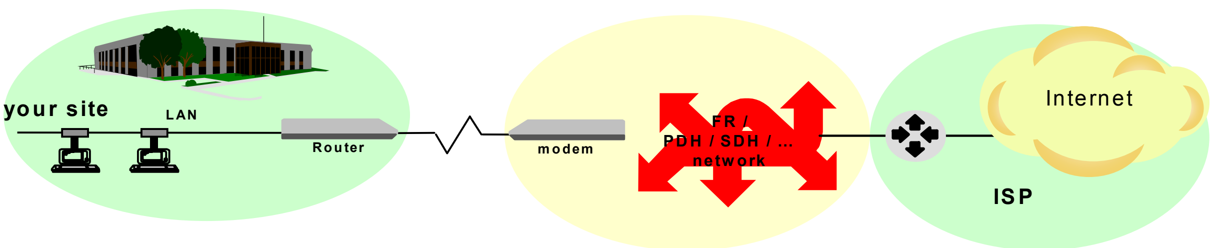
LAN extension over a PDH or SDH backbone



LAN extension over a Frame Relay network



LAN to Internet connection



1.3 WAN protocols

The Telindus 1420 SHDSL Router supports several encapsulation protocols on its WAN interface. These are introduced in this section.

The following gives an overview of this section:

1.3.1 Frame Relay

Frame Relay is suited for high-speed lines with a low error rate, as on baseband lines with Crocus modems. IP traffic is encapsulated in Frame Relay using the techniques described in RFC1490 (FRAD). Since Frame Relay networks use typically dedicated lines, only Permanent Virtual Circuits (PVCs) on dedicated lines are supported.

The Telindus 1420 SHDSL Router supports the Frame Relay Local Management Interface (LMI). Compliance with LMI revision 1, ANSI T1.617 D and CCITT can be selected. Several LMI parameters are configurable.

Dynamic mapping between IP addresses and DLCIs is based on the Inverse ARP protocol. It allows the Telindus 1420 SHDSL Router to discover the IP address of a remote gateway associated with a virtual circuit. Inverse ARP creates dynamic address mappings in contrast with mappings that are statically configured. Inverse ARP is always enabled.

The Telindus 1420 SHDSL Router supports multiple DLCIs over its Frame Relay interface.

1.3.2 PPP

The Point to Point Protocol (PPP) is the standard protocol for LAN to LAN connections over a dedicated line. PPP features link monitoring and CHAP authentication.

If link monitoring is enabled, the Telindus 1420 SHDSL Router sends a monitor request packet over the line at regular intervals. The peer router should answer them to indicate the link is still OK. If on several consecutive requests no reply is received, the PPP link is disconnected. In that case, the PPP handshake starts again.

CHAP is an authentication protocol to secure the WAN link. CHAP authentication is supported with clear passwords and with the MD5 hashing algorithm.

1.3.3 HDLC

High-level Data Link Control (HDLC) encapsulation means that the Ethernet frames are put in an HDLC frame without any additional encapsulation (such as Frame Relay or PPP). This means that there is no protocol which monitors the status of the link, but it also means that there is no encapsulation overhead.

Because the Ethernet frames are directly encapsulated, only bridging is possible.

Important remark

The HDLC encapsulation on the Telindus 1420 SHDSL Router is compatible with the HDLC encapsulation on the Crocus Bridge interface. It is however not compatible with the Cisco HDLC encapsulation.

1.4 Routing

The Telindus 1420 SHDSL Router supports IP routing using static routes and the RIP version 2 routing protocol. Simple access lists can be applied on both the LAN and the WAN interfaces.

NAT and PAT

Network Address Translation (NAT) and Port Address Translation (PAT) are supported. These are two features that help solve the lack of official IP version 4 addresses. They are also known as IP masquerading.

Address translation	Description
NAT	NAT allows the use of private IP addresses on the local Ethernet, while still having access via the WAN interface to the Internet (official IP addresses). Each Ethernet IP address that needs Internet access is translated into an official IP address before sending traffic on the WAN interface. The number of simultaneous users with Internet access is limited to the number of official IP addresses. This is a dynamic process.
PAT	PAT uses only one single official IP address on the WAN network. The Telindus 1420 SHDSL Router translates all private IP addresses on the local Ethernet to the single official IP address. Only outgoing TCP sessions are supported.
NAT and PAT	You can combine both translation methods and tune them to specific needs.

Instead of using official IP addresses on the WAN and private IP addresses on the LAN, you can also do the opposite: private IP addresses on the WAN and official IP addresses on the LAN.

1.5 Bridging

The Telindus 1420 SHDSL Router can be configured to act as a bridge. This enables you to split up your LAN network into smaller parts or segments. This decreases the amount of data traffic on the separated LAN segments and, consequently, increases the amount of available bandwidth.

Self-learning and TST principle

You can configure the Telindus 1420 SHDSL Router so that it either uses the …

- self-learning principle
- self-learning principle in conjunction with the Transparent Spanning Tree algorithm.

Bridging principle	Description
self-learning	The bridge itself learns which data it has to forward to the other LAN segment and which data it has to block. I.e. it builds its own bridging table. In other words, you yourself do not have to configure a bridging table with MAC addresses of stations that are located on the separated LAN segments but that have to be able to communicate with each other.
self-learning + TST	This is based on the self-learning principle, but a protocol is used to implement the TST algorithm. **Bridging loops** The primary goal of this algorithm is to avoid that bridging loops arise. A bridging loop occurs when two self-learning bridges are placed in parallel. This results in data that keeps circling around as each bridge forwards the same data. **The TST algorithm** Using the TST algorithm, bridges know of each others existence. By communicating with each other, they establish one single path for reaching any particular network segment. If necessary, they may decide to disable some bridges in the network in order to establish this single path. This is a continuous process. So if a bridge fails, the remaining bridges will reconfigure their bridging tables keeping each LAN segment reachable.

1.6 Layer 2 tunnelling

What is the Layer 2 Tunnelling Protocol?

The Layer 2 Tunnelling Protocol (L2TP) is a protocol used for connecting VPNs (Virtual Private Networks) over public lines.

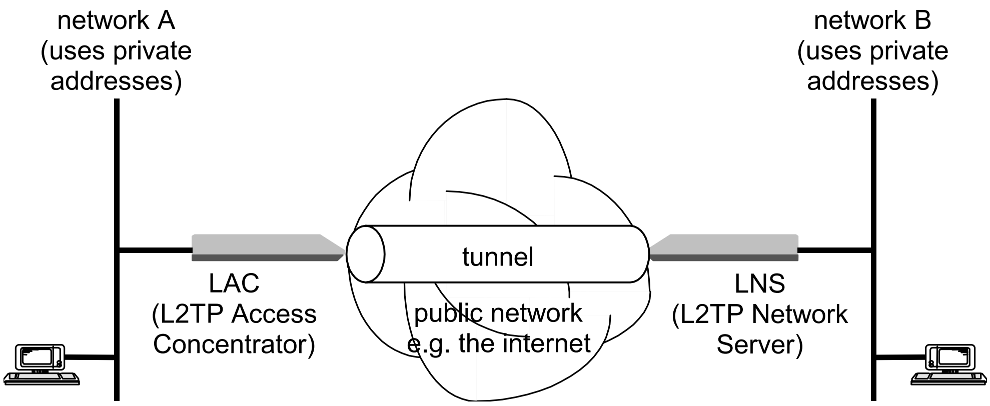
More specific, it allows you to set up virtual PPP connections. In other words, an L2TP tunnel simulates an additional PPP interface which directly connects two routers with each other.

L2TP - concrete

Concrete, using the Layer 2 Tunnelling Protocol you can connect several private and physically dispersed local networks with each other over public lines (such as the Internet) in order to create one big (virtual) local network. This without the need for address translation.

Example

In the following example, network A is virtually connected to network B through a tunnel in the public network:



1.7 Auto install

The Telindus 1420 SHDSL Router supports a number of features that allow it to be auto-installed, either over its Ethernet interface or over the WAN interface.

Automatically obtaining an IP address

If no IP address is configured on the LAN interface, the Telindus 1420 SHDSL Router sends BootP requests on its LAN interface to obtain an IP address from a BootP server.

If connected to a Frame Relay network, the Telindus 1420 SHDSL Router learns its DLCI number via LMI status messages. If no IP address is configured on both the LAN and WAN interfaces, it sends BootP requests over this DLCI. If the remote router is a Cisco router or another Telindus 1420 SHDSL Router, it acts as a BootP server and returns the IP address.

If connected over a PPP link and no IP address is configured on both the LAN and WAN interfaces, the Telindus 1420 SHDSL Router learns its IP address from the IPCP handshake.

TFTP configuration

Once an IP address is assigned, the Telindus 1420 SHDSL Router is reachable for further configuration. Alternatively it may retrieve its full configuration from a TFTP server.

Using the IP address assignment over the WAN link, installation of a Telindus 1420 SHDSL Router on a remote location is plug and play. It can be completely prepared and managed from a central site.

1.8 Management tools

The Telindus 1420 SHDSL Router is manageable in many different ways. This section gives a quick overview of the various management possibilities.

Management tool	**Description and reference**
TMA	TMA (Telindus Management Application) is a free Windows® software package that enables you to manage the Telindus products completely. I.e. to access their configuration attributes and look at status, performance and alarm information. For more information, refer to 4 - Managing the Telindus 1420 SHDSL Router on page 37 and the TMA manual.
TMA for HP OpenView	TMA for HP OpenView is the management application that runs on the widely spread network management platform HP OpenView. It offers the combination of the easy to use graphical interface of the stand-alone version of TMA, together with the advantages and features of HP OpenView. For more information, refer to the TMA for HP OpenView manual.
TMA CLI	TMA CLI (TMA Command Line Interface) enables you to use its commands in scripts in order to automate management actions. This is particularly useful in large networks. TMA CLI is a complementary product to TMA and TMA for HP OpenView. For more information, refer to the TMA CLI manual.
ATWIN	ATWIN is a menu-driven user interface. You can read and change all attributes as with TMA, but in a more basic, textual representation using a VT100 terminal. For more information, refer to the Maintenance Tools manual.
CLI	CLI is also a Command Line Interface, although not so extensive as TMA CLI. Experienced users who are familiar with the syntax can access the Telindus devices more quickly than with TMA or ATWIN. For more information, refer to the Maintenance Tools manual.
Web Interface	The Web Interface is an ATWIN alike menu-driven user interface. You can read and change all attributes as with TMA, but in a more basic representation using a web browser. For more information, refer to the Maintenance Tools manual.
EasyConnect terminal	Connecting the Telindus EasyConnect hand-held terminal through the auxiliary connector to the Telindus 1420 SHDSL Router, allows you to manage the Aster 5 in a basic way using the LCD display and keyboard. This is called keyboard management. For more information, refer to the Maintenance Tools manual.

Management tool	Description and reference
SNMP	You can manage the Telindus 1420 SHDSL Router through SNMP using any SNMP browser. The Telindus 1420 SHDSL Router supports MIB2 and a private MIB, including traps. The private MIB comes with your copy of TMA. After installation of the TMA data files, the private MIB file is available in directory *C:\Program Files\TMA\snmp* with the name *router.mib*. The first part of the directory path may be different if you did not choose the default path during the installation of the TMA data files. For more information, refer to 8.12 - SNMP proxy configuration attributes on page 202 and the documentation of your SNMP browser.

Management tools connection possibilities

The following table gives an overview of all the management possibilities and how you can connect them:

Management tool	PC - Telindus 1420 SHDSL Router connection		PC - Orchid connection (Orchid 1003 LAN as proxy[1])	
	Serial[2]	IP[3]	Serial[2]	IP[3]
EasyConnect	X		X	
CLI	X[4]	X[5]	X[4]	X[5]
ATWIN	X[4]	X[5]	X[4]	X[5]
TMA	X	X	X	X
TMA CLI	X	X	X	X
TMA for HPOV		X		X
SNMP[6]		X		X
Web Interface[7]		X		X

1. For more information on how to set up the Orchid as a proxy agent, refer to the Orchid 1003 LAN manual.
2. A serial connection is a connection between the COM port of your PC and the auxiliary connector of the Telindus 1420 SHDSL Router using a male-female DB9 cable.
3. An IP connection is a connection between your PC and the Telindus 1420 SHDSL Router over an IP network.
4. Using a VT100 terminal (emulation program).
5. Using Telnet.
6. Using an SNMP browser.
7. Using a web browser.

2 Installing and connecting the Telindus 1420 SHDSL Router

First this chapter gives some important safety instructions. Then it explains how to install and connect the Telindus 1420 SHDSL Router.

You are advised to read this chapter from the beginning to the end, without skipping any part. By doing so, your Telindus 1420 SHDSL Router will be completely installed and ready for configuration when you reach the end of this chapter.

The following gives an overview of this chapter:

2.1 Safety instructions

IMPORTANT SAFETY INSTRUCTIONS

Unplug the unit from the wall power outlet before installing, adjusting or servicing.

The safety of this unit depends upon the third pin (ground pin) of the 3-wire grounding type plug. Do not defeat this safety feature. If the power outlet at your site only has 2 pins, please consult a qualified electrician.

ACHTUNG! WICHTIGE SICHERHEITSINSTRUKTIONEN

Vor sämtlichen Arbeiten am Gerät (Installation, Einstellungen, Reparaturen etc.) sollten Sie den Netzstecker aus der Steckdose ziehen.

Die Sicherheit dieses Gerätes ist abhängig von dem dritten Kontakt (dem Erdungspin) des 3-poligen Steckers. Beachten Sie unbedingt diese Sicherheitsstandard. Sollten Sie nur eine ältere 2-polige Steckdose zur Verfügung haben, lassen Sie diese von einem Elektriker gegen eine 3-polige Steckdose auswechseln.

SAFETY WARNING

To avoid damage to the unit, please observe all procedures described in this chapter.

SICHERHEITSBESTIMMUNGEN

Um eine Beschädigung des Gerätes zu verhindern, beachten Sie bitte unbedingt die Sicherheitsbestimmungen, die in diesem Abschnitt beschrieben werden.

Ensure that the unit and its connected equipment all use the same AC power and ground, to reduce noise interference and possible safety hazards caused by differences in ground or earth potentials.

2.2 Unpacking

Checking the shipping carton

Rough handling during shipping causes most early failures. Before installation, check the shipping carton for signs of damage:

- If the carton box is damaged, please place a claim with the carrier company immediately.
- If the carton box is undamaged, do not dispose of it in case you need to store the unit or ship it in the future.

Package contents

The box should contain the following items:

- Telindus 1420 SHDSL Router
- TMA CD-ROM (including this User and Reference manual in PDF format)

Optionally (depending which sales item you ordered):

- external power supply with power cord (2 meter)

2.3 Selecting a site

WARNING

Always place the unit on its feet without blocking the air vents.

Do not stack multiple units directly onto each other, as stacking can cause heat build-up that could damage the equipment.

ACHTUNG

Stellen Sie das Gerät niemals seitlich, sondern nur auf den Füßen auf und achten Sie darauf, daß die Lüftungsschlitze an der Seitenverkleidung frei bleiben.

Stapeln Sie nicht mehrere Geräte direkt übereinander, dies kann zu einem Hitzestau führen.

Install the unit in an area free of extreme temperatures, humidity, shock and vibration. Position it so that you can easily see and access the front panel and its control indicators. Leave enough clearance at the back for cables and wires. Position the unit within the correct distances for the different accesses and within 2m of a power outlet.

2.4 Installation and connection precautions

ESD WARNING

The circuit boards are sensitive to electrostatic discharges (ESD) and should be handled with care. It is advisable to ensure an optimal electrical contact between yourself, the working area and a safety ground before touching any circuit board. Take special care not to touch any component or connector on the circuit board.

EMC WARNING

EMC compliant installation

The Telindus access products are fully EMC compliant. To ensure compliance with EMC directive 89/336/EEC, shielded cables or ferrite beads have to be used.

NOTE

This unit may be powered by an IT power system.

ANMERKUNG

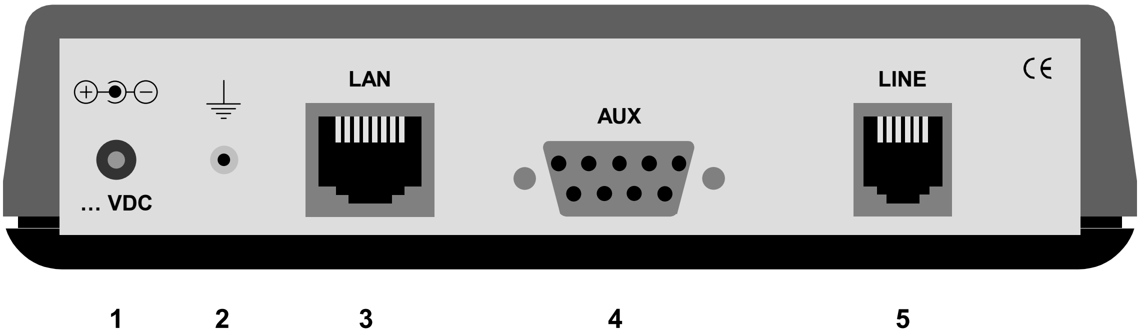
Das Gerät kann gespeist wurden durch ein IT power System.

2.5 Connecting the Telindus 1420 SHDSL Router

This section explains how to connect the Telindus 1420 SHDSL Router. The following gives an overview of this section:

2.5.1 Rear view of the Telindus 1420 SHDSL Router

The following is a rear view of the Telindus 1420 SHDSL Router:



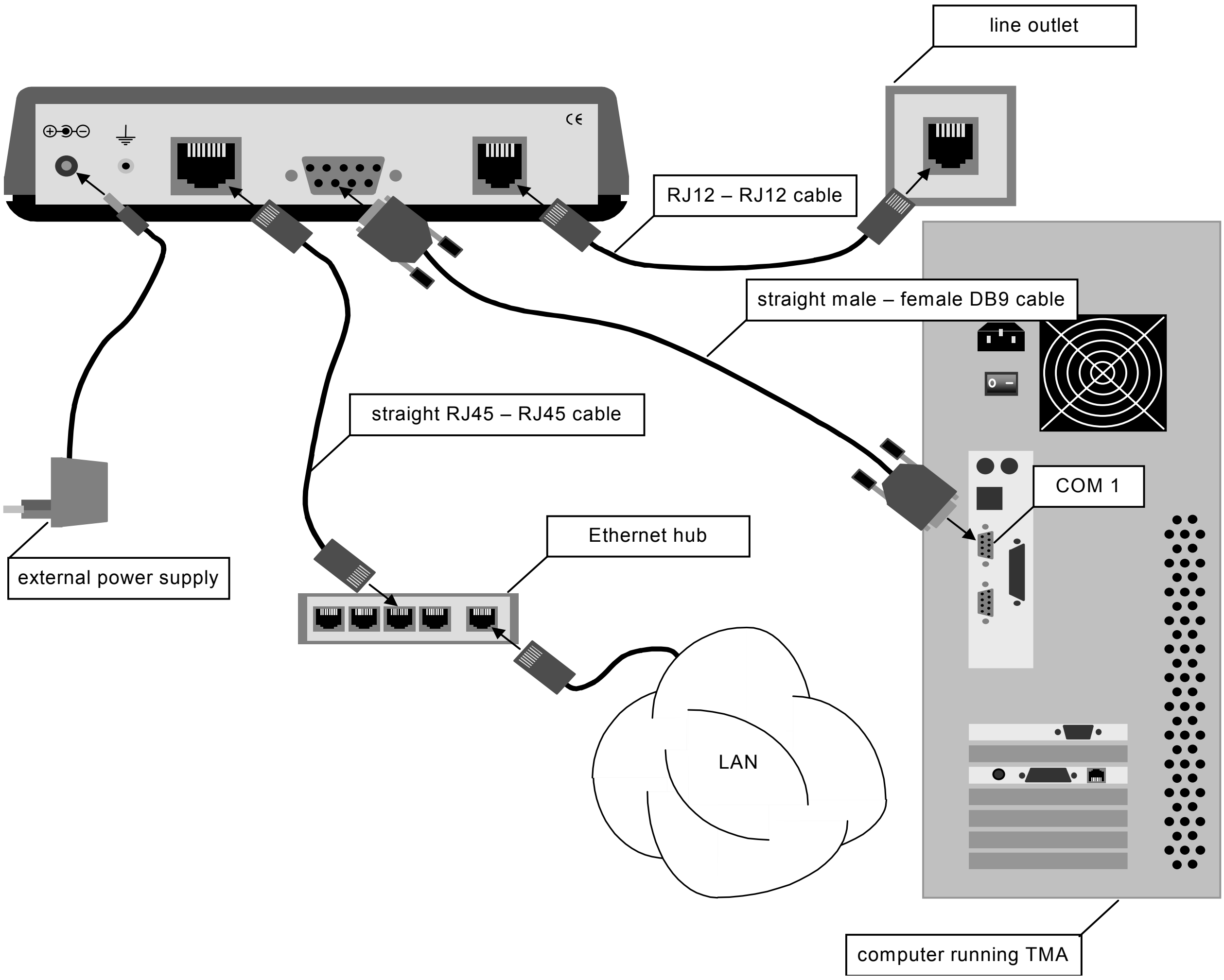
2.5.2 Connecting the different parts of the Telindus 1420 SHDSL Router

The following table gives an overview of the parts located at the back of the Telindus 1420 SHDSL Router:

Part	Label	Description
1	9 VDC	This is the power input. Insert the plug of the external power supply in this socket.
2	⏚	This is the protective ground connection (PGND). Ensure that the unit and its connected equipment all use the same PGND on order to reduce noise interference and possible safety hazards caused by differences in earth potentials.
3	LAN	This RJ45 Twisted Pair Interface (TPI) is the connection towards the LAN. Connect one side of an RJ45 to RJ45 cable to the LAN connector of the Telindus 1420 SHDSL Router and the other side to a network outlet. If you want to connect the Telindus 1420 SHDSL Router to … • a regular Ethernet network outlet, then use a crossed RJ45 cable. • an Ethernet hub, then use a straight RJ45 cable. For more information on this connector, refer to 15.3 - Ethernet LAN interface on page 311.
4	AUX	This female 9-pin subD connector is the auxiliary connector. You can connect this connector to a COM port of your PC with a straight male-female DB9 cable. This enables you to manage the Telindus 1420 SHDSL Router locally, using TMA, CLI, ATWIN etc. You can also connect this connector to the Orchid 1003 LAN, also for management purposes. For more information on this connector, refer to 15.5 - Auxiliary connector on page 312.
5	LINE	This RJ12 connector is the connection towards the SHDSL line. Connect one side of an RJ12 to RJ12 cable to the LINE connector of the Telindus 1420 SHDSL Router and the other side to an SHDSL outlet.

2.5.3 Connecting the Telindus 1420 SHDSL Router - an example

The following figure shows a typical Telindus 1420 SHDSL Router set-up:



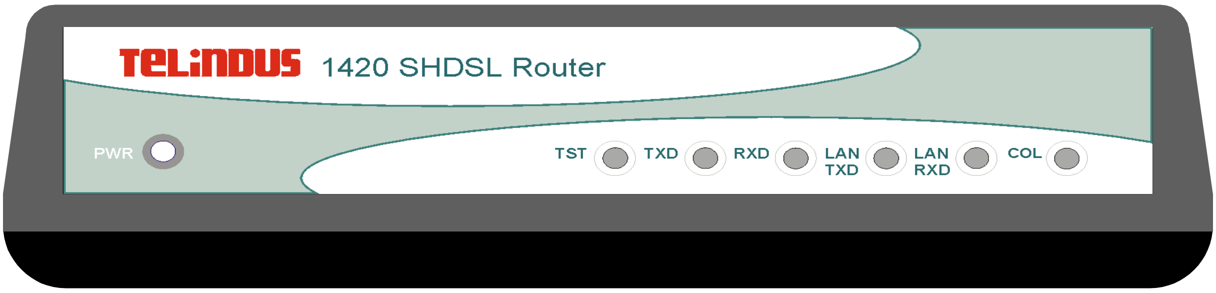
2.6 The front panel LED indicators

This section gives an overview of the front panel LEDs and what they indicate. The following gives an overview of this section:

2.6.1 Introducing the front panel LEDs

When all the connections are made and the Telindus 1420 SHDSL Router is powered, the LEDs on the front panel reflect the actual status of the device.

The following figure shows the front panel LED indicators of the Telindus 1420 SHDSL Router:



LED status modes

For some front panel LED indicators different status modes exist. These status modes can be distinguished by the way the LED is lit up:

LED status	LED duty cycle	Description
continuously off	0 %	The LED never lights up.
continuously on	100 %	The LED lights up continuously.
blinking	50 %	The LED is as much lit as it is out.
flashing	20 %	The LED only lights up during 20% of the time.
mostly off	-	The LED occasionally lights up, without a fixed duty cycle.
mostly on	-	The LED occasionally goes out, without a fixed duty cycle.
monitoring	-	The LED lights up irregularly. For instance, it lights up on detection of a certain signal. I.e. it monitors this signal.

2.6.2 The power LED (PWR)

The power LED indicates the following:

LED status	Description
continuously off	No DC input power is available.
blinking	When the Telindus 1420 SHDSL Router boots, it performs a self test. If this test fails, the power LED blinks and the TST, TXD and RXD LEDs light up continuously. The power LED also blinks briefly when the Telindus 1420 SHDSL Router switches from running in boot mode to normal flash memory operation.
continuously on	The Telindus 1420 SHDSL Router is powered and the boot sequence has been completed successfully.

When the Telindus 1420 SHDSL Router runs in boot mode, because it is forced in this mode by DIP switch or because no firmware is present in the flash memory, the PWR, TST, TXD and RXD LEDs light up continuously.

2.6.3 The test LED (TST)

This LED indicates whether a test is active or not:

LED status	Description
continuously off	No test is active.
continuously on	A test is active.

2.6.4 The transmit data LED (TXD)

This LED reflects the status of the link and monitors the transmitted user data on the WAN (line) interface:

LED status	Description
continuously off	Nothing is connected to the line.
mostly off	A layer 2 handshake is in progress.
monitoring	Layer 2 is up. The LED goes out for a fixed time when a user data frame is sent on the line.
continuously on	Layer 2 is up. No user data is sent on the line.

2.6.5 The receive data LED (RXD)

This LED monitors the received user data on the WAN (line) interface:

LED status	Description
continuously off	No user data is received on the line.
monitoring	The LED lights up for a fixed time when a user data frame is received on the line.

2.6.6 The LAN transmit data LED (LAN TXD)

This LED reflects the status of the link and monitors the transmitted user data on the LAN interface:

LED status	Description
continuously off	Nothing is connected to the LAN interface.
monitoring	The Ethernet link is up. The LED goes out for a fixed time when a user data frame is sent on the LAN interface.
continuously on	The Ethernet link is up. No user data is sent on the LAN interface.

2.6.7 The LAN receive data LED (LAN RXD)

This LED monitors the received user data on the LAN interface:

LED status	Description
continuously off	No user data is received on the LAN interface.
monitoring	The LED lights up for a fixed time when a user data frame is received on the LAN interface.

2.6.8 The collision LED (COL)

This LED monitors the collisions on the LAN:

LED status	Description
continuously off	No collisions are detected on the LAN.
monitoring	The LED lights up every time a collision is detected on the LAN.

3 DIP switches and straps of the Telindus 1420 SHDSL Router

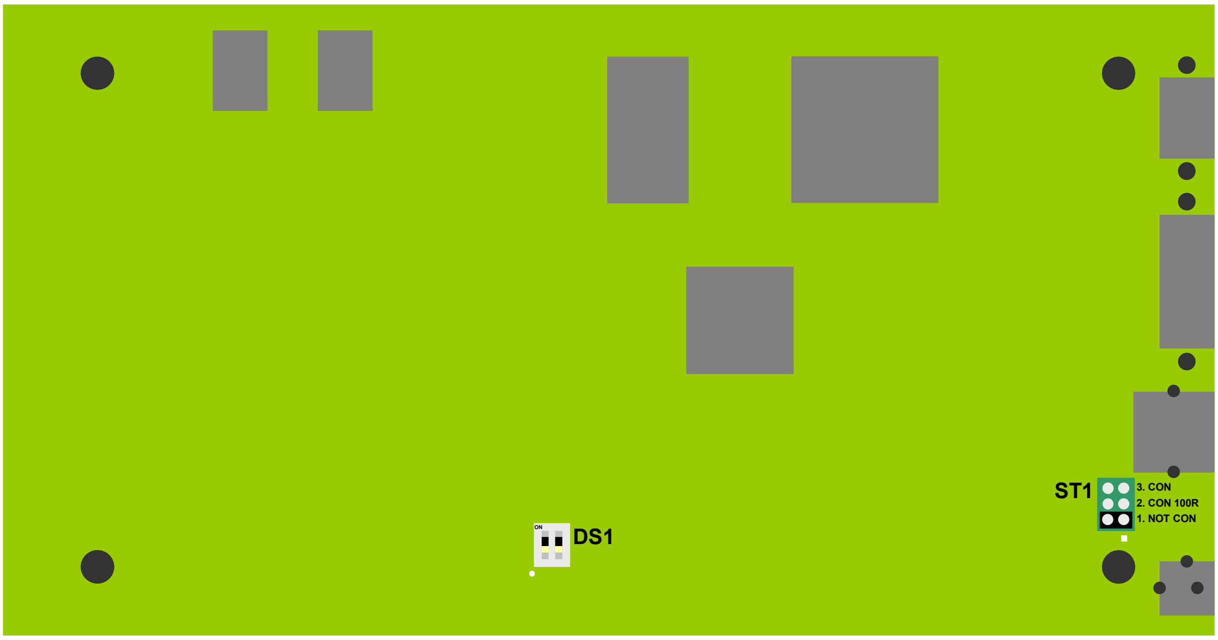
This chapter locates the DIP switches and straps on the Telindus 1420 SHDSL Router motherboard. It gives an overview of their function and it explains how to change their settings.

The following gives an overview of this chapter:

Default settings are printed in **bold**.

3.1 The Telindus 1420 SHDSL Router motherboard

The figure below shows the position of the DIP switches and straps on the Telindus 1420 SHDSL Router motherboard:



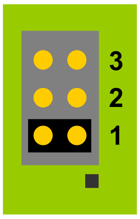
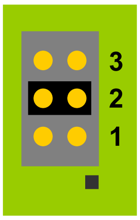
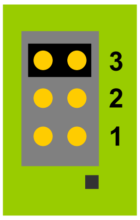
3.2 DIP switches of the Telindus 1420 SHDSL Router

The following table gives an overview of the DIP switches on DIP switch bank DS1:

DIP switch name	DS1 no.	Setting	Function
start-up mode	1	**on**	Start up from flash memory.
		off	Start up in boot mode.
load default configuration	2	**on**	Normal operation.
		off	Load default configuration.

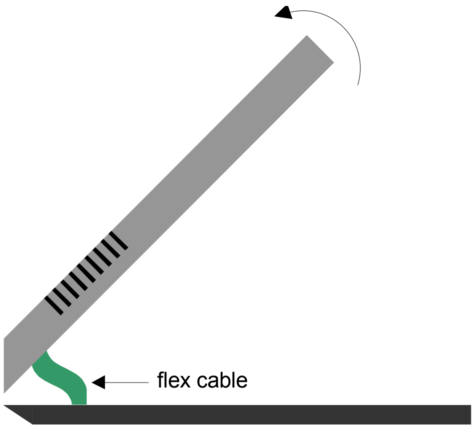
3.3 Straps of the Telindus 1420 SHDSL Router

With strap ST1, you can configure the interconnection between signal ground and protective ground (earth). The following table gives an overview of the strap settings of strap ST1:

Strap settings	Connection	Description
position 1 	disconnected	As default, the signal ground is disconnected from the earth. This avoids problems which might occur when the earth potential of the Telindus 1420 SHDSL Router and the connected device is not the same. In such a situation earth current loops may induce distortion on the transmitted data, resulting in transmission errors.
position 2 	connected through 100 ohms resistor	Sometimes you might want to connect the Telindus 1420 SHDSL Router earth to the earth of the connected device although both earth potentials are not the same. (E.g. to avoid a big difference between both earth potentials.) To avoid that high earth currents are generated, you can make this connection through a 100 ohms resistor.
position 3 	directly connected	Sometimes it is not possible to connect the connected device directly to the earth. In that case you can earth the device through the Telindus 1420 SHDSL Router by connecting the Telindus 1420 SHDSL Router to the earth and setting strap ST1 in position 3. Also the opposite situation might occur: it is not possible to earth the Telindus 1420 SHDSL Router. In that case you can earth the Telindus 1420 SHDSL Router through the connected device by connecting the device to the earth and setting strap ST1 in position 3.

3.4 Changing DIP switch and strap settings

To change the DIP switch and / or strap settings of the Telindus 1420 SHDSL Router, proceed as follows:

Step	Action
1	Disconnect the external power supply.
2	Unscrew the four screw located at the bottom of the housing. 
3	Carefully lift the housing cover. Do not lift the cover too high, in order not to damage the flex cable attached to the front panel.
4	Carefully tilt the cover towards the front. The following figure clarifies this: 
5	Change the DIP switch and / or strap settings.
6	Carefully replace the cover and close tight.
7	Fasten the four screw located at the bottom of the housing.
8	Reconnect the external power supply.

4 Managing the Telindus 1420 SHDSL Router

Once you installed the Telindus 1420 SHDSL Router, you can proceed with the configuration of the Telindus 1420 SHDSL Router. You can do this using any of the management tools introduced in 1.8 - Management tools on page 14.

This chapter briefly highlights one of those management tools: the Telindus Maintenance Application (TMA). This chapter introduces TMA and describes how to start a session on the Telindus 1420 SHDSL Router. Furthermore, it gives an introduction to the management attributes of the Telindus 1420 SHDSL Router.

The following gives an overview of this chapter:

4.1 Introducing TMA

What is the Telindus Maintenance Application?

TMA is a free Windows® software package that enables you to maintain the Telindus 1420 SHDSL Router, i.e. to access its configuration attributes and look at status, performance and alarm information using a user friendly graphical user interface.

TMA is an excellent tool for complete management of the Telindus access devices. When using TMA in combination with a network management system such as HP OpenView, complete networks can be managed from one central site.

Consult the TMA user manual to install it and get acquainted with the TMA user interface.

You will need a new version of the model file distribution if changes have been made to the attributes of the Telindus 1420 SHDSL Router. The most recent model files and TMA engine can always be downloaded from the Telindus web site. Go to http://www.telindus.com/accessproducts and select *Products → Maintenance & Management → Download TMA software*.

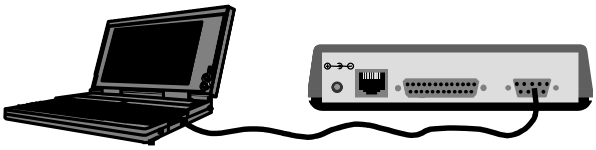
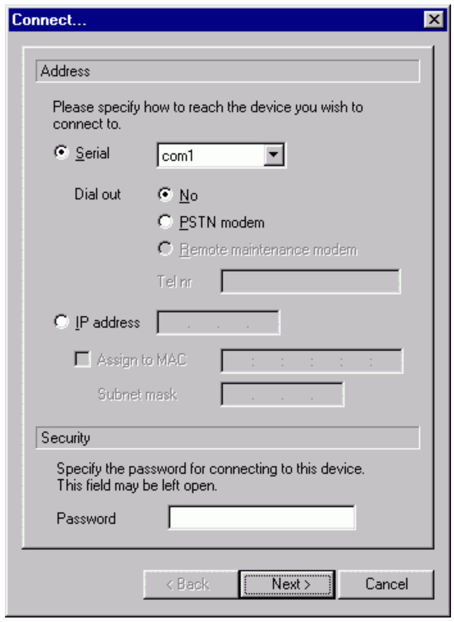
How to connect TMA?

There are two ways to establish a connection between the computer running TMA and the Telindus 1420 SHDSL Router:

- through a serial connection, i.e. through the auxiliary connector of the Telindus 1420 SHDSL Router.
- through an IP connection, i.e. through the LAN connector of the Telindus 1420 SHDSL Router.

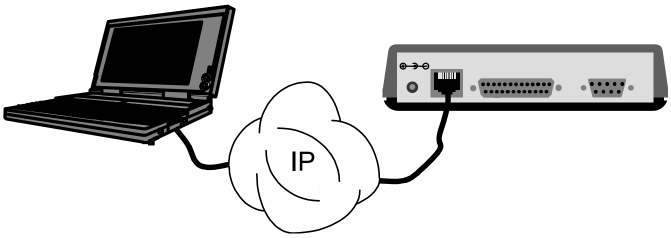
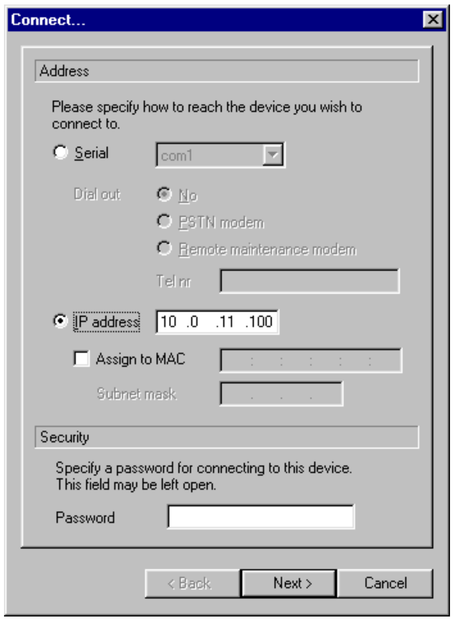
4.2 Connecting through the auxiliary connector

To established a connection between TMA and the Telindus 1420 SHDSL Router through the auxiliary connector, proceed as follows:

Step	Action
1	Connect a serial port of your computer (e.g. COM1) through a straight DB9 male - female cable with the auxiliary connector of the Telindus 1420 SHDSL Router. 
2	Start TMA.
3	In the TMA window, either … • select from the menu bar: *Connect* → *Device…* • or press the short-cut key: Ctrl+N • or click on the *Connect to device* button:  The *Connect…* (to a device) window is being displayed as in the following figure: 
4	In the *Connect…* (to a device) window, specify the following: • Select the option *Serial* and specify the COM port of your computer to which the Telindus 1420 SHDSL Router is connected. • If a password has previously been configured in the Telindus 1420 SHDSL Router then also fill in the password field.
5	Click on the *Next >* button. ⇒ After a couple of seconds, the attributes of the selected Telindus 1420 SHDSL Router appear in the TMA window.

4.3 Connecting over an IP network

To established a connection between TMA and the Telindus 1420 SHDSL Router over an IP network, proceed as follows:

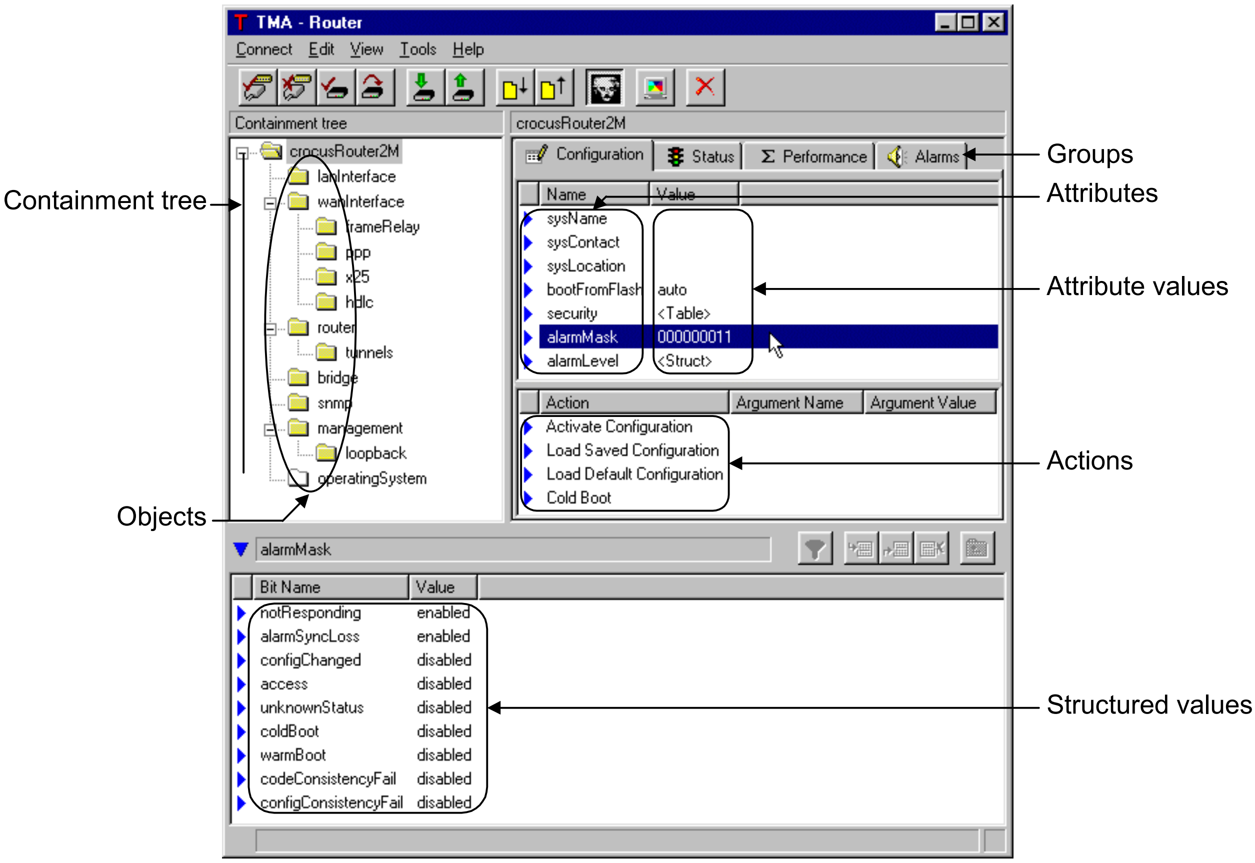
Step	Action
1	Connect the IP network to … • the network port of your PC, • the LAN connector of the Telindus 1420 SHDSL Router. 
2	Start TMA.
3	In the TMA window, either … • select from the menu bar: *Connect* → *Device…* • or press the short-cut key: Ctrl+N • or press on the *Connect to device* button:  The *Connect…* (to a device) window is being displayed as in the following figure: 
4	In the *Connect…* (to a device) window, specify the following: • Select the option *IP address* and enter the IP address of the Telindus 1420 SHDSL Router. • If a password has previously been configured in the Telindus 1420 SHDSL Router then also fill in the password field. Before you are able to establish a connection over an IP network, you have to configure an IP address and a default gateway in the Telindus 1420 SHDSL Router. You can do this by first connecting TMA to the Telindus 1420 SHDSL Router through the auxiliary connector, and then configuring an IP address and a default gateway (refer to 5.3 - Configuring IP addresses on page 54).
5	Click on the *Next >* button. ⇒ After a couple of seconds, the attributes of the selected Telindus 1420 SHDSL Router appear in the TMA window.

4.4 Introducing the management terminology

This section introduces the terminology concerning the management of a Telindus device. It explains terms such as containment tree, group, object, attribute, value and action.

Graphical representation of the containment tree

The most comprehensible graphical representation of the containment tree is given in TMA. The following figure depicts the TMA window containing the Telindus 1420 SHDSL Router containment tree:



Containment tree terminology

The following table explains the terminology associated with the containment tree:

Term	Description
containment tree	The containment tree represents the hierarchical structure of the Telindus 1420 SHDSL Router. It is composed of a number of objects that are ordered in a tree. This tree resembles a Windows® directory structure: • it is also a levelled structure, with nodes which can be expanded or reduced. • the containment tree objects can be compared with file folders. • the objects contain attributes like file folders contain files.
object	An object represents a physical interface, an application or a combination of both. Each object has its own set of attributes. Example: The object shdslRouter contains the sub-object lanInterface. This object contains all the attributes concerning the LAN interface. E.g. the configuration attribute ipAddress.
attribute	An attribute is a parameter related to a certain object. It has a certain value. Example: The object lanInterface contains the status attribute ifOperStatus, which has as possible values up and down.
value	An attribute has a certain value which is … • changeable in case of a configuration attribute (provided you have write access). • read only in case of a status, performance and alarm attribute. Example: The configuration attribute ripMode can be set to the value disabled, passive or active.
structured value	Some attribute values contain underlying values: a structured value. These values are displayed in the structured value window. If an attribute contains structured values then a bit string, <Table> or <Struct> is displayed after the attribute. Example: The alarmLevel attribute contains a structured value which displays alarms and their corresponding priority level.
group	Groups assemble a set of attributes related by functionality. There are four groups in TMA, which correspond with the four tabs in the attribute window: • configuration, • status, • performance, • alarms.

Term	Description
action	A group in combination with an object may have actions assigned to them. These actions are displayed in the action window. Example: The Activate Configuration action only appears when the object shdslRouter is selected in combination with the group Configuration.

4.5 The Telindus 1420 SHDSL Router containment tree

The following table lists the different objects of the Telindus 1420 SHDSL Router containment tree:

Object	This object contains …
> shdslRouter	the general system attributes. It is the top object in the containment tree E.g. the configuration attributes sysName, sysContact and sysLocation.
>> lanInterface	the attributes of the LAN interface. E.g. the configuration attributes ipAddress, ipNetMask and secondaryIpAddresses.
>> wanInterface	the attributes of the WAN interface. E.g. the configuration attributes ipAddress, ipNetMask and encapsulation.
>>> frameRelay	the attributes related with the Frame Relay encapsulation on the WAN interface. E.g. the configuration attributes dlciTable and lmi.
>>> ppp	the attributes related with the PPP encapsulation on the WAN interface. E.g. the configuration attributes linkMonitoring and authentication.
>>> hdlc	the attributes related with the HDLC encapsulation on the WAN interface.
>>> line	the general attributes of the line. E.g. the configuration attribute speed.
>>>> linePair [1]	the specific line attributes. E.g. the status attribute lineAttenuation.
>> router	the attributes concerning the routing itself. E.g. the configuration attribute routingTable.
>>> tunnels	the attributes concerning the layer 2 tunnelling.
>> bridge	the attributes concerning the bridging functionality. E.g. the configuration attribute spanningTree.
>> snmp	the attributes concerning SNMP traps. E.g. the configuration attribute trapDestinations.
>> management	attributes concerned with the management of the Telindus 1420 SHDSL Router. E.g. the configuration attribute cms2Address.
>> operatingSystem	the operating system attributes. E.g. the performance attribute freeMemory.

4.6 Telindus 1420 SHDSL Router attribute overview

The reference part of this manual explains all the attributes of the Telindus 1420 SHDSL Router. One chapter describes one group of attributes:

- chapter 8 describes the configuration attributes,
- chapter 9 describes the status attributes,
- chapter 10 describes the performance attributes,
- chapter 11 describes the alarm attributes.

5 Step-by-step configuration

This chapter describes in a step-by-step method how to perform a basic configuration on Telindus 1420 SHDSL Router. First it explains how DIP switch configuration tables and TMA attribute strings should be interpreted.

You are advised to read this chapter in a sequential manner, from the beginning to the end, without skipping any part. By doing so, your Telindus 1420 SHDSL Router will be completely configured and ready for use when you reach the end of this chapter.

The following gives an overview of this chapter:

For a complete overview of the attributes of the Telindus 1420 SHDSL Router, refer to the reference manual.

5.1 Reading the configuration settings

As this chapter explains the basic configuration of the Telindus 1420 SHDSL Router, it contains some DIP switch configuration tables and a lot of TMA attribute strings. To enable you to read this information in a correct manner, this section explains the structure of such tables and strings.

The following gives an overview of this section:

5.1.1 DIP switch configuration table

A DIP switch configuration table has the following layout:

DIP switch name	DS1 no.	Setting	Function
	1	**on**	
		off	

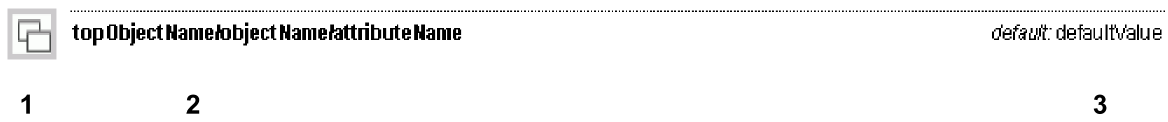
1 **2** **3** **4** **5**

The following table explains the DIP switch configuration table layout:

Number	This position displays …
1	the DIP switch icon. It indicates that the table which follows is a DIP switch configuration table.
2	the DIP switch name.
3	the DIP switch position on the DIP switch bank. The abbreviations mean the following: DS1 no. 1: DIP switch bank number 1, switch position number 1
4	the possible settings of the DIP switch: on and off. The default setting is printed in bold.
5	the function associated with the corresponding DIP switch setting.

5.1.2 TMA attribute string

A TMA attribute string has the following layout:



The following table explains the TMA attribute string layout:

Number	This position displays …
1	the TMA attribute icon. It indicates that the string which follows is a TMA attribute string. Two different TMA attribute icons exist: • a basic attribute icon, • an advanced attribute icon. For more information refer to Graphical conventions on page vii.
2	the attribute name and its position in the containment tree. In the figure above, the string shdslRouter/lanInterface/ipAddress means the following: • the attribute name is ipAddress, • this attribute is located in the sub-object lanInterface, • this sub-object is located in the top object shdslRouter.
3	the default value of a configuration attribute.

5.2 Loading the default configuration

If you install the Telindus 1420 SHDSL Router for the first time, all configuration attributes are set to their default value. If the Telindus 1420 SHDSL Router has already been configured a number of times and you want to reconfigure it starting from scratch, it might be best to load the default configuration.

The following gives an overview of this section:

5.2.1 Loading the default configuration with a DIP switch

The following procedure shows how to load the default configuration using the *Load Default Configuration* DIP switch on the Telindus 1420 SHDSL Router PCB:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Disconnect the power supply and open the housing as described in 3.4 - Changing DIP switch and strap settings on page 35.</td></tr>
<tr><td>2</td><td>Set DIP switch bank DS1 position 2 to off.

To locate this DIP switch bank, refer to 3 - DIP switches and straps of the Telindus 1420 SHDSL Router on page 31.</td></tr>
<tr><td>3</td><td>Replace the cover without fastening the screws and reconnect the power supply.

⇒ The Telindus 1420 SHDSL Router reboots and loads the default configuration.</td></tr>
<tr><td>4</td><td>Activate the loaded default configuration:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Open a TMA session on the Telindus 1420 SHDSL Router. Refer to 4 - Managing the Telindus 1420 SHDSL Router on page 37.</td></tr>
<tr><td>2</td><td>Execute the Activate Configuration action.[1]</td></tr>
</table>

1. If you are performing this load default configuration procedure because you accidentally made a configuration error, you have the possibility to retrieve this erroneous configuration before executing the Activate Configuration command. In that case you do not have to reconfigure the complete device again, but you only have to correct the error in question. Retrieve the erroneous configuration by executing the Load Saved Configuration command.</td></tr>
<tr><td>5</td><td>Again, disconnect the power supply and open the housing.</td></tr>
<tr><td>6</td><td>Reset DIP switch bank DS1 position 2 to on.</td></tr>
<tr><td>7</td><td>Properly replace the cover and reconnect the power supply.</td></tr>
</table>

5.2.2 Loading the default configuration with TMA

The following procedure shows how to load the default configuration using the *Load Default Configuration* action in TMA:

shdslRouter/Load Default Configuration

To load the default configuration, proceed as follows:

Step	Action
1	In the TMA window, select the top object shdslRouter and the group Configuration.
2	In the action window of TMA, click the left mouse button on the Load Default Configuration action so that it is selected.
3	Press the right mouse button and select *Execute*. Alternatively, double-click on the Load Default Configuration action.
4	To see the default configuration, click on the *Retrieve all attributes from device* button .
5	In the action window of TMA, click the left mouse button on the Activate Configuration action so that it is selected.
6	Press the right mouse button and select *Execute*. Alternatively, double-click on the Activate Configuration action.

5.3 Configuring IP addresses

The first thing you have to configure is the Telindus 1420 SHDSL Router its IP address. You can assign an IP address to the LAN and WAN interface:

Select the object …	in order to assign an IP address to the …
lanInterface	Ethernet interface.
wanInterface	serial interface.

You can also use the BootP procedure in order to obtain an IP address. An IP address obtained using such a dynamic procedure is not displayed in the configuration window, but can be found in the status window.

Use the following two attributes to configure the IP address yourself.

shdslRouter/<interface>/ipAddress

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to assign an IP address to the interface. The address should belong to the subnet the interface is connected to.

shdslRouter/<interface>/ipNetMask

Default:255.255.255.0
Range: up to 255.255.255.255

Use this attribute to assign an IP subnet mask to the interface. The subnet mask defines the number of IP devices that may be present on the corresponding IP segment.

Example

shdslRouter/lanInterface/ipAddress = 192.168.47.254 and shdslRouter/lanInterface/ipNetMask = 255.255.255.0. This means that all IP devices on the Ethernet segment have an IP address in the range from 192.168.47.1 up to 192.168.47.254.

5.4 Configuring the line

To establish a connection over the line successfully, the following attributes are essential:

shdslRouter/wanInterface/line/channel

Default:central
Range: enumerated, see below

Use this attribute to determine which unit is the central unit and which the remote unit.

I.e. it determines which unit acts as master and which as slave during the synchronisation procedure. Therefore set one Telindus 1420 SHDSL Router to central and its remote counterpart to remote.

shdslRouter/wanInterface/line/speed

Default:auto
Range: enumerated, see below

Use this attribute to set the line speed.

The speed attribute has the following values:

Value	Description
auto	In auto speed mode the central and remote Telindus 1420 SHDSL Router negotiate the speed they are going to use on the line.
64Kbps … 2304Kbps	Besides auto speed, you can also select a fixed line speed ranging from 64Kbps up to 2304Kbps in steps of 64 kbps.

5.5 Configuring the WAN encapsulation

This section explains how to select the WAN encapsulation. It also explains the most important attributes for configuring the encapsulation protocols.

The following gives an overview of this section:

5.5.1 Selecting the WAN encapsulation

shdslRouter/wanInterface/encapsulation

Default:frameRelay
Range: enumerated, see below

Use this attribute to select the encapsulation protocol on the WAN interface.

The encapsulation attribute has the following values:

Value	Description
frameRelay	Selects Frame Relay encapsulation. Frame Relay is a synchronous communication protocol.
ppp	Selects Point-To-Point encapsulation. PPP can be synchronous or asynchronous.
hdlc	Selects High-Level Data Link Control encapsulation.

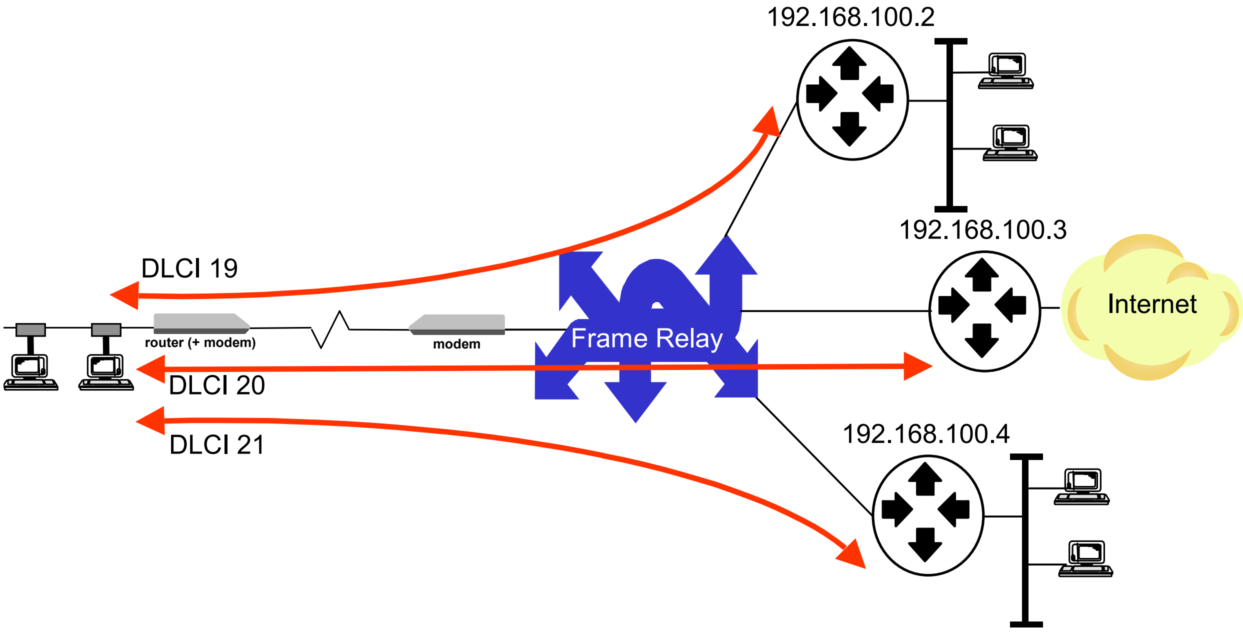
5.5.2 Configuring the Frame Relay encapsulation

Use the configuration attributes dlciTable and lmi to configure the Frame Relay encapsulation.

What is a DLCI?

A DLCI or Data Link Connection Identifiers is a logical channel through which the Telindus 1420 SHDSL Router can connect to a remote router. What is more, the Telindus 1420 SHDSL Router can connect to multiple remote routers via different DLCIs using a single WAN interface. The Telindus 1420 SHDSL Router supports a maximum of 5 DLCIs.

The following figure gives an example of a local Ethernet segment connected to three different networks through three different DLCIs. For each DLCI there is a corresponding router.



Each DLCI connects to one remote router. Through LMI Full Status Enquiry messages, the Telindus 1420 SHDSL Router can learn its active and inactive DLCIs. If the Frame Relay network also supports the Inverse ARP protocol, the Telindus 1420 SHDSL Router can learn the IP address of the corresponding router for each DLCI.

If however neither LMI nor Inverse ARP is supported by the Frame Relay network, then you can define which DLCI number corresponds with which remote router in the dlciTable. This is also called static routing on a WAN.

The following screenshot shows the dlciTable of the set-up depicted in the figure above:

dlciTable

	dlci	gateway
1	19	192.168.100.2
2	20	192.168.100.3
3	21	192.168.100.4

shdslRouter/wanInterface/frameRelay/dlciTable

Default:<empty>
Range: table, see below

Use this attribute to configure the Frame Relay Data Link Connection Identifiers (DLCIs).

The dlciTable contains the following elements:

Element	Description
dlci	This is the DLCI number to reach a remote network. Default:16 Range: 16 … 1022 The DLCI number may have any value between 16 and 1022. However, if you set the configuration attribute lmi to q933-Annex-A, you should only use DLCIs up to 1007.
cir	This is the Committed Information Rate for the corresponding DLCI. Default:0 Range: 0 … 2048000 The CIR is expressed in bps. Any value between 0 and 2048000 (bps) can be configured. If the cir value is set to 0 (default), it means the complete bandwidth may be used (no flow control).
eir	This is the Excess Information Rate for the corresponding DLCI. Default:0 Range: 0 … 2048000 The EIR is expressed in bps. Any value between 0 and 2048000 (bps) can be configured. If the eir value is set to 0 (default), it means no excess burst is allowed. If you configure EIR, then CIR must also be configured. Else there is no flow control.
routing	Use this attribute to determine whether IP packets are treated by the bridging process or not. Default:enabled Range: enabled / disabled The routing element has the following values: **Value** – **Description** enabled – IP packets are passed directly to the routing process. IP packets not destined for the router its MAC address are discarded. disabled – The IP packets are first passed to the bridging process. If necessary, IP packets destined for the router itself are passed on to the routing process.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>gateway</td><td>This is the corresponding IP address of the remote router.
Default:0.0.0.0
Range: up to 255.255.255.255</td></tr>
<tr><td>local</td><td>This address is used in the response on an Inverse ARP request received on the DLCI.
Default:0.0.0.0
Range: up to 255.255.255.255

The local attribute is optional and only needs to be defined in case secondary IP addresses are used on the Frame Relay WAN interface.</td></tr>
<tr><td>bridgePortInfo</td><td>This sets the bridging attributes of the Frame Relay WAN interface.
Default:-
Range: structure, see below

The bridgePortInfo structure contains the following elements:
<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>bridging</td><td>Enables or disables bridging on the interface.
Default:disabled
Range: enabled / disabled</td></tr>
<tr><td>priority</td><td>Each port of a bridge has a unique port identifier. The priority attribute is a part of this port identifier and allows you to change the priority of the port. It is taken as the more significant part in priority comparisons.
Default:128
Range: 0 … 255

The other part of the unique port identifier has a fixed relationship to the physical or logical port. This assures the uniqueness of the unique port identifier among the ports of a single bridge.

For more information on port priority, refer to 5.9.7 - What is Spanning Tree priority and cost? on page 100.</td></tr>
<tr><td>pathCost</td><td>This is the value that is added to the total cost of the path to the root bridge, provided that this particular port is a root port, i.e. that the path to the root goes through this port.
Default:100
Range: 1 … 65535

The total cost of the path to the root bridge should not exceed 65500.

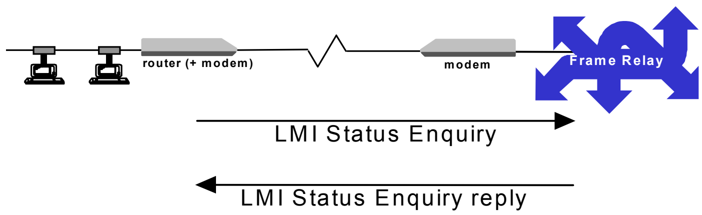
For more information on path cost, refer to 5.9.7 - What is Spanning Tree priority and cost? on page 100.</td></tr>
<tr><td>topologyChange-Detection</td><td>Enables or disables the communication of Spanning Tree topology changes to the root bridge.
Default:enabled
Range: enabled / disabled</td></tr>
</table></td></tr>
</table>

What is LMI?

LMI or Local Management Interface is used in most Frame Relay networks to exchange information between end nodes (like the Telindus 1420 SHDSL Router) and switching nodes. This information concerns, among other things, flow control and link status monitoring.

In a Frame Relay network there are …

- Frame Relay Access Devices (FRADs) or the DTEs. These encapsulate user data into Frame Relay packets.
- Frame Relay nodes or the DCEs. These have multiple serial interfaces and switch the Frame Relay packets.



The LMI exchanges packets between these Frame Relay DTEs and DCEs.

One such a type of packets is the Full Status Enquiry message. At regular intervals, The DTE sends Full Status Enquiry messages to the DCE. The DCE answers with the status of all its DLCIs on the interface. At smaller intervals, the DTE sends Status Enquiry messages. In that case, the DCE only answers with DLCI status changes.

shdslRouter/wanInterface/frameRelay/lmi

Default:-
Range: structure, see below

Use this attribute to select the Local Management Interface (LMI) protocol and to fine-tune the LMI operation.

The lmi structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>type</td><td>This is the LMI variant. There are several standards for the LMI protocol with small variations between them. Therefore you should configure the Telindus 1420 SHDSL Router according to the standard that is used by your service provider.
Default:q933-Annex-A
Range: enumerated, see below
The type attribute has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>noLmiConfigured</td><td>No LMI is used.</td></tr>
<tr><td>lmiRev1</td><td>Set this value only for compatibility with older equipment.</td></tr>
<tr><td>ansit1-617-d</td><td>Set this value for ANSI LMI compliance.</td></tr>
<tr><td>q933-Annex-A</td><td>Set this value for ITU-T LMI compliance.</td></tr>
</table></td></tr>
<tr><td>pollingInterval</td><td>This defines the time between successive Status Enquiry messages.
Default:00000d 00h 00m 10s
Range: 00000d 00h 00m 05s - 00000d 00h 00m 30s</td></tr>
</table>

Element	Description
errorThreshold	This defines the maximum number of unanswered Status Enquiry messages that the Telindus 1420 SHDSL Router will accept before declaring the interface down. See also the attribute monitoredEvents. Default:3 Range: 1 … 10
monitoredEvents	This defines the number of status polling intervals over which the error threshold is counted. Default:4 Range: 1 … 10 In other words, if the station receives an errorThreshold number of unanswered Status Enquiry messages within a monitoredEvents number of pollingInterval intervals, then the interface is declared down. **Example** If the station receives 3 unanswered Status Enquiry messages within 4 x 10s = 40s, then the interface is declared down.
expectedPollInterval	This defines the maximum time between two consecutive incoming Status Enquiry messages. Select the value 0 in order to disable verification. Default:00000d 00h 00m 15s Range: 00000d 00h 00m 00s - 00000d 00h 00m 30s This attribute is only relevant when using Frame Relay over a point-to-point link (no Frame Relay network): In Frame Relay language, a router is normally considered as a DTE. However, if two routers are connected to each other in Frame Relay but without a real Frame Relay network in between, then the routers also take the role of a DCE. This happens automatically, without the need of a reconfiguration. The Status Enquiry messages are sent in both directions.
fullEnquiryInterval	This defines the number of Status Enquiry intervals that have to go by before sending a Full Status Enquiry message. Default:6 Range: 1 … 255

5.5.3 Configuring the PPP encapsulation

The PPP handshake

The Point-to-Point Protocol (PPP) makes a handshake in two phases:

Phase	Description
1	The Link Control Protocol (LCP) builds the link layer.
2	The IP Control Protocol (IPCP) prepares the exchange of IP packets.

During this handshake, it is possible that the IP address is exchanged between the two routers:

IP address requester	Description
Telindus 1420 SHDSL Router	If neither on the LAN nor on the WAN interface an IP address has been configured, then the Telindus 1420 SHDSL Router requests an IP address from the remote router. This is an alternative to the BootP protocol to obtain an IP address.
remote router	If the remote router requests an IP address, the Telindus 1420 SHDSL Router looks in its routing table and replies with the gateway address of the first route which passes the WAN interface. In absence of a specific route which passes the WAN interface, this may also be the default route.

Configuring the PPP encapsulation

The most essential of the PPP encapsulation configuration is …

- enabling or disabling link monitoring,
- enabling or disabling authentication (and setting the corresponding secrets).

shdslRouter/wanInterface/ppp/linkMonitoring

Default:-
Range: structure, see below

Use this attribute to enable or disable link monitoring and to fine-tune it.

The PPP protocol features link monitoring. You can use this to verify whether the WAN link is up or down.

If link monitoring is enabled, then the Telindus 1420 SHDSL Router sends an echo request packet over the line at regular intervals. If on consecutive requests no reply is given, then the PPP link is declared down. Data traffic is stopped until the PPP handshake succeeds again.

The linkMonitoring structure contains the following elements:

Element	Description
operation	Enables or disables link monitoring. Default:disabled Range: enabled / disabled
interval	This defines the time interval between two consecutive echo requests. Default:00000d 00h 00m 10s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
replyTimeOut	This defines the period that the Telindus 1420 SHDSL Router waits for a reply on the echo request. If no reply has been received within this time-out, then the Telindus 1420 SHDSL Router considers this as a failed echo request. Default:00000d 00h 00m 02s Range: 00000d 00h 00m 00s - 00000d 00h 04m 15s
failsPermitted	This defines the number of failed echo requests after which the Telindus 1420 SHDSL Router declares the WAN link down. Default:4 Range: 1 … 30 **Example** Suppose failsPermitted is set to 10. If on 10 consecutive echo requests no reply is given, then the Telindus 1420 SHDSL Router declares the WAN link down and the PPP handshake is started again.

shdslRouter/wanInterface/ppp/authentication

Default:disabled
Range: chap / disabled

Use this attribute to enable or disable CHAP authentication on the PPP link.

The authentication attribute has the following values:

Value	Description
disabled	Authentication is disabled.
chap	This side of the link requests a CHAP authentication from the remote router.

What is CHAP authentication?

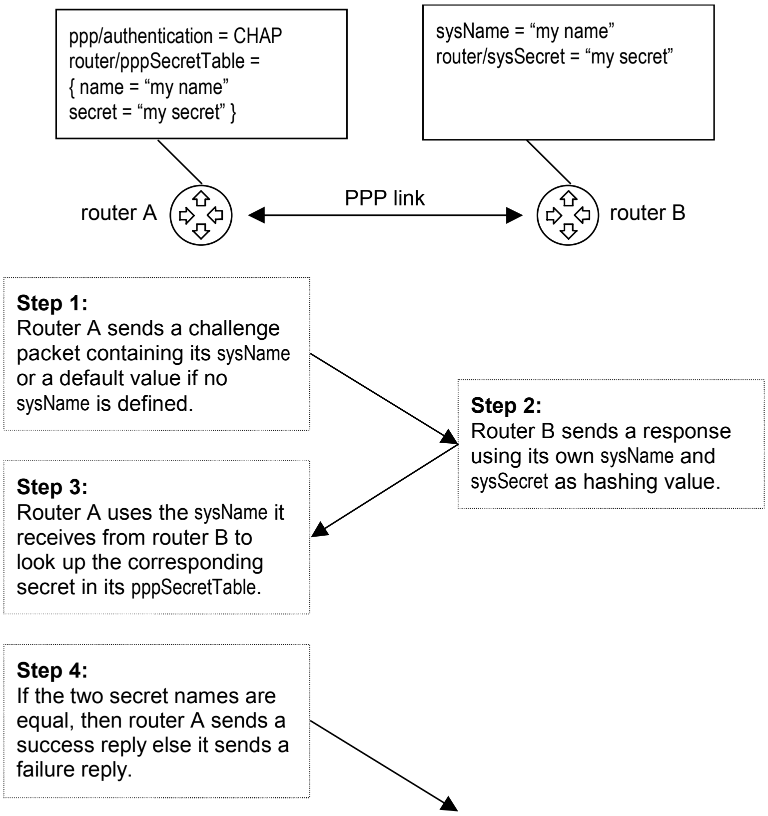
The Challenge Handshake Authentication Protocol (CHAP) is a standardised authentication protocol (in compliance with RFC 1994) over PPP links. The password is hashed before sending it over the link. The used hashing algorithm is MD5. CHAP authentication over a link can be performed in one direction or in both directions.

CHAP authentication in one direction

The figure shows CHAP authentication in one direction.

Router A is called the authenticator and the router B is called the peer. Router A is configured for CHAP authentication and the router B is not.

Router A authenticates after building its LCP layer and prior to building the IPCP layer. If the authentication succeeds, then the PPP link is built further until data can be sent. Else PPP starts its handshake again. During data transfer it also authenticates at regular intervals (refer to the configuration attribute shdslRouter/wanInterface/ppp/authenPeriod on page 169).



CHAP authentication in both directions

If CHAP authentication is enabled on both routers, then they both request and respond to the authentication. If the remote router is a router from another vendor, then read the documentation in order to find out how to configure the CHAP name and secret values.

shdslRouter/router/sysSecret

Default:<empty>
Range: max. 64 characters

Use this attribute for the CHAP authentication process. The CHAP authenticator uses the sysSecret attribute in order to verify the peer its response.

shdslRouter/router/pppSecretTable

Default:<empty>
Range: table, see below

Use this attribute for the CHAP authentication process. Enter the CHAP name and secret of the remote router in this table.

The ripv2SecretTable table contains the following elements:

Element	Description
name	Enter here the CHAP name of the remote router. Default:<empty> Range: max. 64 characters If the remote router is a Telindus 1420 SHDSL Router, then the name element should correspond with the remote Telindus 1420 SHDSL Router its sysName attribute.
secret	Enter here the CHAP secret of the remote router. Default:<empty> Range: max. 64 characters If the remote router is a Telindus 1420 SHDSL Router, then the secret element should correspond with the remote Telindus 1420 SHDSL Router its sysSecret attribute.

5.6 Configuring static routes

Now you have to decide whether to use static routes or the RIPv2 routing protocol:

If your network …	then …
exclusively uses the RIP routing protocol,	you may skip this section.
does not use the RIP routing protocol, or only part of it does,	read this section to learn how to define static routes to the remote IP networks that have to be reached.

If you only have to reach one remote LAN network from your local Ethernet via this router, you may skip the routingTable attribute. In that case it is sufficient to define the defaultRoute attribute only.

Use the configuration attributes defaultRoute and routingTable to configure static routes:

shdslRouter/router/defaultRoute

Default:-
Range: structure, see below

Use this attribute to set the default route, also called gateway address.

Besides specifying routing entries for specific networks, you can also specify a gateway address. Packets for destinations that do not match one of the routing table entries are sent to this gateway address.

The defaultRoute structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>gateway</td><td>This is the IP address of the next router that will route all packets for which no specific (static or dynamic) route is exists in the routing table.
Default:0.0.0.0
Range: up to 255.255.255.255
Whether you can omit the gateway element or not, is linked to the following conditions:
<table>
<tr><th>If the interface element is set to …</th><th>then ...</th></tr>
<tr><td>lan,</td><td>you can not omit the gateway element.</td></tr>
<tr><td>wan,</td><td>you can omit the gateway element only when using PPP encapsulation.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>interface</td><td>This specifies the interface through which the gateway can be reached.
Default:<opt>
Range: enumerated, see below

The interface element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td><opt></td><td>The interface element value is deduced from the setting of the gateway element (refer to Deducing the interface element value on page 76).

Select the <opt> value for routes that use a tunnel.</td></tr>
<tr><td>lan</td><td>The gateway can be reached through the Ethernet interface.</td></tr>
<tr><td>wan</td><td>The gateway can be reached through the serial interface.</td></tr>
<tr><td>discard</td><td>Packets for this destination are discarded.</td></tr>
</table></td></tr>
<tr><td>preference</td><td>This defines the level of importance of the default route with respect to routes learnt via RIP.
Default:10
Range: 1 … 200

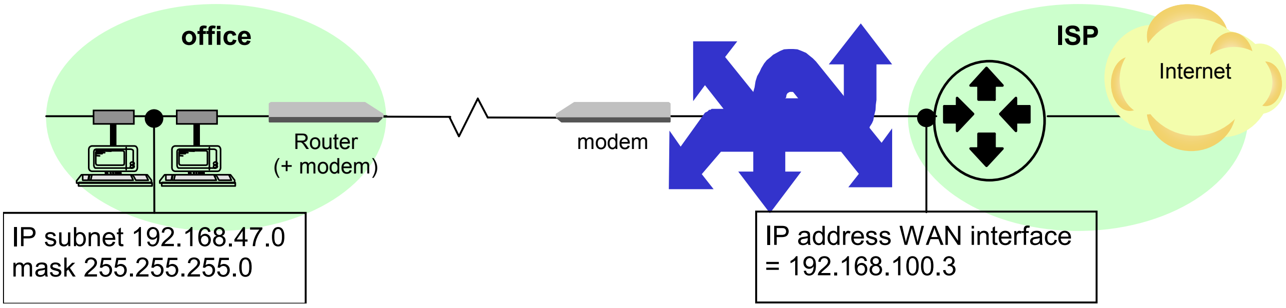
RIP routes always have a preference of 60. Routes with a lower preference value are chosen over routes with higher preference value.</td></tr>
<tr><td>metric</td><td>This determines with how much the Telindus 1420 SHDSL Router increments the metric parameter of a route.
Default:1
Range: 1 … 15

Routing information includes a metric parameter. Every time a router is passed, this parameter is incremented. Also the Telindus 1420 SHDSL Router increments the metric parameter (default by 1) before it writes the route in the routing table. Hence, the metric parameter indicates for each route how many routers have to be passed before reaching the network. When several routes to a single network exist and they all have the same preference, then the route with the smallest metric parameter is chosen.

However, using the metric element, you can increment the metric parameter by more than 1 (up to a maximum of 15). You could do this, for instance, to indicate that a certain interface is less desirable to route through. As a result, the Telindus 1420 SHDSL Router adds this value to the metric parameter of every route learnt through that interface.

The metric attribute is also used to represent the directly connected subnets on the LAN and WAN interfaces.</td></tr>
</table>

Example of a default route



In this example, an office is connected via a modem link over a network of an operator to an Internet Service Provider (ISP). The Telindus 1420 SHDSL Router in the office does not need any static routes. All traffic is sent to the ISP. Hence, the Telindus 1420 SHDSL Router its default route is towards the Internet:

- gateway = 192.168.100.3
- interface = wan

shdslRouter/router/routingTable

Default:<empty>
Range: table, see below

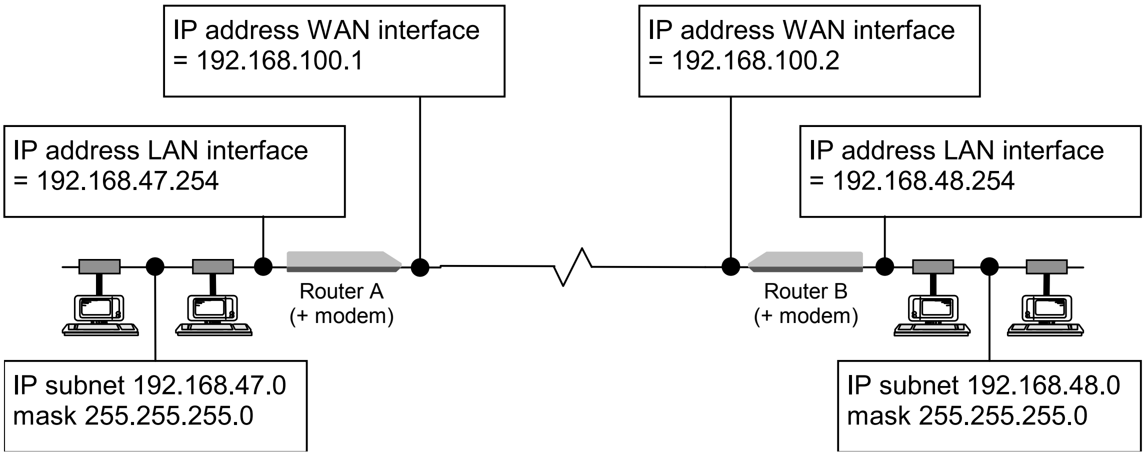
Use this attribute to configure the static IP routes.

The routingTable table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>network</td><td>This is the IP address of the destination network.
Default:0.0.0.0
Range: up to 255.255.255.255</td></tr>
<tr><td>mask</td><td>This is the network mask of the destination network.
Default:255.255.255.0
Range: up to 255.255.255.255</td></tr>
<tr><td>gateway</td><td>This is the IP address of the next router on the path to the destination network.
Default:0.0.0.0
Range: up to 255.255.255.255
Whether you can omit the gateway element or not, is linked to the following conditions:
<table>
<tr><th>If the interface element is set to …</th><th>then ...</th></tr>
<tr><td>lan,</td><td>you can not omit the gateway element.</td></tr>
<tr><td>wan,</td><td>you can omit the gateway element only when using PPP encapsulation.</td></tr>
</table></td></tr>
<tr><td>interface</td><td>This specifies the interface through which the destination network can be reached.
Default:<opt>
Range: enumerated, see below
The interface element has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td><opt></td><td>The interface element value is deduced from the setting of the gateway element (refer to Deducing the interface element value on page 76).
Select the <opt> value for routes that use a tunnel.</td></tr>
<tr><td>lan</td><td>The gateway can be reached through the Ethernet interface.</td></tr>
<tr><td>wan</td><td>The gateway can be reached through the serial interface.</td></tr>
<tr><td>discard</td><td>Packets for this destination are discarded.</td></tr>
</table></td></tr>
<tr><td>preference</td><td>This defines the level of importance of the route with respect to routes learnt via RIP.
Default:10
Range: 1 … 200
RIP routes always have a preference of 60. Routes with a lower preference value are chosen over routes with higher preference value.</td></tr>
</table>

Element	Description
metric	This determines with how much the Telindus 1420 SHDSL Router increments the metric parameter of a route. Default:1 Range: 1 … 15 Routing information includes a metric parameter. Every time a router is passed, this parameter is incremented. Also the Telindus 1420 SHDSL Router increments the metric parameter (default by 1) before it writes the route in the routing table. Hence, the metric parameter indicates for each route how many routers have to be passed before reaching the network. When several routes to a single network exist and they all have the same preference, then the route with the smallest metric parameter is chosen. However, using the metric element, you can increment the metric parameter by more than 1 (up to a maximum of 15). You could do this, for instance, to indicate that a certain interface is less desirable to route through. As a result, the Telindus 1420 SHDSL Router adds this value to the metric parameter of every route learnt through that interface. The metric attribute is also used to represent the directly connected subnets on the LAN and WAN interfaces.

Example 1: Static IP route with an IP address on the WAN interface



In this example, two LANs are interconnected via a modem link. The two routers have an IP address on their WAN interface. To make network 192.168.48.0 reachable from network 192.168.47.0 and vice versa, you have to define one static route in router A (left) and one static route in router B (right) as follows:

Router A:

routingTable

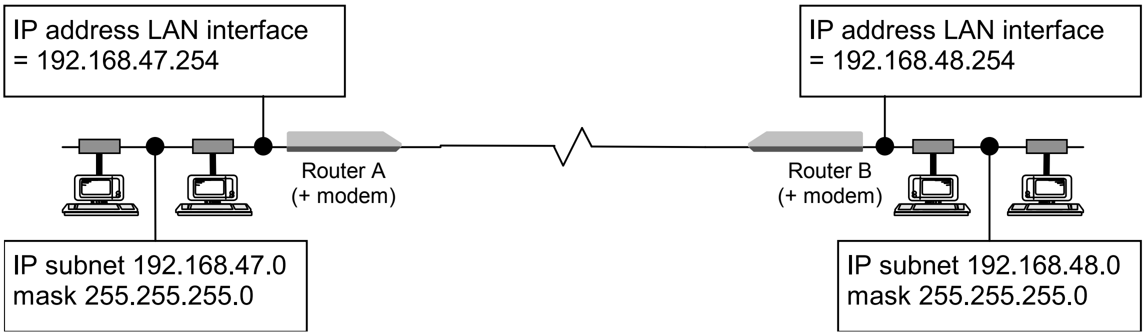
	network	mask	gateway	interface	preference	metric
1	192.168.48.0	255.255.255.0	192.168.100.2	<Opt>	10	2

Router B:

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.47.0	255.255.255.0	192.168.100.1	<Opt>	10	2

Example 2: Static IP route without an IP address on the WAN interface



This example is similar to the previous one, except that now the WAN interfaces do not have an IP address. To make network 192.168.48.0 reachable from network 192.168.47.0 and vice versa, you have to define one static route in router A (left) and one static route in router B (right) as follows:

Router A:

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.48.0	255.255.255.0	192.168.48.254	wan	10	2

Router B:

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.47.0	255.255.255.0	192.168.47.254	wan	10	2

Deducing the interface element value

If you do not specify a value for the interface element, then this value is deduced from the setting of the gateway element. Depending on the presence of an IP address on the WAN interface, the deduction is done as follows:

<table>
<tr><th>WAN IP address</th><th>Deduction</th></tr>
<tr><td>not present</td><td>In this case, the interface element value is deduced as follows:
<table>
<tr><th>If the gateway address …</th><th>then the interface element is set to …</th></tr>
<tr><td>belongs to the Ethernet interface subnet,</td><td>lan</td></tr>
<tr><td>does not belong to the Ethernet interface subnet,</td><td>wan</td></tr>
</table>
</td></tr>
<tr><td>present</td><td>In this case, the interface element value is deduced as follows:
<table>
<tr><th>If the gateway address …</th><th>then …</th></tr>
<tr><td>belongs to the Ethernet interface subnet,</td><td>the interface element is set to lan.</td></tr>
<tr><td>belongs to the serial interface subnet,</td><td>the interface element is set to wan.</td></tr>
<tr><td>neither belongs to the Ethernet interface subnet nor to the serial interface subnet,</td><td>the route is discarded (i.e. not used).</td></tr>
</table>
</td></tr>
</table>

5.7 Configuring the Routing Information Protocol

What is RIP?

RIP or Routing Information Protocol is a protocol that routers use to exchange dynamic routing information.

How does RIP work?

When RIP is enabled, the Telindus 1420 SHDSL Router advertises every 30 seconds its routing information to adjacent routers. It also receives the routing information from the adjacent routers. With this information it adapts its routing table dynamically. If after 180 seconds no information about a certain route has been received, then this route is declared *down*. If after an additional 120 seconds (i.e. 300 seconds in total) still no information about the route has been received, then this route is deleted from the routing table.

RIP support

The Telindus 1420 SHDSL Router supports RIP protocol version 2. RIP version 1 is a very common routing protocol. Version 2 includes extra features like variable subnet masks and authentication. Check that the other routers in the network also use RIP protocol version 2.

Currently, the RIPv2 routing protocol requires the use of an IP address on the WAN interface.

shdslRouter/router/routingProtocol

Default:none
Range: enumerated, see below

Use this attribute to activate or deactivate the Routing Information Protocol (RIP).

The routingProtocol attribute has the following values:

Value	Description
none	No routing protocol is used. Only static routes are used.
Rip2	The RIP version 2 routing protocol is used.

shdslRouter/<interface>/ripMode

Default:active
Range: enumerated, see below

Use this attribute to modify the RIP behaviour of the interface. By default the Telindus 1420 SHDSL Router transmits and receives RIP updates on all interfaces.

The ripMode attribute has the following values:

Value	Description
active	RIP updates are transmitted and received on this interface.
passive	RIP updates are not transmitted on this interface, but received updates are parsed.
disabled	RIP updates are nor transmitted nor received on this interface.

RIP authentication

RIPv2 provides the possibility to authenticate the routing updates. You can configure this using:

- the rip2Authentication attribute in the interface objects (for more information refer to shdslRouter/lanInterface/rip2Authentication on page 154).
- the ripv2SecretTable attribute in the router object (for more information refer to shdslRouter/router/ripv2SecretTable on page 176).

Other, advanced attributes to tune RIP are:

- the metric attribute in the interface objects (for more information refer to shdslRouter/lanInterface/metric on page 153).
- the splitHorizon attribute in the WAN interface object (for more information refer to shdslRouter/wanInterface/splitHorizon on page 161).
- the ripUpdateInterval attribute in the router object (for more information refer to shdslRouter/router/ripUpdateInterval on page 176).

5.8 Configuring NAT and PAT

This section explains Network Address Translation (NAT) and Port Address Translation (PAT). Firstly, it gives an introduction. Secondly, a table is presented that will help you to determine which translation method meets your requirements. Then this section teaches you how to configure NAT and PAT.

The following gives an overview of this section:

5.8.1 Introducing NAT and PAT

What is NAT and PAT?

Network Address Translation (NAT) and Port Address Translation (PAT) are used to translate private IP addresses into official IP addresses.

If you use the Telindus 1420 SHDSL Router to have a permanent connection to the Internet, you may need NAT and/or PAT.

If you do not need address translation, you may skip this section.

Why use NAT and PAT?

Each device connected to the Internet must have an *official* (i.e. unique) IP address. The success of the Internet has caused a lack of these official IP addresses. As a result, your Internet Service Provider (ISP) may offer you only one or a small number of official IP addresses.

If the number of IP devices on your local network is larger than the number of official IP addresses, you can assign test or private IP addresses to your local network. In that case, you have to configure your Telindus 1420 SHDSL Router to translate IP addresses using NAT or PAT.

Even when there are sufficient official IP addresses available, you may still choose to use NAT e.g. for preserving previously assigned test addresses to all the devices on your local network.

Private IP address range

The international authority IANA assigns the official (also called global) IP addresses. It has also defined 3 ranges of IP addresses for private use. This means that you can use these addresses without registration on your internal network, as long as you are not connected to the Internet.

Private IP address range	Remarks
10.0.0.0 - 10.255.255.255	1 class A network
172.16.0.0 - 172.31.255.255	16 class B networks
192.168.0.0 - 192.168.255.255	256 class C networks

You can define (sub-)networks in these ranges for your *private IP addresses*.

5.8.2 When use NAT and/or PAT

Check in the next table whether you need NAT and/or PAT:

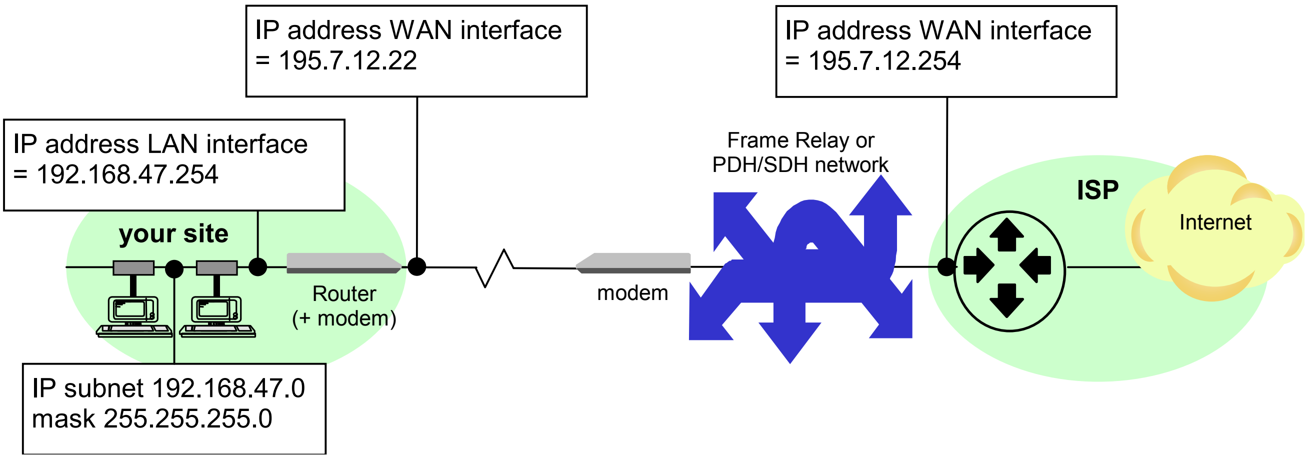
No. of official IP addresses	No. of devices on local network	Use NAT of PAT?	Refer to …
1	more than 1	Use PAT.	5.8.4 - Configuring PAT on page 85
k (> 1)	more than k	Use NAT in combination with PAT.	5.8.7 - Combining PAT and NAT on page 91
at least k	k (≥ 1)	1. No translation needed. 2. If you want translation, use NAT.	1. Skip this section. 2. 5.8.6 - Configuring NAT on page 89

5.8.3 How does PAT work?

Example of a network topology for Internet connection

Consider the following network topology:

A Telindus 1420 SHDSL Router is installed at your site. The Internet Service Provider has an IP router with a high speed Frame Relay interface or one or more G.704 framed E1 interfaces running PPP. You received only one single official IP address from you ISP, being 195.7.12.22.



What does PAT do?

The Telindus 1420 SHDSL Router replaces the source address by its PAT address in all the traffic coming from the Ethernet and destined for the Internet. Depending on the IP transport protocol and the number of simultaneous users accessing the Internet, the Telindus 1420 SHDSL Router takes different actions.

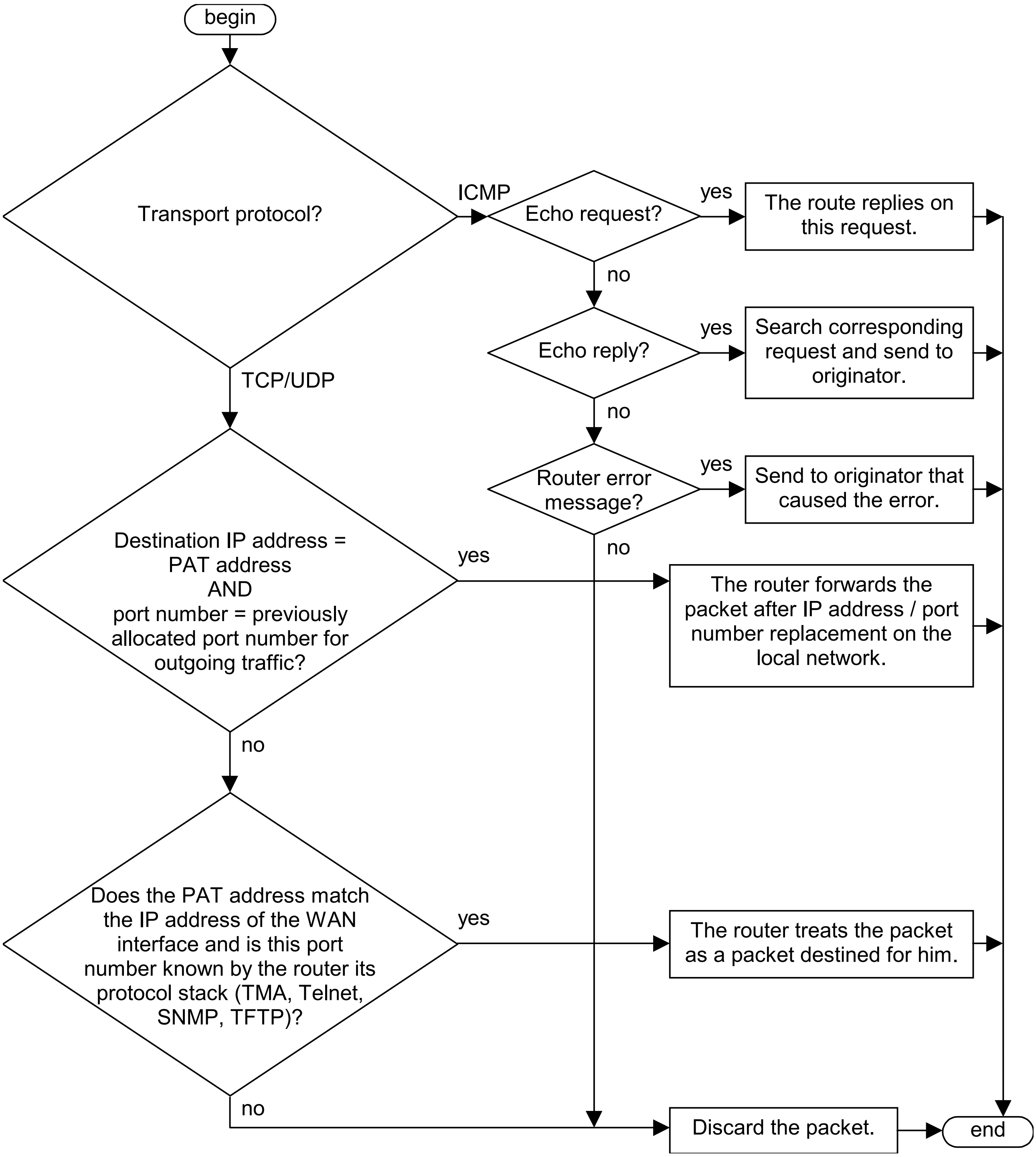
First, let us take a look at the different IP transport protocols:

Transport protocol	Description
TCP	This is a connection-oriented protocol: two devices communicating with the TCP protocol build a session before exchanging user data. When they have finished exchanging user data, the session is closed. Examples of such applications are Telnet, HTTP and FTP. The TCP header contains a *port* field indicating the higher-layer protocol.
UDP	This is a connection-less protocol: user data can be sent without first building a session. Examples of such applications are SNMP and TFTP. Although TFTP is session-oriented, it builds the session at a higher level and uses UDP for its simplicity as transport protocol. The UDP header contains a *port* field indicating the higher-layer protocol.
ICMP	This is a connection-less protocol: user data can be sent without first building a session. An example of such an application is ping. These protocols do not have port numbers.

As said before, depending on the IP transport protocol the Telindus 1420 SHDSL Router takes different actions. For the outgoing traffic towards the Internet, the following actions are taken:

Transport protocol	Action
TCP	When a session is started, a specific port number is assigned to this session. All traffic from this session is assigned this specific port number. The specific port number is freed within 5 minutes after the TCP session is closed (i.e. after TCP Reset or TCP Finish is seen). If the session has not been properly closed, the port number is freed 24 hours after the last session traffic. This time is configurable (refer to the attribute shdslRouter/router/natTcpSocketTimeOut on page 183).
UDP	The Source Port Number is replaced by a specific port number. All traffic from this source IP address / port number pair is assigned this specific port number. If there is no traffic for 5 to 10 minutes, the specific port number is freed.
ICMP	Each ICMP packet is forwarded towards the Internet. Each ICMP packet is considered as a new session. If there is no traffic for 5 to 10 minutes, the session is closed. The fact that it is possible to open a total of 2048 simultaneous sessions and that each ICMP packet is considered as a new session, implies that for instance a continuous series of ping requests at a rate of one per second will allocate between 300 and 600 sessions.

Suppose the WAN IP network depicted in Example of a network topology for Internet connection on page 82 works in numbered mode[1]. The incoming traffic from the Internet may be destined either for the local network, or for the Telindus 1420 SHDSL Router itself. The router treats incoming traffic on the PAT address as follows:



1. Numbered mode means that each WAN interface has an IP address. In that case, you need the single official IP address for your WAN interface.

5.8.4 Configuring PAT

Use the following attributes to configure PAT.

shdslRouter/router/patAddress

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to define the Port Address Translation address.

The PAT address is always an official IP address. Entering an address different from the default value 0.0.0.0 automatically enables PAT.

In the network depicted in Example of a network topology for Internet connection on page 82, assign the IP address 195.7.12.22 to the PAT address. In this case, it is the same address as on your WAN interface.

shdslRouter/router/natGateways

Default:<empty>
Range: table, see below

Use this attribute to define the gateway addresses from routes on which NAT or PAT should be applied.

If you are connected over a leased line to the ISP, then this table should contain only one gateway address: the IP address of the router at the ISP.

In the network depicted in Example of a network topology for Internet connection on page 82, the natGateways table should only contain the gateway addresses 195.7.12.254. However, if you already defined your defaultRoute to be 195.7.12.254, then you can leave the natGateways table empty. This because if the natGateways table is empty, then the defaultRoute is taken as only gateway addresses.

5.8.5 PAT limitations

Example of PAT and multiple remote networks over Frame Relay

Now, consider the following network topology:

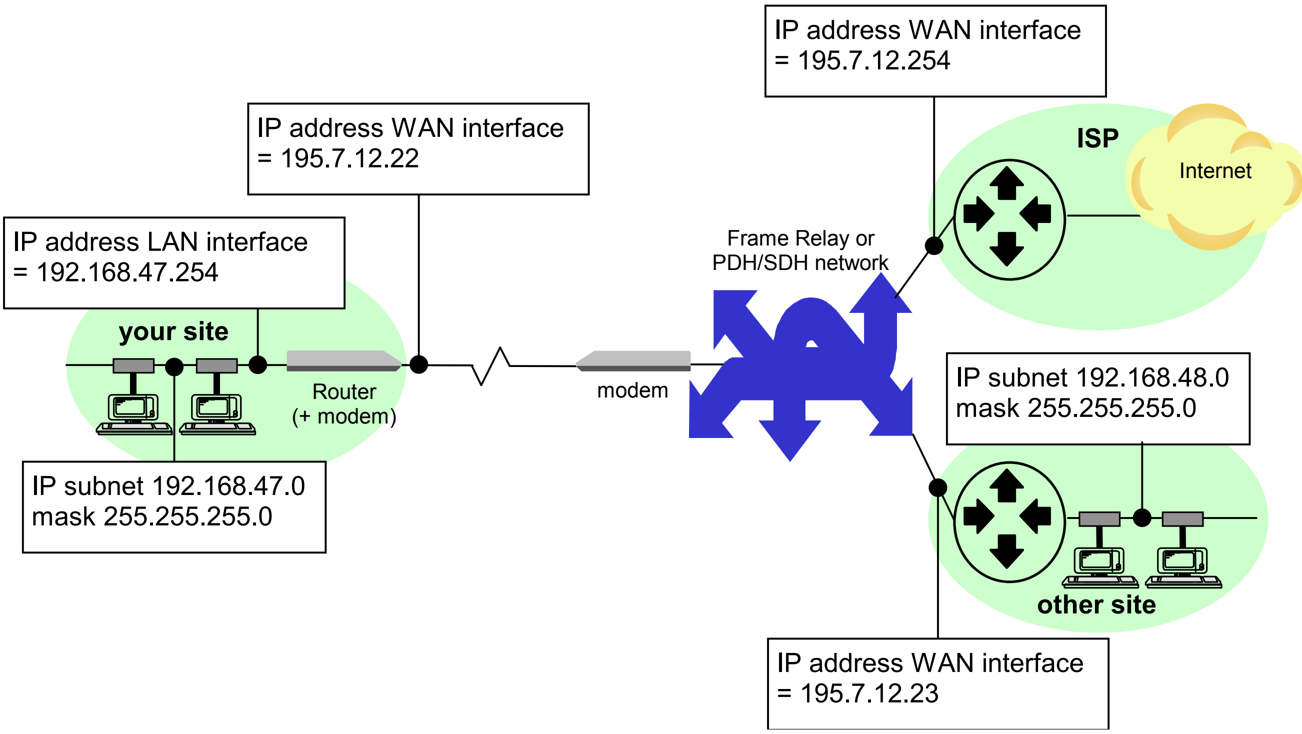
Your network is connected to the Internet via a Frame Relay network and to another site that does not have official IP addresses either.

Now you can choose whether to apply PAT to:

- all traffic towards the Frame Relay network

or

- the traffic destined for the Internet only.



In this example, PAT is only used for the traffic destined for the Internet. In that case, the configuration of the most relevant attributes of the router object is as follows:

```
SELECT router
      {
      LIST
        {
        defaultRoute = {gateway = 195.7.12.254     interface = wan}
        routingTable =
          {
          [a] = {  network = 192.168.48.0    gateway = 195.7.12.23    }
          }
        patAddress = 195.7.12.22
        }
      }
```

As you can see, the natGateways table is left empty since the Internet traffic uses the default route.

PAT limitations

As seen from the previous, Port Address Translation has some limitations:

- Only outgoing sessions are supported. This implies that you can not access servers on your local network over the Internet.
- Some TCP or UDP applications do not support port translation.
- Limited ICMP support.

PAT limitation workaround

The next attributes partly overcome the limitations of PAT.

---

shdslRouter/router/portTranslations

Default:<empty>
Range: table, see below

Use this attribute to define specific port number ranges that should not be translated.

Some TCP or UDP applications do not allow port translations: these applications require a dedicated source port number. In the portTranslations table you can define UDP and TCP port ranges that should not be translated. If a packet with a source port number in such a range is received, PAT replaces only the source IP address provided it is the first device using this port number. When other devices using the same application (hence the same port number) try to send traffic to the same Internet destination address, PAT discards this traffic.

It is also possible to define port ranges that PAT should always discard. The port translation range PAT uses goes from 60928 up to 65535.

The portTranslations table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>protocol</td><td>This selects the protocol: tcp or udp.
Default:tcp
Range: tcp / udp</td></tr>
<tr><td>startPort</td><td>This defines the lowest value of the TCP or UDP port range.
Default:0
Range: 0 … 65535</td></tr>
<tr><td>endPort</td><td>This defines the highest value of the TCP or UDP port range.
Default:<Opt>
Range: 0 … 65535
If no endPort value is defined (<Opt>), then the port range is limited to the startPort value only.</td></tr>
<tr><td>action</td><td>If a packet is received with a source port number in the previously specified range, a certain action can be taken.
Default:noTranslation
Range: enumerated, see below
The action element has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>noTranslation</td><td>The port numbers that fall within the defined port range are not translated.</td></tr>
<tr><td>deny</td><td>Packets with port numbers in that fall within the defined port range are discarded.</td></tr>
</table></td></tr>
</table>

Example of a portTranslations table

TMA is an example of an application that does not support port translation. If you want to make TMA connections from your local network to the outside world, you have to list TMA port number 1728 in this table. However, keep in mind that even then it is still not possible to have two simultaneous TMA sessions to the same outside world address.

portTranslations

	protocol	startPort	endPort	action
1	udp	1728	<Opt>	no translation
2	udp	2000	3000	deny

If you do not want that UDP packets with port numbers in the range 2000 up to 3000 are sent to the outside world, then you also have to include those in the table.

shdslRouter/router/servicesAvailable

Default:<empty>
Range: table, see below

Use this attribute to define specific port number ranges for incoming Internet traffic that should not be translated. Instead it is sent to the corresponding private IP address.

The servicesAvailable table makes it possible to have a server on the local network that can be accessed from the Internet, although it has no official IP address.

The servicesAvailable table contains the following elements:

Element	Description
protocol	This selects the protocol: tcp or udp. Default:tcp Range: tcp / udp
startPort	This defines the lowest value of the TCP or UDP port range. Default:0 Range: 0 … 65535
endPort	This defines the highest value of the TCP or UDP port range. Default:<Opt> Range: 0 … 65535 If no endPort value is defined (<Opt>), then the port range is limited to the startPort value only.
serverAddress	This sets the private server address. Default:0.0.0.0 Range: up to 255.255.255.255 If a packet is received with a source port number in the previously specified range, it is sent to the private server address.

Example of a servicesAvailable table

In this example, a web server with address 192.168.47.250 on the local network is accessible from the Internet using the PAT address instead of using the server address.

servicesAvailable

	protocol	startPort	endPort	serverAddress
1	tcp	80	<Opt>	192.168.47.250

5.8.6 Configuring NAT

Despite the workarounds offered by the previous two PAT configuration attributes to overcome the limitations of PAT, there are situations where PAT is inadequate. For example, it is not possible to have several web servers on your local network. It is also impossible to run an application with fixed source port numbers on several local devices that are connected simultaneously to a single Internet device. This can only be solved by using several official IP addresses: Network Address Translation.

Use the following attributes to configure NAT.

shdslRouter/router/natAddresses

Default:<empty>
Range: table, see below

Use this attribute to define all the official IP addresses. Entering an address in the table automatically enables NAT.

The natAddresses table contains the following elements:

Element	Description
officialAddress	This is the official IP address. These addresses are used in the reverse order as they appear in the list.
privateAddress	This is the private IP address. Use this element to permanently assign an official IP address to a private address.

How does the NAT address table work?

If a local station sends data to the Internet for the first time, NAT looks for an unused official IP address. It assigns this official IP address to the local station. The amount of local stations that can have simultaneous Internet access equals the amount of NAT addresses you defined. If all sessions between a local station and the Internet have been closed by the application (in case of TCP) or because of time-outs, then the previously assigned official IP address is freed for another local station.

Optionally, the NAT address entry may contain a corresponding private IP address. This allows to permanently assign an official IP address to a local station. This is useful for stations or servers that should have Internet access at all times. Another example of permanently assigned official IP addresses is a network where only a limited number of users has Internet access.

NAT only converts IP addresses and thus allows traffic in both directions. However, incoming traffic on one of the official IP addresses can only be forwarded to the local network if a corresponding private IP address has been configured.

Example of a natAddresses table

In this example, the first address is continuously assigned to a server with IP address 192.168.47.250. The others are assigned dynamically.

natAddresses

	officialAddress	privateAddress
1	195.7.12.21	192.168.47.250
2	195.7.12.22	<Opt>
3	195.7.12.23	<Opt>
4	195.7.12.24	<Opt>

shdslRouter/router/natGateways

Default:<empty>
Range: table, see below

Use this attribute to define the gateway addresses from routes on which NAT or PAT should be applied.

For more information, refer to shdslRouter/router/natGateways on page 85.

Important remark - using NAT on the LAN interface

Suppose the following configuration:

- shdslRouter/lanInterface/ipAddress = 172.31.74.1
- shdslRouter/router/natAddresses → first row → officialAddress = 172.31.74.1 privateAddress = <opt>
- shdslRouter/wanInterface/ipAddress = 2.2.2.2

The above means that NAT is used on the LAN interface and the router uses the address 172.31.74.1 as official IP address.

The problem that arises here is that the router can no longer be managed via the LAN interface using the management tool (TMA, Telnet, etc.). This because the NAT route has priority over the LAN route and, because it is a NAT address, the router does not accept incoming traffic on the address 172.31.74.1.

The solution is to add the WAN IP address to the natAddresses table as private address: shdslRouter/router/natAddresses → officialAddress = 172.31.74.1 privateAddress = 2.2.2.2. In that case, the management tool “service” runs on the WAN IP address. This means however, that the WAN has to be up.

5.8.7 Combining PAT and NAT

It is possible to use a combination of PAT and NAT. However, make sure the PAT address does not appear in the NAT address table.

How does the PAT / NAT combination work?

The router first assigns NAT addresses until they are all used. Then it uses PAT addresses for further translations.

5.9 Configuring bridging

This section explains how to configure the bridging functionality of the Telindus 1420 SHDSL Router. The following gives an overview of this section:

5.9.1 Enabling bridging

If you want to use the bridging functionality of the Telindus 1420 SHDSL Router, you have to activate it. Do this on both the LAN and WAN interface.

Enabling bridging on the LAN interface

shdslRouter/lanInterface/bridgePortInfo/bridging

Default:disabled
Range: enabled / disabled

Use the bridging element of the bridgePortInfo structure to enable or disable bridging on the LAN interface.

shdslRouter/lanInterface/routing

Default:enabled
Range: enabled / disabled

Use this attribute to determine whether IP packets are treated by the bridging process or not.

The routing attribute has the following values:

Value	Description
enabled	IP packets are passed directly to the routing process. IP packets not destined for the router its MAC address are discarded.
disabled	The IP packets are first passed to the bridging process. If necessary, IP packets destined for the router itself are passed on to the routing process. If the routing attribute is set to disabled, it is possible to have an IP subnet that spans multiple interfaces (or the LAN interface and some DLCIs).

Enabling bridging on the WAN interface

On the WAN interface, bridging and routing have to be configured for each encapsulation protocol separately:

Encapsulation	Attribute location
Frame Relay	In case of Frame Relay encapsulation, bridging and routing have to be set for each DLCI. • shdslRouter/wanInterface/frameRelay/dlciTable/bridgePortInfo/bridging • shdslRouter/wanInterface/frameRelay/dlciTable/routing
PPP	• shdslRouter/wanInterface/ppp/bridgePortInfo/bridging • shdslRouter/wanInterface/ppp/routing

5.9.2 Selecting a bridging protocol

shdslRouter/bridge/spanningTree/spanningTreeProtocol

Default:none
Range: enumerated, see below

Use the spanningTreeProtocol element of the spanningTree structure to select a bridging mechanism.

The spanningTreeProtocol element has the following values:

Value	Description
none	The Telindus 1420 SHDSL Router uses the self-learning principle. This means that the bridge itself learns which data it has to forward and which data it has to block. I.e. it builds its own bridging table.
IEEE p802.1D	The Telindus 1420 SHDSL Router uses the self-learning principle in conjunction with the Spanning Tree protocol. Because Spanning Tree bridging is somewhat more complicated than self-learning bridging, an introduction is given in 5.9.3 - What is Spanning Tree? on page 95.

When using Frame Relay encapsulation on the WAN interface together with the Spanning Tree protocol, every DLCI is considered as a separate bridge port. Each DLCI link is than considered as a special kind of LAN with only both end points connected.

5.9.3 What is Spanning Tree?

Spanning Tree

Spanning Tree is a link management protocol. Its primary goal is to provide path redundancy while preventing undesirable loops in the network.

Network loops are caused by multiple active paths between stations. If a loop exists in a network, stations might receive duplicate messages. In addition, bridges might learn MAC addresses on multiple ports. These conditions result in an unstable network.

The Spanning Tree algorithm

As said before, for a layer 2 Ethernet network to function properly, only one active path must exist between two stations. The Spanning Tree algorithm calculates the best loop-free path throughout a bridged network.

This single, loop-free path can only be established because the bridges in the network know of each others existence. They communicate with each other by sending and receiving Spanning Tree frames at regular intervals. The bridges do not forward these frames, but use them to construct a loop-free path.

5.9.4 What is the Spanning Tree root bridge?

The root bridge

Spanning Tree defines a tree with a root bridge and a loop-free path from the root to all bridges in the extended network. The root bridge is the logical centre of the Spanning Tree topology.

Redundant data paths are forced into a stand-by (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the stand-by path.

How is a root bridge selected?

All bridges in the network participating in Spanning Tree gather information about other bridges in the network. They do this through an exchange of data messages called Bridge Protocol Data Units (BPDUs).

This exchange of messages results in the following phases:

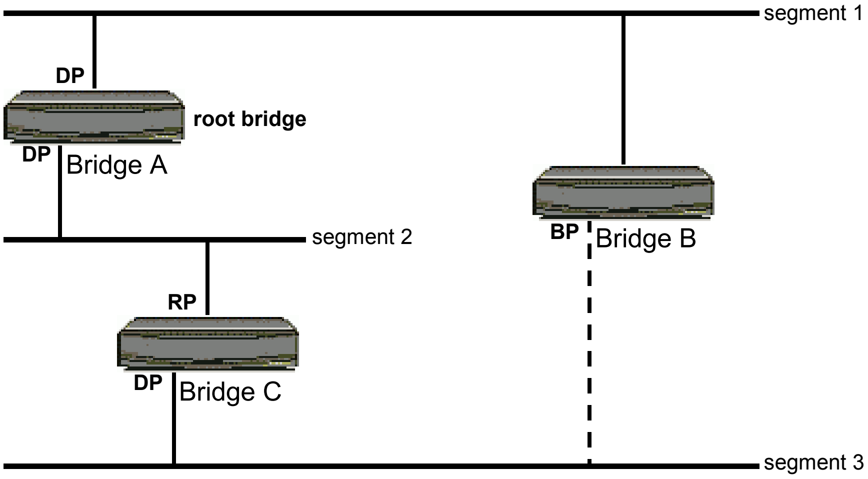
Phase	Description
1	The selection of a root bridge. The bridge with the highest bridge priority (i.e. the lowest numerical priority value) is selected as the root bridge. If all bridges are configured with the default priority (32768), the bridge with the lowest MAC address becomes the root bridge.
2	The selection of a designated bridge for every bridged LAN segment.
3	The removal of loops in the bridged network by blocking bridge ports connected to redundant links.

5.9.5 Spanning Tree topology

The cost factor is used to calculate the distance from each port of a bridge to the root bridge. On the basis of this, each port on a bridge is assigned one of the following states:

State	Description
root port	The port that is closest to the root bridge. Only one port on each bridge is assigned as the root port.
designated port	The port that connects to bridges further away from the root bridge. The root bridge only has designated ports.
blocking	If a port is not assigned a root port or a designated port state, they are assigned a blocking state. Frames (with the exception of Configuration BPDUs) are not accepted or transmitted by the port when it is in the blocking state. The port can be said to be in stand-by.

An elementary example of a Spanning Tree topology is given in the figure below:



RP = Root Port
DP = Designated Port
BP = Blocking Port

What is a BPDU?

To establish a stable path, each bridge sends Configuration Bridge Protocol Data Units (BPDUs) to its neighbouring bridges. These Configuration BPDU messages contain information about the spanning tree topology. The contents of these frames only changes when the bridged network topology changes or has not been established.

Each Configuration BPDU contains the following minimal information:

- The unique bridge identifier of the bridge that the transmitting bridge believes to be the root bridge.
- The cost of the path to the root from the transmitting port.
- The unique port identifier of the transmitting port.

When a bridge transmits a BPDU frame, all bridges connected to the LAN on which the frame is transmitted receive the BPDU. When a bridge receives a BPDU, it does not forward the frame. Instead, it uses the information in the frame to:

- calculate a BPDU,
- initiate a BPDU transmission if the topology changes.

The propagation of Configuration BDPUs

When a bridged network is in a stable condition, switches continue to send Configuration BPDUs to its neighbouring bridges at regular intervals. Configuration BPDUs are transmitted down the spanning tree from designated ports to root ports. If a Configuration BPDU is not received by the root port of a bridge within a predefined time interval (for example, because a bridge along the path has dropped out), the port enters the listening state to re-determine a stable path.

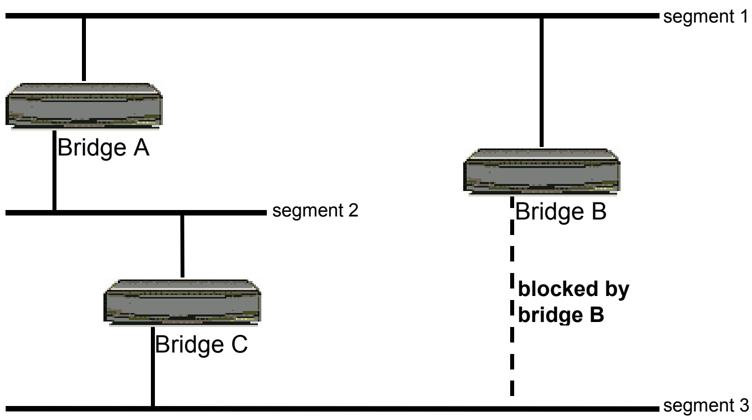
5.9.6 Spanning Tree behaviour

The following are some examples of how Spanning Tree behaves when certain events occur in your network.

Bridging loops

Bridges connected in a LAN must detect potential bridge loops. They must then remove these loops by blocking the appropriate ports to other bridges.

This is illustrated in the following figure:

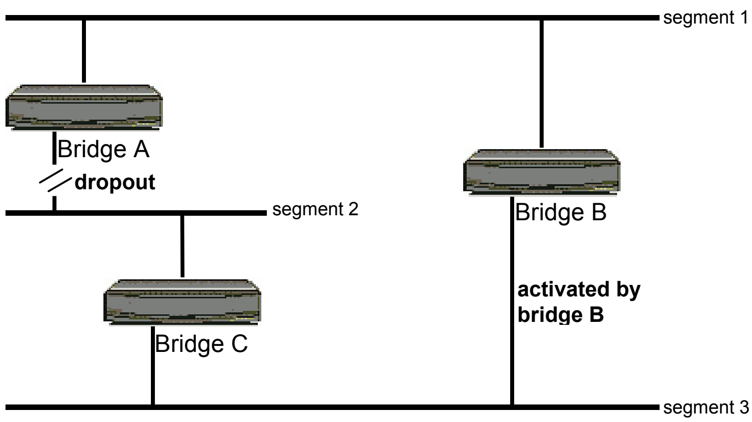


An alternate path has been established by connecting Bridge B in parallel with Bridges A and C. This also creates a potential bridge loop. However, by using the Spanning Tree Algorithm, Bridge B breaks the loop and blocks its path to segment 3.

Bridge failure

Bridges connected in a LAN must also detect bridge failure. They must then establish an alternative path. Should the root bridge fail, also a new root bridge must be selected.

A bridge failure is illustrated in the following figure:

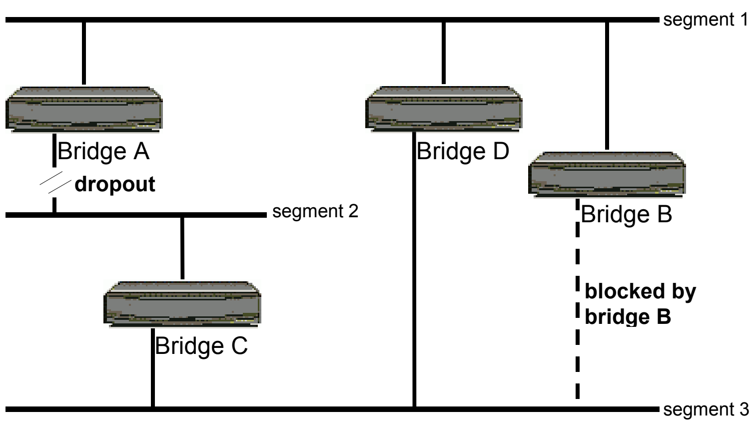


If Bridge A fails, the Spanning Tree Algorithm must be capable of activating an alternative path, such as Bridge B.

Network extension

Bridges connected in a LAN must also detect topology changes. They must adapt to these changes.

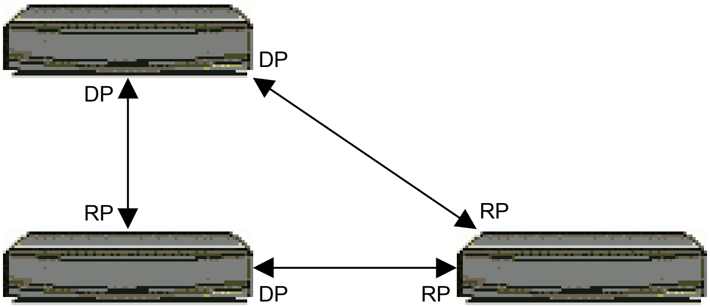
A topology change is illustrated in the following figure:



If the network is extended by adding Bridge D, the Spanning Tree Algorithm must be capable of adapting automatically to the new topology. This means that Bridge B stops looping by blocking the path to segment 3.

5.9.7 What is Spanning Tree priority and cost?

Consider the following Spanning Tree Topology:



RP = Root Port
DP = Designated Port

By means of the example above, the following table explains the terms *bridge priority*, *port priority* and *port* or *path cost*:

Term	Description
bridge priority	In the example above, Bridge A is selected as the root bridge. This because the bridge priority of all the bridges is set to the default value (32768) and Bridge A has the lowest MAC address. However, due to traffic patterns or link types, Bridge A might not be the ideal root bridge. By increasing the bridge priority (lowering the numerical priority value) of the ideal bridge so that it becomes the root bridge, you force a Spanning Tree recalculation to form a new spanning-tree topology with the ideal bridge as the root.
port priority and path cost	When the spanning-tree topology is calculated based on default parameters, the path between source and destination stations in a bridged network might not be ideal. The goal is to make the fastest link the root port. For example, assume on Bridge B that … • port 1, currently the root port, is an unshielded twisted-pair link, • port 2 is a fibre-optic link. Network traffic might be more efficient over the high-speed fibre-optic link. By changing the spanning-tree port priority or path cost for port 2 to a higher priority (lower numerical value) than port 1, port 2 becomes the root port.

5.9.8 Setting Spanning Tree priorities and costs

Setting the bridge priority

shdslRouter/bridge/spanningTree/bridgePriority

Default:32768
Range: 0 … 65535

The bridgePriority element of the spanningTree structure forms a unique bridge identifier together with the bridge its MAC address. This identifier is used to determine which bridge becomes the root bridge.

The bridge with the lowest bridgePriority value becomes the root bridge. If two bridges have the same bridgePriority value, then the bridge with the lowest MAC address becomes the root bridge.

Setting the port priority and path cost on the LAN interface

shdslRouter/lanInterface/bridgePortInfo/priority

Default:128
Range: 0 … 255

Each port of a bridge has a *unique port identifier*. The priority element of the bridgePortInfo structure is a part of this port identifier and allows you to change the priority of the port. It is taken as the more significant part in priority comparisons.

The other part of the unique port identifier has a fixed relationship to the physical or logical port. This assures the uniqueness of the unique port identifier among the ports of a single bridge.

shdslRouter/lanInterface/bridgePortInfo/pathCost

Default:100
Range: 1 … 65535

The pathCost element of the bridgePortInfo structure is the value that is added to the total cost of the path to the root bridge, provided that this particular port is a root port, i.e. that the path to the root goes through this port.

The total cost of the path to the root bridge should not exceed 65500.

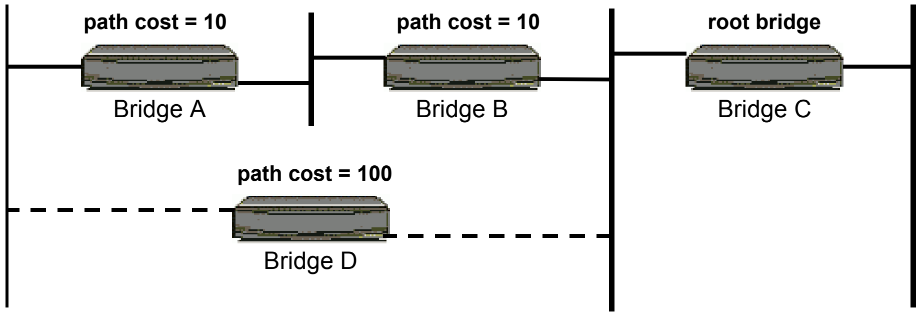
Setting the port priority and path cost on the WAN interface

On the WAN interface, priority and pathCost have to be configured for each encapsulation protocol separately:

Encapsulation	Attribute location
Frame Relay	In case of Frame Relay encapsulation, priority and pathCost have to be set for each DLCI. • shdslRouter/wanInterface/frameRelay/dlciTable/bridgePortInfo/priority • shdslRouter/wanInterface/frameRelay/dlciTable/bridgePortInfo/pathCost
PPP	• shdslRouter/wanInterface/ppp/bridgePortInfo/priority • shdslRouter/wanInterface/ppp/bridgePortInfo/pathCost
HDLC	• shdslRouter/wanInterface/hdlc/bridgePortInfo/priority • shdslRouter/wanInterface/hdlc/bridgePortInfo/pathCost

Example

By changing the priority and/or the pathCost, you can create a "preferred" path:



By setting the path costs of Bridge A and B to a lower value than the path cost of Bridge D, you can create a *preferred* path through Bridge A and B. The path through Bridge D becomes the *back-up* path.

5.9.9 Detecting Spanning Tree topology changes

Detecting Spanning Tree topology changes on the LAN interface

shdslRouter/lanInterface/bridgePortInfo/topologyChangeDetection

Default:enabled
Range: enabled / disabled

The topologyChangeDetection element of the bridgePortInfo structure enables or disables the communication of Spanning Tree topology changes to the root bridge:

Value	If a change in topology is detected by or notified to the bridge via this port, …
enabled	then the bridge communicates this to the root bridge.
disabled	then the bridge does not communicate this to the root bridge.

Detecting Spanning Tree topology changes on the WAN interface

On the WAN interface, topologyChangeDetection has to be configured for each encapsulation protocol separately:

Encapsulation	Attribute location
Frame Relay	In case of Frame Relay encapsulation, topologyChangeDetection has to be set for each DLCI. • shdslRouter/wanInterface/frameRelay/dlciTable/bridgePortInfo/topologyChangeDetection
PPP	• shdslRouter/wanInterface/ppp/bridgePortInfo/topologyChangeDetection
HDLC	• shdslRouter/wanInterface/hdlc/bridgePortInfo/topologyChangeDetection

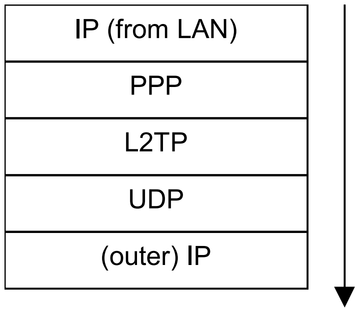
5.10 Configuring tunnelling

This section explains how you can configure the Layer 2 Tunnelling Protocol (L2TP) on the Telindus 1420 SHDSL Router. First it introduces L2TP and explains some L2TP terminology.

The following gives an overview of this section:

5.10.1 How does the Layer 2 Tunnelling Protocol work?

Suppose a packet coming from the LAN has a destination address for a network that is accessible through a tunnel. The following happens:

Phase	Description
1	The packet goes through the routing decision process. If the result of this decision is a route which uses the tunnel interface, then the packet is encapsulated in PPP first, then L2TP, UDP and finally IP. 
2	Then the packet goes through the routing decision process again. This time using the outer IP header.
3	The packet is routed over the Internet using the outer IP header.
4	The packet is received in the tunnel's end point, where it is then routed again using the original IP header.

5.10.2 L2TP terminology

The following table gives some specific L2TP terminology:

Term	Description
L2TP Access Concentrator (LAC)	A node that acts as one side of an L2TP tunnel. It is a peer to the L2TP Network Server (LNS). Packets sent from the LAC to the LNS require tunnelling with the L2TP protocol.
L2TP Network Server (LNS)	A node that acts as one side of an L2TP tunnel. It is a peer to the L2TP Access Concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunnelled from the remote system by the LAC.
Tunnel	A tunnel exists between a LAC-LNS pair. The tunnel consists of a Control Connection and zero or more L2TP sessions. The tunnel carries encapsulated PPP datagrams and Control Messages between the LAC and the LNS.
Control Connection	A control connection operates in-band over a tunnel to control the establishment, release, and maintenance of sessions and of the tunnel itself.
Control Messages	Control messages are exchanged between LAC and LNS pairs, operating in-band within the tunnel protocol. Control messages govern aspects of the tunnel and sessions within the tunnel.

5.10.3 Setting up a tunnel

shdslRouter/router/tunnels/l2tpTunnels

Default:<empty>
Range: table, see below

Use this attribute to configure the Layer 2 Tunnelling Protocol tunnels you want to set up.

The l2tpTunnels table contains the following elements:

Element	Description
name	This is the name of the tunnel. Default:<empty> Range: max. 64 characters The tunnel name is used in status and performance information to distinguish the different tunnels from one another.
adminStatus	This activates (up) or deactivates the tunnel (down). Default:down Range: up / down
ip	Use this structure to assign IP addresses to the tunnel. For more information, refer to shdslRouter/router/tunnels/l2tpTunnels/ip on page 189.
bridging	Use this structure to configure the bridging feature in the tunnel. For more information, refer to the configuration attribute shdslRouter/lanInterface/bridgePortInfo on page 157. When bridging is enabled on a tunnel interface, the tunnel acts exactly as a bridge port for a physical PPP connection.
l2tp	Use this structure to configure the L2TP properties of the tunnel. For more information, refer to shdslRouter/router/tunnels/l2tpTunnels/l2tp on page 190.

5.11 Configuring the priority and traffic policy

This section explains how you can configure the priority and traffic policy on the Telindus 1420 SHDSL Router. First it gives an introduction. Then it shows how to add the priorityPolicy and trafficPolicy objects to the containment tree.

The following gives an overview of this section:

5.11.1 What is priority policy?

The purpose of a priority policy is to determine, on overload conditions, the data that will be given the highest priority (i.e. serviced first and discarded last).

Priority policy may be used in a variety of ways e.g. to ensure that voice, video or other streaming media is serviced before (or after) other traffic types, to ensure that web response traffic is routed before normal web browsing traffic, etc.

5.11.2 What is a priority queue?

A mechanism used in priority policy is priority queuing. This means that the user can decide which data goes into which priority queue.

There are 7 priority queues:

Queue	Queue type	Description
1 - 5	configurable queue	The user can decide which data goes into which queue.
6	low delay queue	This queue is always addressed between every user configurable queue.
7	system queue	This queue is filled with link monitoring messages etc. and has priority over all other queues.

5.11.3 Queuing routed and bridged data

The following table shows how the Telindus 1420 SHDSL Router queues routed and bridged data:

In case … is enabled,	then …
only routing	the routed data is queued as specified in the traffic policy settings.
routing and bridging	• the routed data is queued as specified in the traffic policy settings. • the bridged data is sent to queue 1.
only bridging	priority queuing is not applicable.

5.11.4 What is traffic policy?

The purpose of a traffic policy is to determine exactly which data is sent to which queue.

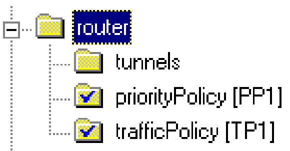
5.11.5 Adding a policy object

The priorityPolicy and trafficPolicy objects are not present in the containment tree by default. If you want to use priority and traffic policy, then you have to add these objects first. Proceed as follows:

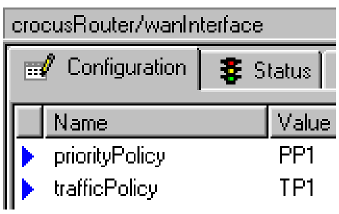
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Start a management session on the Telindus 1420 SHDSL Router (e.g. TMA, ATWIN, CLI, etc.).</td></tr>
<tr><td>2</td><td>Go to the router object.
<table>
<tr><th>In case of …</th><th>Proceed as follows …</th></tr>
<tr><td>TMA</td><td>Right click on the router object. A pop-up menu appears. In this menu, select Add Child… and select the object you want to add. A pop-up window appears. In this window, type the instance value for the object and click on OK.</td></tr>
<tr><td>ATWIN</td><td>Use the CREATE INSTANCE command. Type the instance value for the object.</td></tr>
<tr><td>CLI</td><td>Use the following command:
<code>set {select objectName[instanceValue]{}}</code>, where <code>instanceValue</code> is a string of your choice.
Example: <code>set {select priorityPolicy[PP1]{}}</code></td></tr>
<tr><td>WEB if</td><td>Use the CREATE INSTANCE command. Type the instance value for the object.</td></tr>
</table>
⇒ The new object appears.</td></tr>
<tr><td>3</td><td>The instance values you defined for the priorityPolicy and trafficPolicy objects also have to be entered in the priorityPolicy and trafficPolicy attributes located in the wanInterface object.
The following example will clarify this.</td></tr>
</table>

Example

Suppose you create a priorityPolicy object with the instance value PP1 and a trafficPolicy object with the instance value TP1. The containment tree would look as depicted at the right:



Now, enter these instance values of these objects in the wanInterface object. This would look as follows:



5.11.6 Configuring the priority policy

shdslRouter/router/priorityPolicy[ ]/algorithm

Default:fifo
Range: enumerated, see below

Use this attribute to determine which mechanism is used to queue the data when the Telindus 1420 SHDSL Router experiences an overload condition.

The algorithm attribute has the following values:

Value	Description
fifo	This is a First In First Out queue. The data that enters the queue first, also leaves the queue first. This is the fastest but most superficial queuing mechanism.
roundRobin	This is a priority queuing mechanism. In this case, all queues containing data have an equal weight, disregarding the setting of the weight element in the shdslRouter/router/priorityPolicy[ ]/queueConfigurations attribute.
absolutePriority	This is a priority queuing mechanism. In this case, queues with a high priority have *absolute* priority over queues with a low priority. In other words, no lower priority queue is emptied as long as a higher priority queue contains data. The priority of the queues runs parallel to the queue number. I.e. the user configurable queue number 1 has the lowest priority, whereas the system queue (number 7) has the highest priority. For the queue numbers refer to 5.11.2 - What is a priority queue? on page 109. Note that there is a risk of *starvation*. This means that it is possible that the lower weight queues are never emptied because a higher weight queue continuously receives data.
weightedFair-Queueing	This is a priority queuing mechanism. In this case, the queues are emptied based on their weight. The weight can be configured in the shdslRouter/router/priorityPolicy[ ]/queueConfigurations attribute. **Example** Suppose queue 1 has weight 2, queue 2 has weight 1 and both queues contain data. In that case the queues are emptied in the following order: queue 1 → queue 1 → queue 2 → queue 1 → queue 1 → queue 2 → etc.

Priority queuing

The options roundRobin, absolutePriority and weightedFairQueueing are priority queuing mechanisms. In order to determine which data goes into which priority queue, use the shdslRouter/router/trafficPolicy[ ]/method attribute. The queues themselves can be configured using the shdslRouter/router/priorityPolicy[ ]/queueConfigurations attribute.

shdslRouter/router/priorityPolicy[ ]/countingPolicy

Default:bytes
Range: enumerated, see below

Use this attribute to define whether the quotum of the queues is expressed in bytes or packets.

shdslRouter/router/priorityPolicy[ ]/queueConfigurations

Default:<empty>
Range: table, see below

Use this attribute to set the relative importance of the user configurable queues.

The queueConfigurations table contains the following elements:

Element	Description
quotum	This sets the number of bytes/packets that is dequeued from the user configurable queue when the queue is addressed. Default:1500 Range: 1 … 25000 The unit of the quotum (bytes or packets) can be set with the shdslRouter/router/priorityPolicy[ ]/countingPolicy attribute.
weight	This sets the relative importance of the queue. Default:1 Range: 1 … 10 The weight element is only relevant in case the shdslRouter/router/priorityPolicy[ ]/algorithm attribute is set to absolutePriority or weightedFairQueueing.

shdslRouter/router/priorityPolicy[ ]/lowdelayQuotum

Default:50
Range: 1 … 25000

This sets the number of bytes/packets that is dequeued from the low delay queue when the queue is addressed. For more information on the low delay queue, refer to 5.11.2 - What is a priority queue? on page 109.

The unit of the quotum (bytes or packets) can be set with the shdslRouter/router/priorityPolicy[ ]/countingPolicy attribute.

5.11.7 Configuring the traffic policy

shdslRouter/router/trafficPolicy[ ]/method

Default:trafficShaping
Range: enumerated, see below

Use this attribute to choose a method for redirecting the data to a specific queue.

The method attribute has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>trafficShaping</td><td>The data is redirected to the queues based on the settings of the attribute shdslRouter/router/trafficPolicy[ ]/trafficShaping.</td></tr>
<tr><td>tosDiffServ</td><td>The data is redirected to the queues based on DiffServ (refer to RFC2597) regarding class and drop precedence.

This means that, depending on their Type Of Service (TOS) field, some packets are moved to other queues and/or dropped sooner than other packets in case the queue is full.

The highest 3 bits of the TOS field are mapped as follows:
<table>
<tr><th>Bit values …</th><th>are mapped to …</th></tr>
<tr><td>000 up to 100</td><td>queues 1 up to 5, respectively.</td></tr>
<tr><td>101 and higher</td><td>the low delay queue.</td></tr>
</table>
The next 2 bits define the drop precedence:
<table>
<tr><th>Bit values …</th><th>correspond with …</th></tr>
<tr><td>00 and 01</td><td>maxLength1.</td></tr>
<tr><td>10</td><td>maxLength2.</td></tr>
<tr><td>11</td><td>maxLength3.</td></tr>
</table>
For more information on drop precedence, refer to the attribute shdslRouter/router/trafficPolicy[ ]/dropPrecedence.</td></tr>
<tr><td>tosMapped</td><td>The data is redirected to the queues based on the settings of the attribute shdslRouter/router/trafficPolicy[ ]/tos2QueueMapping.</td></tr>
</table>

shdslRouter/router/trafficPolicy[ ]/dropPrecedence

Default:-
Range: table, see below

Use this attribute to define for each user configurable queue, how many packets with a certain drop level may be queued before they are dropped.

The dropPrecedence table contains the following elements:

Element	Description
maxLength1	This is the maximum length or drop level 1. Default:100 Range: 1 … 3000 In case you set the attribute shdslRouter/router/trafficPolicy[ ]/method to … • trafficShaping or tosMapped, then only this drop level is relevant. • tosDiffServ, then this drop level corresponds with the drop precendence bits value 00 and 01.
maxLength2	This is the maximum length or drop level 2. Default:100 Range: 1 … 3000 In case you set the attribute shdslRouter/router/trafficPolicy[ ]/method to … • trafficShaping or tosMapped, then this drop level is not relevant. • tosDiffServ, then this drop level corresponds with the drop precendence bits value 10.
maxLength3	This is the maximum length or drop level 3. Default:100 Range: 1 … 3000 In case you set the attribute shdslRouter/router/trafficPolicy[ ]/method to … • trafficShaping or tosMapped, then this drop level is not relevant. • tosDiffServ, then this drop level corresponds with the drop precendence bits value 11.

Example

Suppose …

- the shdslRouter/router/trafficPolicy[ ]/method is set to tosDiffServ.
- for queue 1 you set maxLength1 = 100, maxLength2 = 200 and maxLength3 = 50.

Now the following applies:

Queue 1 contains … data packets.	**An incoming data packet with … is …**		
	drop level[1] 1	**drop level 2**	**drop level 3**
less than 50	accepted	accepted	accepted
more than 50, less than 100	accepted	accepted	dropped
more than 100, less than 200	dropped	accepted	dropped
more than 200	dropped	dropped	dropped

1. As defined in the TOS field.

shdslRouter/router/trafficPolicy[ ]/trafficShaping

Default:<empty>
Range: table, see below

In case you have set the shdslRouter/router/trafficPolicy[ ]/method attribute to trafficShaping, then use the trafficShaping table to specify which data has to be redirected to which queue.

The trafficShaping table can be compared with an access list. You can “filter” based on several criteria (IP source and destination address, TOS value, etc.). A packet is redirected to the specified queue when the criteria are met and an overload condition occurs. When more than one entry applies to the same packet, then only the most specific one is taken in consideration. I.e. the entry covering the smallest range.

The trafficShaping table contains the following elements:

Element	Description
sourceIpStart-Address	This is the IP source address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
sourceIpEnd-Address	
destinationIpStart-Address	This is the IP destination address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
destinationIpEnd-Address	
tosStartValue	This is the Type Of Service field value. Default:any(start)/optional(end) Range: 0 … 256
tosEndtValue	
ipProtocol	This is the protocol field from the IP header. Default:any Range: 0 … 255 You can specify the protocol by typing the protocol number. For ease of use, some common protocols can be selected from a drop-down box: any (0), ICMP (1), IGMP (2), IPinIP (4), TCP (6), EGP (8), IGP (9), UDP (17), RSVP (46), IGRP (88), OSPFIGP (89), TCPestablished (255).
sourcePortStart	This is the source port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: any or optional (0), echo (7), discard (9), ftp-data (20), ftp (21), telnet (23), smtp (25), domain (53), www-http (80), pop3 (110), nntp (119), snmp (161), snmptrap (162), z39.50 (210), syslog (514), router (520), socks (1080), l2tp (1701), telindus (1728).
sourcePortEnd	

Element	Description
destinationPortStart destinationPortEnd	This is the destination port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: see above.
newTosValue	This is the new TOS field value. Default:unchanged Range: 0 … 256 When you select a new TOS field value, then a packet that matches an entry in the trafficShaping table its TOS field value is changed and the packet is redirected to a queue. Selecting unchanged, leaves the TOS field value as it is.
priority	This is the destination queue for a packet matching an entry in the trafficShaping table. Default:Queue1 Range: enumerated, see below The priority element has the following values: Queue1, Queue2, Queue3, Queue4, Queue5, lowDelayQueue.

Start and end values

Except for the ipProtocol, newTosValue and priority elements, it is possible to specify ranges using the start and end values. There are two special cases:

- A start value is entered, but no end value ⇒ an exact match is needed for the start value.
- Neither a start nor an end value is entered ⇒ the field is not checked.

shdslRouter/router/trafficPolicy[ ]/tos2QueueMapping

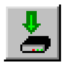
Default:<empty>
Range: table, see below

In case you have set the shdslRouter/router/trafficPolicy[ ]/method attribute to tosMapped, then use the tos2QueueMapping table to specify which data has to be redirected to which queue.

The tos2QueueMapping table contains the following elements:

Element	Description
startTos endTos	Traffic that has a Type Of Service field value within the specified range is redirected to the specified queue. Default:0 (start) / 255 (end) Range: 0 … 255
targetQueue	This is the destination queue for a packet matching an entry in the tos2QueueMapping table. Default:Queue1 Range: enumerated, see below The targetQueue element has the following values: Queue1, Queue2, Queue3, Queue4, Queue5, lowDelayQueue.

5.12 Activating the configuration

Once the basic configuration of the Telindus 1420 SHDSL Router is made, it has to be activated. Do this by clicking on the the *Send all attributes to device* button in TMA: .

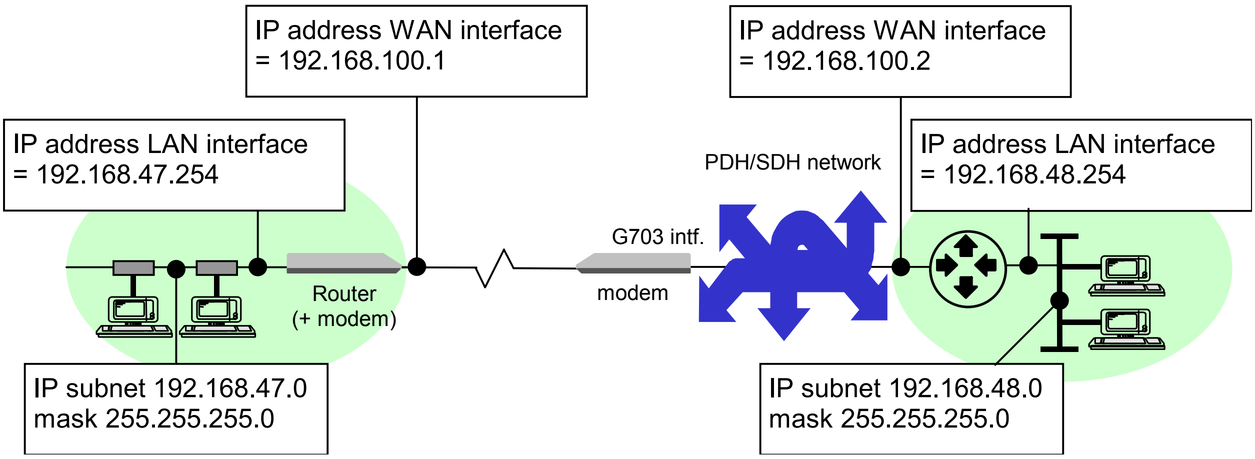
6 Configuration examples

This chapter shows some configuration examples for the Telindus 1420 SHDSL Router. The following gives an overview of this chapter:

6.1 LAN extension over a PDH/SDH network

In this example, a remote office is connected to a central office over a PDH or SDH network.

A modem link connects the remote office to the PDH or SDH network. At the local office a Telindus 1420 SHDSL Router is installed. The central router is a third party router. The WAN encapsulation is PPP with active link monitoring.



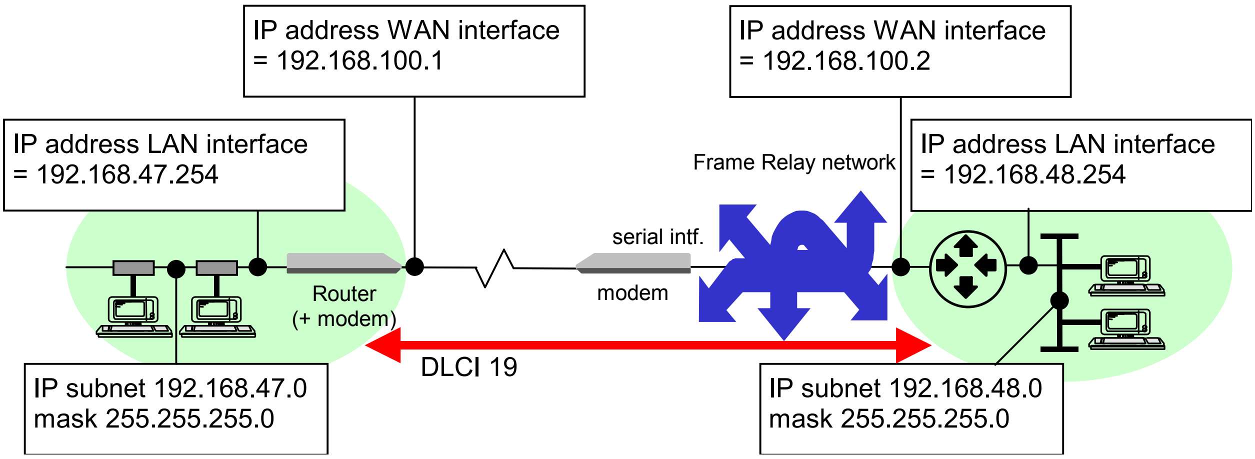
The configuration of the Telindus 1420 SHDSL Router in CLI format is as follows:

```
ACTION "Load Default Configuration"
SET
    {
    SELECT lanInterface
      {
      LIST
        {
        ipAddress = 192.168.47.254
        }
      }
    SELECT wanInterface
      {
      LIST
        {
        ipAddress = 192.168.100.1
        encapsulation = ppp
        }
      SELECT ppp
        {
        LIST
          {
          linkMonitoring = {  operation = enabled    }
          }
        }
      }
    SELECT router
      {
      LIST
        {
        routingTable =
          {  [a]  = {  network = 192.168.48.0    gateway = 192.168.100.2    }  }
        }
      }
    }
ACTION "Activate Configuration"
```

6.2 LAN extension over a Frame Relay network

In this example, a remote office is connected to a central office over a Frame Relay network.

A modem link connects the remote office to the Frame Relay network. At the local office a Telindus 1420 SHDSL Router is installed. The central router is a third party router. The Frame Relay network uses LMI according to the ANSI standard. No inverse ARP is supported by the network.



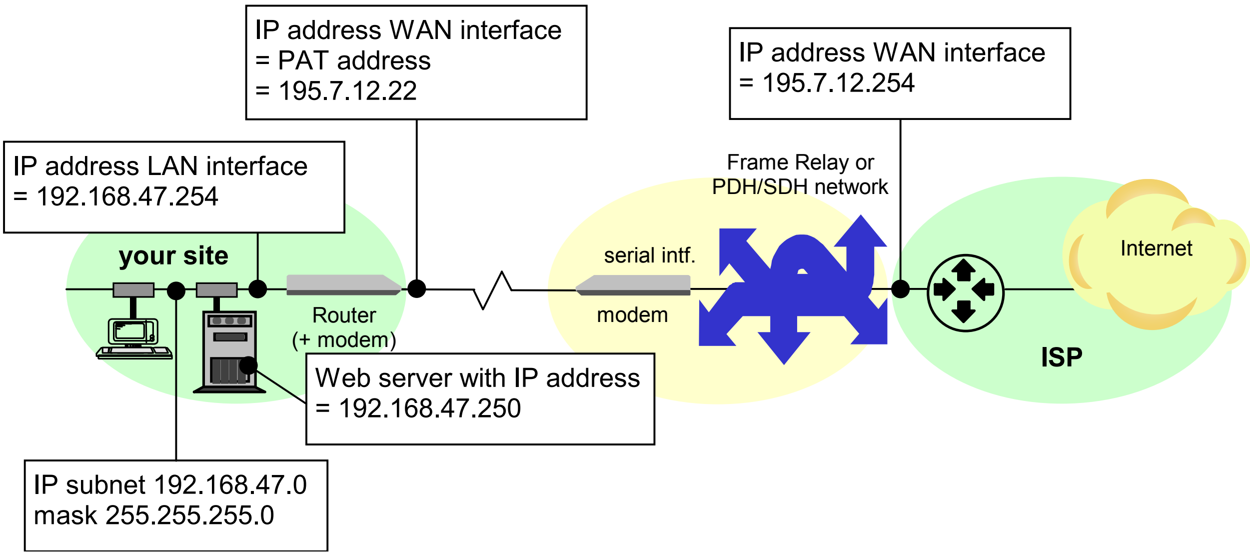
The configuration of the Telindus 1420 SHDSL Router in CLI format is as follows:

```
ACTION "Load Default Configuration"
SET
    {
    SELECT lanInterface
      {
      LIST
        {
        ipAddress = 192.168.47.254
        }
      }
    SELECT wanInterface
      {
      LIST
        {
        ipAddress = 192.168.100.1
        }
      SELECT frameRelay
        {
        LIST
          {
          lmi = {   type = ansit1-617-d     }
          dlciTable =
            {  [a] = {   dlci = 19     gateway = 192.168.100.2     }   }
          }
        }
      }
    SELECT router
      {
      LIST
        {
        routingTable =
          {  [a]  = {   network = 192.168.48.0     gateway = 192.168.100.2     }   }
        }
      }
    }
ACTION "Activate Configuration"
```

6.3 Connecting a LAN to the Internet using NAT and PAT

This is an example of a local network that only uses private addresses.

A PPP link connects your site to the Internet Service Provider. At your site a Telindus 1420 SHDSL Router is installed. You only received 2 official IP addresses from the ISP, one for all outgoing traffic using PAT (195.7.12.22) and one for accessing the local web server using NAT (195.7.12.21) with a dedicated private address.



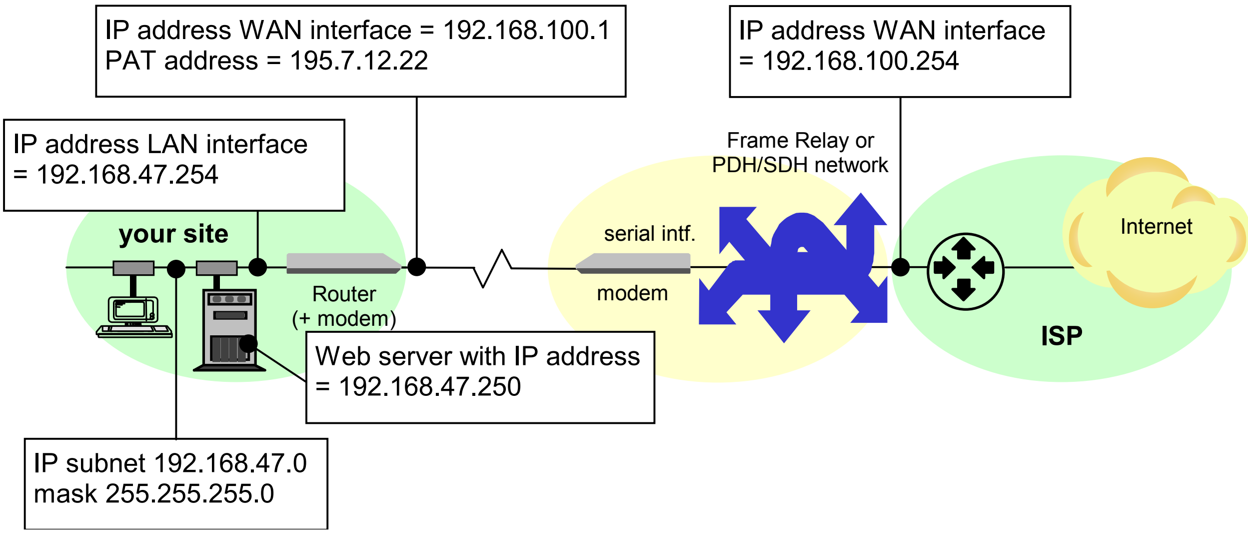
The configuration of the Telindus 1420 SHDSL Router in CLI format is as follows:

```
ACTION "Load Default Configuration"
SET
    {
    SELECT lanInterface
      {
      LIST
        {
        ipAddress = 192.168.47.254
        }
      }
    SELECT wanInterface
      {
      LIST
        {
        ipAddress = 195.7.12.22
        encapsulation = ppp
        }
      }
    SELECT router
      {
      LIST
        {
        defaultRoute = {  gateway = 195.7.12.254    interface = wan     }
        patAddress = 195.7.12.22
        natAddresses =
          {
          [a]  = {officialAddress = 195.7.12.21 privateAddress = 192.168.47.250 }
          }
        }
      }
    }
ACTION "Activate Configuration"
```

6.4 Using PAT over PPP with a minimum of official IP addresses

This is another example of a local network that only uses private addresses.

A PPP link connects your site to the Internet Service Provider. At your site a Telindus 1420 SHDSL Router is installed. You only received 1 official IP address from the ISP. To reduce the number of official IP addresses, the ISP also uses private IP addresses on the PPP link. The central router its routing table has a host route to its PAT address per customer.

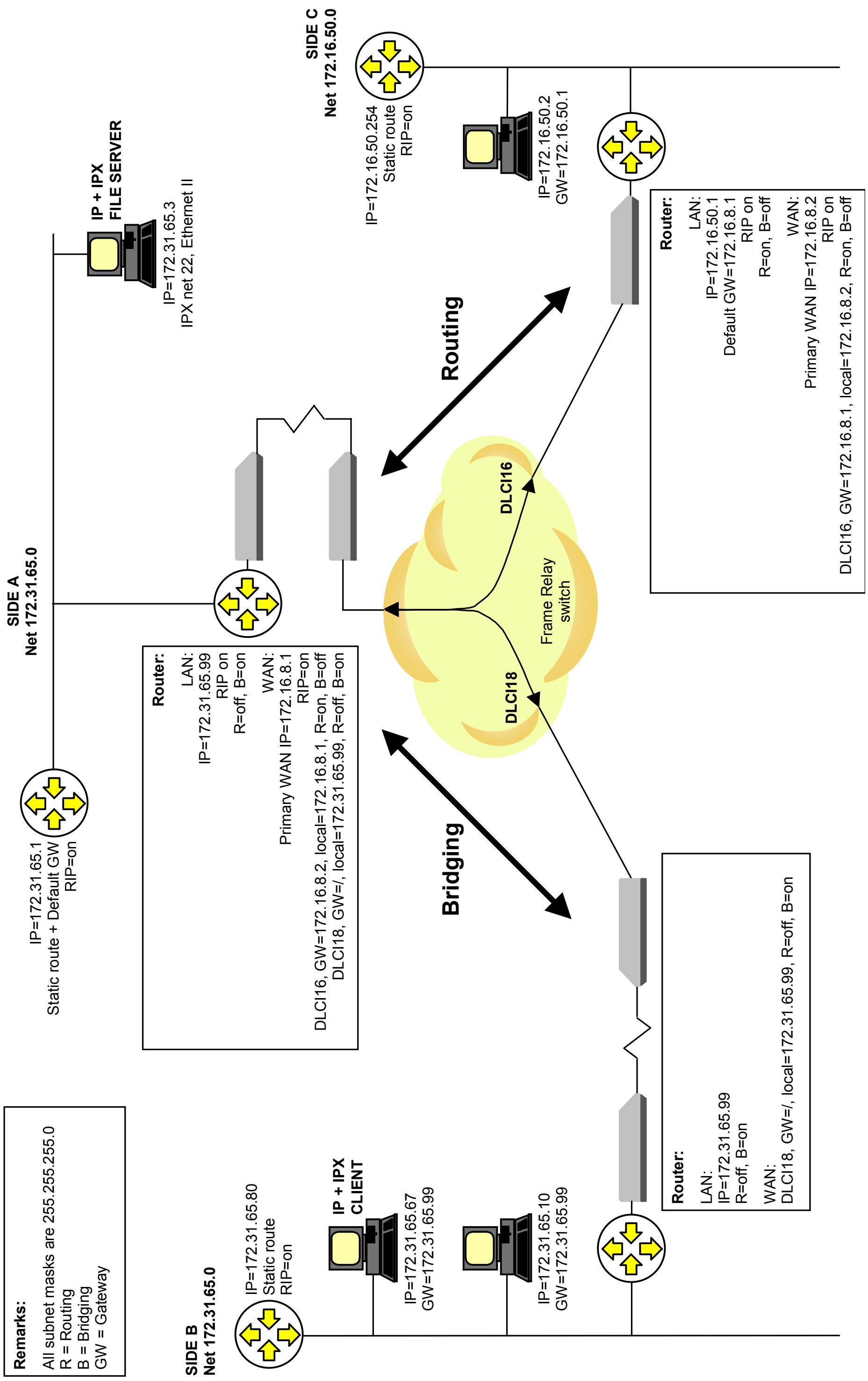


The configuration of the Telindus 1420 SHDSL Router in CLI format is as follows:

```
ACTION "Load Default Configuration"
SET
    {
    SELECT lanInterface
      {
      LIST
        {
        ipAddress = 192.168.47.254
        }
      }
    SELECT wanInterface
      {
      LIST
        {
        ipAddress = 192.168.100.1
        encapsulation = ppp
        }
      }
    SELECT router
      {
      LIST
        {
        defaultRoute = {  gateway = 192.168.100.254    interface = wan    }
        patAddress = 195.7.12.22
        }
      }
    }
ACTION "Activate Configuration"
```

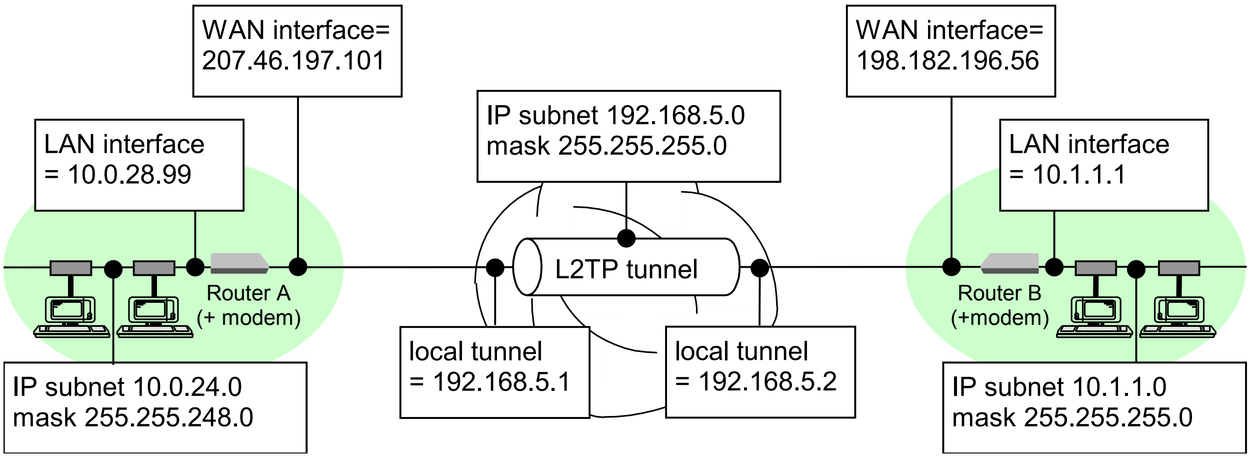
6.5 Bridging and routing in a network

The example on the following page shows a combination of bridging and routing in a network.



6.6 Tunnelling in a network

The following figure gives an example of a tunnel set-up.



Configuring the tunnels/l2tpTunnels table

The following shows how the tunnels/l2tpTunnels table would look like for Router A:

```
>get l2tpTunnels[1]
  l2tpTunnels[1] =
    {
    name = "Outgoing Tunnel 1"
    adminStatus = up
    ip =
      {
      ipAddress = 192.168.5.1
      ipNetMask = 255.255.255.0
      ipGateway = 192.168.5.2
      ripMode = disabled
      }
    bridging =
      {
      bridging = disabled
      priority = 128
      pathCost = 500
      topologyChangeDetection = enabled
      }
    l2tp =
      {
      localIpAddress = 192.168.0.1
      remoteIpAddress = 192.168.0.2
      pppAuthentication = enabled
      type = outgoingLeasedLine
      dataChannelSequenceNumbering = off
      keepAliveTimeOut = 25
      l2tpType = auto
      tunnelAuthentication = on
      tunnelSecret = "tunnel1"
      maxNrOfRetransmissions = 4
      transmitWindowSize = 4
      receiveWindowSize = 4
      udpChecksum = off
      }
    }
```

Configuring a route through the tunnel

Once the tunnel is set up, it is easy to configure a route through this tunnel. Just use the remote IP address of the tunnel as gateway for the network you want to reach:

```
>get routingTable
  routingTable =
    {
    [a] =
      {
      network = 10.1.1.0
      mask = 255.255.255.0
      gateway = 192.168.5.2
      interface = <OPT>
      preference = 10
      metric = 2
      }
    }
```

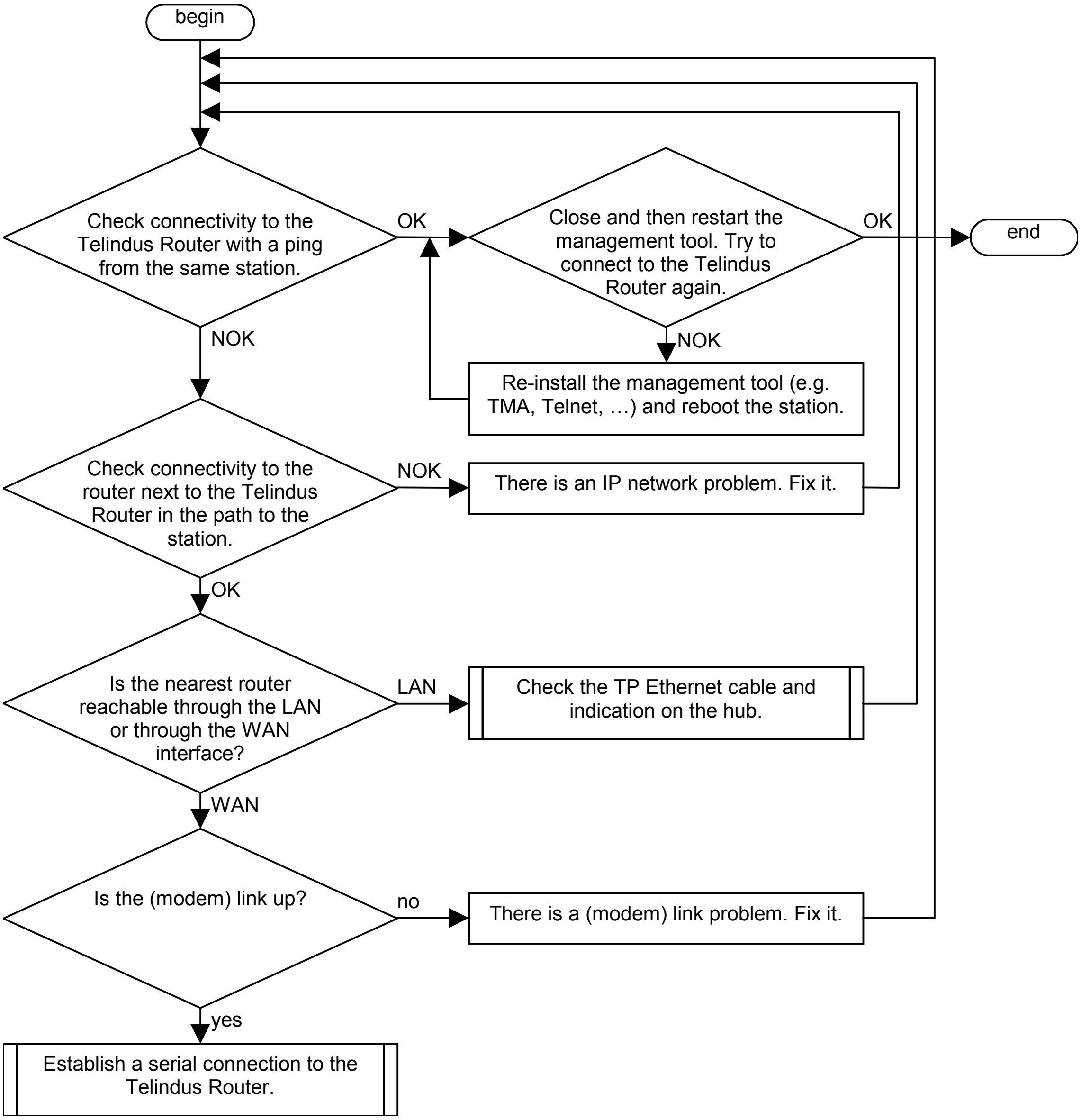
7 Troubleshooting

If you experience problems with establishing a connection to the Telindus 1420 SHDSL Router or with its configuration, you may find the answer to your problem in this chapter.

The following gives an overview of this chapter:

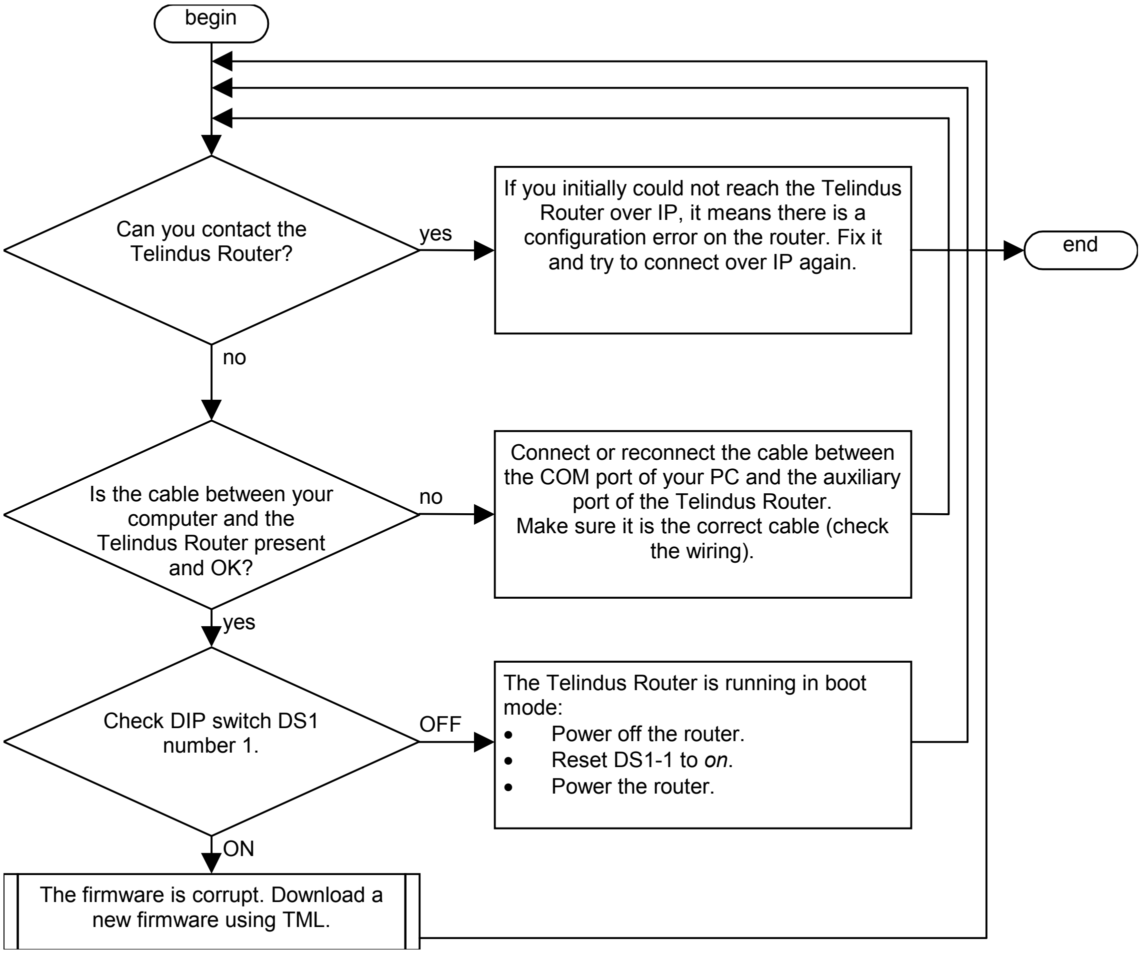
7.1 You can not contact the Telindus 1420 SHDSL Router over an IP connection

If you can not establish an IP connection between your computer running the management tool (e.g. TMA, Telnet, …) and the Telindus 1420 SHDSL Router, then follow the procedure below:



7.2 You can not contact the Telindus 1420 SHDSL Router over a serial connection

If you can not establish a serial connection between your computer running the management tool (e.g. TMA, Telnet, …) and the Telindus 1420 SHDSL Router, then follow the procedure below:



7.3 How to troubleshoot the configuration?

In case of configuration problems you can take a look at the status and performance attributes of the Telindus 1420 SHDSL Router. These attribute values are continuously calculated and stored in the memory of the Telindus 1420 SHDSL Router.

Status and performance information can be used for the following:

- In case of configuration errors, status information may be useful to locate the error.
- If network problems arise, information about the history of the communication link can be reviewed and analysed. These statistics can be useful to locate and solve the problem.
- By collecting performance information, an operator can keep track of the global performance of the network, e.g. network bottlenecks can be traced, etc.

A complete description of all status and performance attributes can be found in the reference manual. In the following sections, you find the most important status attributes that you can check in case the Telindus 1420 SHDSL Router does not function as expected.

7.4 How to check the status of the LAN interface?

If the data traffic does not pass the Telindus 1420 SHDSL Router, then check whether the LAN interface is up and running.

If you connected the Telindus 1420 SHDSL Router to an Ethernet hub or directly to a network station, you can easily check whether the Ethernet connection is OK.

The status attribute ifOperStatus

If you are connected to the Telindus 1420 SHDSL Router with a management tool, simply look at the status of the ifOperStatus attribute.

shdslRouter/lanInterface/fOperStatus

This attribute displays the current operation status of the LAN interface. Possible values are:

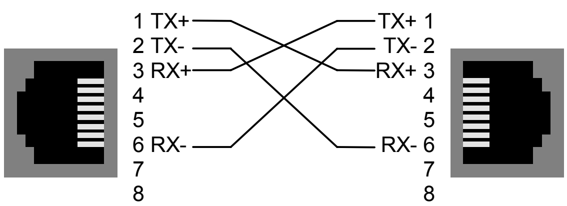
Value	Description
up	The LAN interface is up, data transfer is possible.
down	The LAN interface is down, data transfer is not possible.

The status of the LAN LEDs

Check the status of the LAN LEDs to verify whether data can be sent to or received from the LAN.

What to do if the LAN interface is down?

In case the LAN interface is down, you could check the following:

Step	Action
1	Check whether the Telindus 1420 SHDSL Router is operational. If the front panel LEDs light up and if you can connect TMA, it is working.
2	Check the cable that connects the Telindus 1420 SHDSL Router with the Ethernet hub or the network station: • Is it connected? • Is it connect at both sides?
3	Check the wiring of the cable that connects the Telindus 1420 SHDSL Router with the Ethernet hub or the network station. The wiring should be as follows: • a straight cable when connected to an Ethernet hub, • a crossed cable when connected to a network station. The following figure shows a cross cable: 

Step	Action
4	Replace the cable you are using by another, similar one. Perhaps the RJ45 contacts are not good.
5	Check whether the Ethernet hub or Ethernet card of the network station is operational.

7.5 How to check the status of the WAN interface?

If the data traffic does not pass the Telindus 1420 SHDSL Router, then check whether the WAN interface is up and running.

Similar to the status of the LAN interface, you can check the status of the WAN interface by means of a status attribute or a front panel LED.

The status attribute ifOperStatus

If you are connected to the Telindus 1420 SHDSL Router with a management tool, simply look at the status of the ifOperStatus attribute.

shdslRouter/lanInterface/ifOperStatus

This attribute displays the current operation status of the WAN interface. Possible values are:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>up</td><td>The WAN interface is up, data transfer is possible.

The following table shows you in which case the value of the ifOperStatus attribute is up:

<table><tr><th>Protocol</th><th>The ifOperStatus attribute is up (i.e. the alarm wanInterface/alarmInfo/linkDown = off) in case …</th></tr><tr><td>Frame Relay</td><td>LMI is up.</td></tr><tr><td>PPP</td><td>LCP is open.</td></tr></table></td></tr>
<tr><td>down</td><td>The WAN interface is down, data transfer is not possible.</td></tr>
</table>

Important remarks

- Whether the Telindus 1420 SHDSL Router is configured in bridging or routing has no effect on the value of the attributes shdslRouter/wanInterface/ifOperStatus:Status and shdslRouter/wanInterface/alarmInfo/linkDown:Alarms.
- In case of Frame Relay, if the configuration attribute element shdslRouter/wanInterface/frameRelay/lmi/type is set to noLmiConfigured, then the value of the attribute shdslRouter/wanInterface/frameRelay/lmi/state:Status is always up. However, the other conditions as stated in the table above remain.
- In case of PPP, if the configuration attribute element shdslRouter/wanInterface/ppp/linkMonitoring/operation is set to disabled, then it is possible that the ifOperStatus value does not go down even if the link quality is too bad for a proper data link. This because the link monitoring mechanism is the only PPP mechanism that will start a renegotiation of the LCP layer.

The status of the WAN LEDs

Check the status of the LEDs TXD and RXD to verify whether data can be sent to or received from the WAN.

What to do if the WAN interface is down?

In case the WAN interface is down, you could check the following steps:

Step	Action
1	Check whether the Telindus 1420 SHDSL Router is operational. If the front panel LEDs light up and if you can connect TMA, it is working.
2	Check the cable that connects the Telindus 1420 SHDSL Router with the line (WAN): • Is it connected? • Is it connect at both sides?
3	Check whether the link towards the WAN network is up.
4	If the WAN link is up but no data traffic passes and you use … • Frame Relay encapsulation, then check the Frame Relay status attributes. • PPP encapsulation, then check the PPP status attributes.

7.6 How to check the Frame Relay status?

If the connection to the Frame Relay network is not operational, you could verify the LMI protocol or the DLCI table of your WAN interface. Do this by checking the following attributes:

---

shdslRouter/lanInterface/frameRelay/lmi

This attribute gives a complete LMI status information overview.

The most important elements of the lmi structure are:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>state</td><td>This displays the current state of LMI. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>up</td><td>LMI messages can and are exchanged.</td></tr>
<tr><td>down</td><td>No LMI messages can be exchanged.</td></tr>
</table></td></tr>
<tr><td>lastStateChange</td><td>This is the system-up time when the LMI state entered its current state. I.e. the moment the value of the state element changes (from up to down or vice versa), the system-up time value is written into the lastStateChange element.</td></tr>
</table>

---

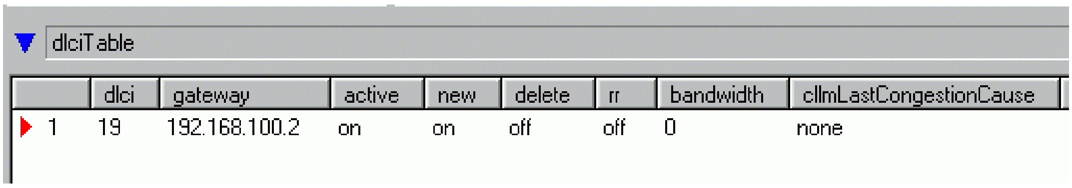
shdslRouter/lanInterface/frameRelay/dlciTable

This attribute gives the complete status information of all known DLCIs.

The most important elements of the dlciTable table are:

Element	Description
dlci	This is the DLCI identification number.
active	This indicates whether the corresponding DLCI is active (on) or not (off).

The following figure displays the DLCI table for the example in 6.2 - LAN extension over a Frame Relay network on page 121.


dlciTable

	dlci	gateway	active	new	delete	rr	bandwidth	cllmLastCongestionCause
1	19	192.168.100.2	on	on	off	off	0	none

7.7 How to check the PPP status?

If the connection to the PPP network is not operational, you could verify the states of the LCP, IPCP or BCP protocol. Do this by checking the following attributes:

shdslRouter/lanInterface/ppp/lcpState

This attribute reflects the status of the LCP (Link Control Protocol) protocol. Possible values are:

Value	Description
Initial	LCP handshake has not started yet.
Starting, Closed, Stopped, Closing, Stopping	These values correspond with the transient states in the LCP state diagram.
Req-Sent	The local side of the PPP link has sent an LCP request. The remote side did not answer yet.
Ack-Rcvd	The local side of the PPP link has received an LCP acknowledge from the remote side. This is a transient state.
Ack-Sent	The local side of the PPP link has acknowledged the LCP request from the remote side.
Opened	The LCP handshake succeeded.

If lcpState is something else than Initial or Opened, the problem is located in the LCP handshake. Also check the LCP state of the remote router. Possibly there is a compatibility problem with the LCP options.

shdslRouter/lanInterface/ppp/ipcpState

This attribute reflects the status of the IPCP (Internet Protocol Control Protocol) protocol. The possible values are the same as those of shdslRouter/lanInterface/ppp/lcpState.

If ipcpState is something else than Initial or Opened, the problem is located in the IPCP handshake. Also check the IPCP state of the remote router. Possibly there is a compatibility problem with the IPCP options.

shdslRouter/lanInterface/ppp/bcpState

This attribute reflects the status of the BCP (Bridging Control Protocol) protocol. The possible values are the same as those of shdslRouter/lanInterface/ppp/lcpState.

If bcpState is something else than Initial or Opened, the problem is located in the BCP handshake. Also check the BCP state of the remote router. Possibly there is a compatibility problem with the BCP options.

7.8 How to check the routing status?

If your LAN and WAN interfaces are up but the data is not routed as desired, you can verify the routing table status information.

shdslRouter/router/routingTable

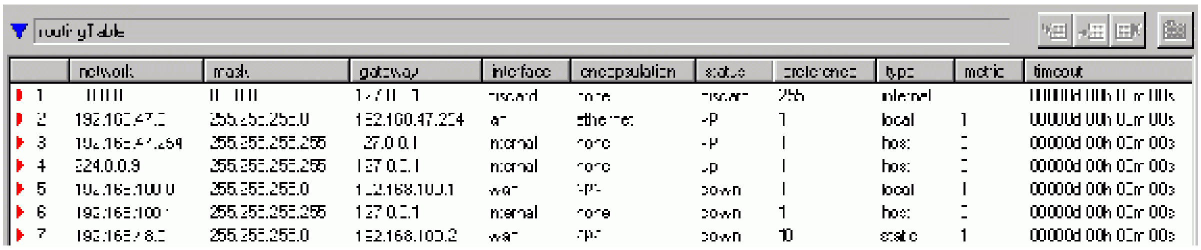
This attribute lists all known routes with their operating status. This information is retrieved from the configured IP addresses, the static routes and the interface status.

The routingTable contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>network</td><td>This is the IP address of the destination network.</td></tr>
<tr><td>mask</td><td>This is the network mask of the destination network.</td></tr>
<tr><td>gateway</td><td>This is the IP address of the next router on the path to the destination network.</td></tr>
<tr><td>interface</td><td>This is the interface through which the destination network can be reached. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>internal</td><td>The own protocol stack is used.</td></tr>
<tr><td>lan</td><td>The destination network can be reached through the Ethernet interface.</td></tr>
<tr><td>wan</td><td>The destination network can be reached through the serial interface.</td></tr>
<tr><td>discard</td><td>Packets for this destination are discarded.</td></tr>
</table></td></tr>
<tr><td>encapsulation</td><td>This indicates the used encapsulation. It is related to the interface for this route. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>none</td><td>The IP packets are not encapsulated.</td></tr>
<tr><td>ethernet</td><td>The IP packets are encapsulated with the ARPA MAC header.</td></tr>
<tr><td>frameRelay</td><td>The IP packets are encapsulated in Frame Relay (RFC 1490).</td></tr>
<tr><td>ppp</td><td>The IP packets are encapsulated in PPP.</td></tr>
<tr><td>x25</td><td>The IP packets are encapsulated in X.25.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>status</td><td>This is the route status. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>up</td><td>The route can be used.</td></tr>
<tr><td>down</td><td>The route is currently not in use.</td></tr>
<tr><td>discard</td><td>Packets for this destination are discarded.</td></tr>
</table></td></tr>
<tr><td>preference</td><td>This displays the route preference.
If more than one route matches the IP destination address, this attribute determines which route is used. The route with the lowest preference value will be used.</td></tr>
<tr><td>type</td><td>This is the type of the route. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>host</td><td>This is a host route, i.e. a route to a single IP address instead of a complete network. This is also used for the router its own IP address.</td></tr>
<tr><td>internal</td><td>A route with this status is irrelevant.</td></tr>
<tr><td>local</td><td>This route is for directly connected networks.</td></tr>
<tr><td>rip</td><td>This route has been received by a RIP update.</td></tr>
<tr><td>static</td><td>This route has been configured, i.e. it is a static route.</td></tr>
</table></td></tr>
<tr><td>metric</td><td>If two routes exist with the same preference, then the route with the lowest metric value is chosen. The metric attribute serves as a cost for using the route. In most cases it indicates the number of hops (= routers) required to reach a destination.</td></tr>
<tr><td>timeOut</td><td>In case of a RIP route, the timeOut attribute displays the time the route will remain in the routing table if no RIP updates are received anymore. For other routes this attribute always displays 00000d 00h 00m 00s.</td></tr>
</table>

The following figure displays the routing table for the example in 6.1 - LAN extension over a PDH/SDH network on page 120:



routingTable

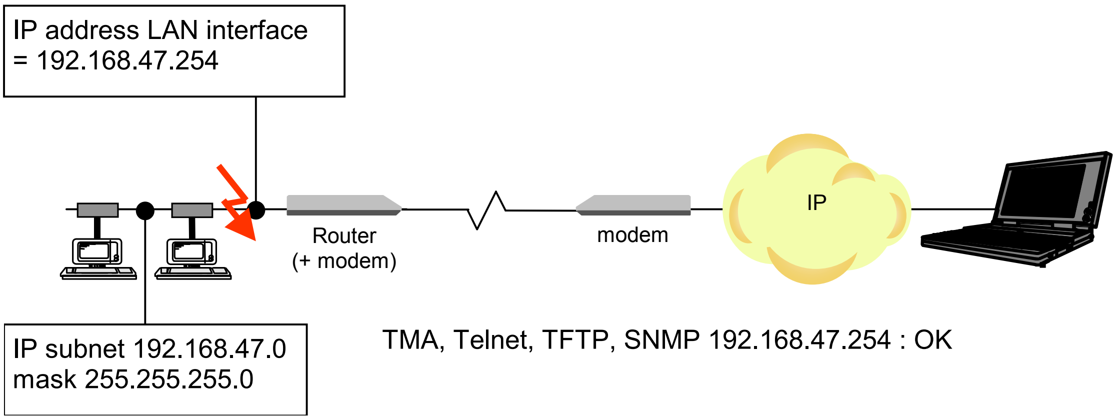
	network	mask	gateway	interface	encapsulation	status	preference	type	metric	timeout
1	0.0.0.0	0.0.0.0	127.0.0.1	discard	none	discard	255	internal		00000d 00h 00m 00s
2	192.168.47.0	255.255.255.0	192.168.47.254	lan	ethernet	up	1	local	1	00000d 00h 00m 00s
3	192.168.47.254	255.255.255.255	127.0.0.1	internal	none	up	1	host	0	00000d 00h 00m 00s
4	224.0.0.9	255.255.255.255	127.0.0.1	internal	none	up	1	host	0	00000d 00h 00m 00s
5	192.168.100.0	255.255.255.0	192.168.100.1	wan	ppp	down	1	local	1	00000d 00h 00m 00s
6	192.168.100.1	255.255.255.255	127.0.0.1	internal	none	down	1	host	0	00000d 00h 00m 00s
7	192.168.48.0	255.255.255.0	192.168.100.2	wan	ppp	down	10	static	1	00000d 00h 00m 00s

The lines in the routing table depicted above represent the following:

- Line 1 represents the default gateway, which is not defined.
- Lines 2 and 5 represent the subnets on the LAN and WAN interface respectively.
- Lines 3 and 6 represent the interface its IP addresses.
- Line 7 represents the static route to the remote LAN.
- Finally, line 4 represents the multicast address for RIP version 2.

Remark

The host routes to the local interface IP address are always up. The following figure illustrates this:



If the Ethernet LAN is not connected to the Telindus 1420 SHDSL Router, it is still possible to contact the Telindus 1420 SHDSL Router with e.g. TMA or Telnet over the WAN link by using the LAN IP address. It will however not respond on a ping made to its LAN IP address.

Reference manual

8 Configuration attributes

This chapter discusses the configuration attributes of the Telindus 1420 SHDSL Router. The following gives an overview of this chapter:

8.1 Configuration attribute overview

> shdslRouter
- sysName
- sysContact
- sysLocation
- bootFromFlash
- security
- alarmMask
- alarmLevel
- Action: Activate Configuration
- Action: Load Saved Configuration
- Action: Load Default Configuration
- Action: Cold Boot

>> lanInterface
- ipAddress
- ipNetMask
- secondaryIpAddresses
- routing
- metric
- ripMode
- rip2Authentication
- accessList
- extendedAccessList
- bridgePortInfo
- bridgeAccessList
- arpTimeOut
- directedBroadcasts
- ipHelpers
- sendIcmpRedirect
- lanWanStatusCoupling
- alarmMask
- alarmLevel

>> wanInterface
- ipAddress
- ipNetMask
- secondaryIpAddresses
- autoInstallMode
- priorityPolicy
- trafficPolicy
- metric
- ripMode
- rip2Authentication
- accessList
- extendedAccessList
- bridgeAccessList
- directedBroadcasts
- ipHelpers
- splitHorizon
- encapsulation
- alarmMask
- alarmLevel

>>> frameRelay
- dlciTable
- lmi

>>> ppp
- linkMonitoring
- authentication
- authenPeriod
- routing
- bridgePortInfo

>>> hdlc
- bridgePortInfo

>>> line
- channel
- speed
- retrain
- alarmMask
- alarmLevel

>> router

- defaultRoute
- routingTable
- routingProtocol
- alternativeRoutes
- ripUpdateInterval
- ripv2SecretTable
- sysSecret
- pppSecretTable
- helperProtocols
- sendTtlExceeded
- sendPortUnreachable
- sendAdminUnreachable
- patAddress
- portTranslations
- servicesAvailable
- natAddresses
- natGateways
- natTcpSocketTimeOut
- natUdpSocketTimeOut
- natTcpSockets
- natUdpSockets
- dhcpStatic
- dhcpDynamic
- dhcpCheckAddress
- alarmMask
- alarmLevel

>>> tunnels

- l2tpTunnels

>>> priorityPolicy[1]

- algorithm
- countingPolicy
- queueConfigurations
- lowdelayQuotum

>>> trafficPolicy[1]

- method
- dropPrecedence
- trafficShaping
- tos2QueueMapping

>> bridge

- spanningTree
- bridgeTimeOut

1. Not present by default, has to be added.

>> snmpProxy

- trapDestinations
- mib2Traps

>> management

- cms2Address
- accessList
- snmp
- telnet
- tftp
- consoleNoTrafficTimeOut
- ctrlPortProtocol
- alarmFilter

>>> loopback

- ipAddress

8.2 General configuration attributes

shdslRouter/sysName

Default:<empty>
Range: max. 64 characters

Use this attribute to assign a name to the Telindus 1420 SHDSL Router. The sysName attribute is an SNMP MIB2 parameter.

shdslRouter/sysContact

Default:<empty>
Range: max. 64 characters

Use this attribute to add contact information. You could, for instance, enter the name and telephone number of the person to contact in case problem occur.

The sysContact attribute is an SNMP MIB2 parameter.

shdslRouter/sysLocation

Default:<empty>
Range: max. 64 characters

Use this attribute to specify the physical location of the Telindus 1420 SHDSL Router. The sysLocation attribute is an SNMP MIB2 parameter.

shdslRouter/bootFromFlash

Default:auto
Range: enumerated, see below

If the Telindus 1420 SHDSL Router is equipped with only one flash memory bank, this attribute has no function. To verify how many flash memory banks are present in the Telindus 1420 SHDSL Router, check the status attribute shdslRouter/flashVersions.

Use this attribute to select which flash memory bank is active.

In case the Telindus 1420 SHDSL Router is equipped with two flash memory banks, each bank can contain a complete firmware version but only one version can be active. This allows you to download a new firmware version in the non-active flash bank, while the Telindus 1420 SHDSL Router continues operation from the active flash bank. It also allows you to switch between two different firmware versions.

The bootFromFlash attribute has the following values:

Value	When the Telindus 1420 SHDSL Router boots …
flash1	flash memory bank 1 is active.
flash2	flash memory bank 2 is active.
auto	the Telindus 1420 SHDSL Router automatically chooses the flash memory bank containing the most recent firmware. It does this by comparing the firmware version numbers.

shdslRouter/<configurationAlarmAttributes>

For more information on the configuration alarm attributes alarmMask and alarmLevel and on the alarms in general, refer to 11.2 - Introducing the alarm attributes on page 275.

For more information on the alarms of the shdslRouter object, refer to 11.3 - General alarms on page 278.

shdslRouter/security

Default:<empty>
Range: table, see below

Use this attribute to create a list of passwords with associated access levels in order to avoid unauthorised access to the Telindus 1420 SHDSL Router and the network.

The security table contains the following elements:

Element	Description
password	Enter here the password string. You can then associate this password with a certain access level. Default:<empty> Range: max. 10 characters
accessRights	Use this element to change the access levels associated with the password. It is a bit string of which each bit corresponds to an access level. The different access levels are: Default:111 Range: bit string, see below

Bit	If you set this bit to *on*, you are able to …
readAccess	read all attributes except the security attributes.
writeAccess	change all attributes except the security attributes. Neither can you read the security attributes. Some security related attributes, however, can be read but not changed.
securityAccess	read and change the security attributes.

Important remarks

- If you create no passwords, everybody has complete access.
- If you define at least one password, it is impossible to access the Telindus 1420 SHDSL Router with one of the management systems without entering the correct password.
- If you create a list of passwords, create at least one with write and security access. If not, you will be unable to make configuration and password changes after activation of the new configuration.

Security attributes

The Telindus 1420 SHDSL Router has the following security attributes:

- shdslRouter/security
- shdslRouter/lanInterface/accessList, extendedAccessList, bridgeAccessList and rip2Authentication
- shdslRouter/wanInterface/accessList, extendedAccessList, bridgeAccessList and rip2Authentication
- shdslRouter/wanInterface/ppp/authentication and authenPeriod
- shdslRouter/router/sysSecret, pppSecretTable and ripv2SecretTable
- shdslRouter/management/accessList, snmp, telnet and tftp

Entering passwords

The following table explains how to enter passwords in the different management systems:

Management system	How to enter the password?
TMA	Enter the password in the connect window.
TMA CLI and TMA for HP OpenView	Use the application *TmaUserConf.exe* to create a TMA user and assign a password to this user. The password should correspond with a password configured in the device. For more information refer to the manual of TMA CLI or TMA for HP Open-View.
TML	Enter the password after the destination file name. Separate password and file name by a '`?`'. Example: `tml -fsourcefile@destinationfile?pwd`
CLI	You are prompted to enter the password when the session starts.
ATWIN	You are prompted to enter the password when the CLI session starts. Then you can start an ATWIN session.
Web Interface	You are prompted to enter the password when the session starts.
TFTP	Enter the password after the destination file name. Separate password and file name by a '`?`'. Example: `put sourcefile destinationfile?pwd`
SNMP	Define the password as community string. If no passwords are defined, then you can use any string as community string.

Correcting the security table

If you forgot your password or you forgot to create one with write and security access, then you can set the Load Default Configuration DIP switch. As a result, the Telindus 1420 SHDSL Router reboots in its default configuration. You can then retrieve the erroneous configuration and correct it.

To correct the security table, proceed as follows:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Disconnect the power supply and open the housing as described in 3.4 - Changing DIP switch and strap settings on page 35.</td></tr>
<tr><td>2</td><td>Set DIP switch bank DS1 position 2 to off.

To locate this DIP switch bank, refer to 3 - DIP switches and straps of the Telindus 1420 SHDSL Router on page 31.</td></tr>
<tr><td>3</td><td>Replace the cover without fastening the screws and reconnect the power supply.

⇒ The Telindus 1420 SHDSL Router reboots and loads the default configuration.</td></tr>
<tr><td>4</td><td>Retrieve the erroneous configuration:
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Open a TMA session on the Telindus 1420 SHDSL Router. Refer to 4 - Managing the Telindus 1420 SHDSL Router on page 37.</td></tr>
<tr><td>2</td><td>Execute the Load Saved Configuration action.</td></tr>
<tr><td>3</td><td>Change the password and/or access rights in the security table.</td></tr>
<tr><td>4</td><td>Execute the Activate Configuration action.</td></tr>
</table></td></tr>
<tr><td>5</td><td>Again, disconnect the power supply and open the housing.</td></tr>
<tr><td>6</td><td>Reset DIP switch bank DS1 position 2 to on.</td></tr>
<tr><td>7</td><td>Properly replace the cover and reconnect the power supply.</td></tr>
</table>

Configuration types

This section explains the different configuration types that are present in the Telindus 1420 SHDSL Router.

Which are the configuration types?

Three types of configuration are present in the Telindus 1420 SHDSL Router:

- the non-active configuration
- the active configuration
- the default configuration.

Explaining the configuration types

When you configure the Telindus 1420 SHDSL Router with TMA, the following happens:

Phase	Action	Result
1	Connect the computer running TMA to the Telindus 1420 SHDSL Router.	The non-active configuration is displayed on the screen.
2	Modify the non-active configuration.	The modifications have no immediate influence on the active configuration currently used by the Telindus 1420 SHDSL Router.
3	Complete the modifications on the non-active configuration.	The non-active configuration has to be activated.
4	Execute the Activate Configuration action.	The non-active configuration becomes the active configuration.

shdslRouter/Activate Configuration

If you execute this action, the editable non-active configuration becomes the active configuration. This action corresponds with the TMA button *Send all attributes to device*: .

When use this action?

Use this action after you made all the necessary configuration settings and you want to activate these settings.

shdslRouter/Load Saved Configuration

If you execute this action, the non-active configuration is overwritten by the active configuration currently used by the Telindus 1420 SHDSL Router.

After executing this action, click on the TMA button *Retrieve all attributes from device* to see the new non-active configuration.

When use this action?

If you are in the progress of modifying the non-active configuration but made some mistakes, then use this action to revert to the active configuration.

shdslRouter/Load Default Configuration

If you execute this action, the non-active configuration is overwritten by the default configuration.

After executing this action, click on the TMA button *Retrieve all attributes from device* to see the new non-active configuration.

When use this action?

If you install the Telindus 1420 SHDSL Router for the first time, all configuration attributes have their default values. If the Telindus 1420 SHDSL Router has already been configured but you want to start from scratch, then use this action to revert to the default configuration.

shdslRouter/Cold Boot

If you execute this action, the Telindus 1420 SHDSL Router reboots. As a result, the Telindus 1420 SHDSL Router …

- performs a self-test.
- checks the firmware.
- reads the saved configuration and restarts program execution.

When use this action?

Use this action, for instance, to activate new firmware.

8.3 LAN interface configuration attributes

shdslRouter/lanInterface/ipAddress

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to assign an IP address to the interface. The address should belong to the subnet the interface is connected to.

shdslRouter/lanInterface/ipNetMask

Default:255.255.255.0
Range: up to 255.255.255.255

Use this attribute to assign an IP subnet mask to the interface. The subnet mask defines the number of IP devices that may be present on the corresponding IP segment.

shdslRouter/lanInterface/secundaryIpAddresses

Default:<empty>
Range: table, see below

Use this attribute to create additional virtual networks on the same Ethernet interface.

The secundaryIpAddresses table contains the following elements:

Element	Description
ipAddress	Use this attribute to assign an IP address to the interface. The address should belong to the subnet the interface is connected to. Default:0.0.0.0 Range: up to 255.255.255.255
ipNetMask	Use this attribute to assign an IP subnet mask to the interface. The subnet mask defines the number of IP devices that may be present on the corresponding IP segment. Default:255.255.255.0 Range: up to 255.255.255.255

shdslRouter/lanInterface/routing

Default:enabled
Range: enabled / disabled

Use this attribute to determine whether IP packets are treated by the bridging process or not.

The routing attribute has the following values:

Value	Description
enabled	IP packets are passed directly to the routing process. IP packets not destined for the router its MAC address are discarded.
disabled	The IP packets are first passed to the bridging process. If necessary, IP packets destined for the router itself are passed on to the routing process. If the routing attribute is set to disabled, it is possible to have an IP subnet that spans multiple interfaces (or the LAN interface and some DLCIs).

shdslRouter/lanInterface/metric

Default:1
Range: 1 … 15

Use this attribute to determine with how much the Telindus 1420 SHDSL Router increments the metric parameter of a route.

Routing information includes a metric parameter. Every time a router is passed, this parameter is incremented. Also the Telindus 1420 SHDSL Router increments the metric parameter (default by 1) before it writes the route in the routing table. Hence, the metric parameter indicates for each route how many routers have to be passed before reaching the network. When several routes to a single network exist and they all have the same preference, then the route with the smallest metric parameter is chosen.

However, using the metric attribute, you can increment the metric parameter by more than 1 (up to a maximum of 15). You could do this, for instance, to indicate that a certain interface is less desirable to route through. As a result, the Telindus 1420 SHDSL Router adds this value to the metric parameter of every route learnt through that interface.

The metric attribute is also used to represent the directly connected subnets on the LAN and WAN interfaces.

shdslRouter/lanInterface/ripMode

Default:active
Range: enumerated, see below

Use this attribute to modify the RIP behaviour of the interface. By default the Telindus 1420 SHDSL Router transmits and receives RIP updates on all interfaces.

The ripMode attribute has the following values:

Value	Description
active	RIP updates are transmitted and received on this interface.
passive	RIP updates are not transmitted on this interface, but received updates are parsed.
disabled	RIP updates are nor transmitted nor received on this interface.

shdslRouter/lanInterface/rip2Authentication

Default:disabled
Range: enumerated, see below

Use this attribute to enable or disable RIP authentication on this interface.

Routers exchange information between each other for management purposes. They do this using the Router Information Protocol (RIP). For security reasons, you can enable an authentication.

The rip2Authentication attribute has the following values:

Value	Description
disabled	No authentication is used.
text	The authentication secret is exchanged in clear text.
md5	Instead of sending the authentication secret together with the RIP updates, it is hashed together with the routing information into a unique value. This authentication is the most secure. This because it provides also protection against tampering with the contents of a packet: both an incorrect password and modified routing information results in different hash values.

Remarks

- If authentication is enabled (either text or md5), then only updates using that authentication are processed. All other updates on that interface are discarded.
- If you use md5 and if for a certain interface multiple secrets are present in the ripv2SecretTable, then the first entry in the ripv2SecretTable is used to transmit RIP updates. Authentication of the received RIP updates is done by looking for the first secret with a matching key.
- If you use text and if for a certain interface multiple secrets are present in the ripv2SecretTable, then only the first entry in the ripv2SecretTable is used to transmit and receive RIP updates.

shdslRouter/lanInterface/accessList

Default:<empty>
Range: table, see below

Use this attribute to control the access from certain hosts or networks.

The access list filters *outgoing* traffic for the Telindus 1420 SHDSL Router, based on the source IP address. You can specify multiple entries within the access list. When more than one entry applies to the same packet, then only the most specific one is taken in consideration. I.e. the entry covering the smallest range. If not one entry matches, then the packet is dropped. If the access list is empty, then all packets are forwarded.

The accessList table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>sourceAddress</td><td>This is the IP source address of the packet. The address may be a (sub)network address.
Default:0.0.0.0
Range: up to 255.255.255.255</td></tr>
<tr><td>mask</td><td>This is the IP subnet mask for the sourceAddress. By combining an IP address with a mask you can uniquely identify a range of addresses. Before comparing IP addresses, a logical AND function is made between both addresses and the mask.
Default:255.255.255.255
Range: up to 255.255.255.255</td></tr>
<tr><td>action</td><td>This defines which action has to be taken when a packet arrives with a source IP address that falls within the specified address range.
Default:deny
Range: enumerated, see below
The possible actions are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>deny</td><td>The packet is dropped.</td></tr>
<tr><td>allow</td><td>The packet is forwarded.</td></tr>
</table></td></tr>
</table>

If you specify one entry or multiple entries for which the action is set to deny, then also specify at least one entry for which the action is set to allow. Else all packets are dropped!

Example 1

This example shows an access list that only forwards traffic from subnet 192.168.48.0 to the LAN interface, except for packets from station 192.168.48.10. All other traffic for the LAN interface is dropped.

accessList

	sourceAddress	mask	action
1	192.168.48.0	255.255.255.0	allow
2	192.168.48.10	255.255.255.255	deny

Example 2

The next example shows an access list to forward all traffic, except the traffic from subnet 192.168.48.0. The second entry is the rule to add if you want all packets that do not match the previous entries to be forwarded.

accessList

	sourceAddress	mask	action
1	192.168.48.0	255.255.255.0	deny
2	0.0.0.0	0.0.0.0	allow

shdslRouter/lanInterface/extendedAccessList

Default:<empty>
Range: table, see below

Use this attribute to control the access from certain hosts or networks.

Similar to a simple access list, an extended access list filters *outgoing* traffic for the Telindus 1420 SHDSL Router. However, it allows more selective filtering of traffic and has priority over the simple access lists on the same interface. The entries in an extended access list indicate the traffic that is allowed. Traffic that is not covered by an entry in the extended access list is filtered out.

The extendedAccessList table contains the following elements:

Element	Description
sourceIpStart-Address	This is the IP source address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
sourceIpEnd-Address	
destinationIpStart-Address	This is the IP destination address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
destinationIpEnd-Address	
ipProtocol	This is the protocol field from the IP header. Default:any Range: 0 … 255 You can specify the protocol by typing the protocol number. For ease of use, some common protocols can be selected from a drop-down box: any (0), ICMP (1), IGMP (2), IPinIP (4), TCP (6), EGP (8), IGP (9), UDP (17), RSVP (46), IGRP (88), OSPFIGP (89), TCPestablished (255). When selecting TCPestablished, the flags in the TCP header are also checked. If a SYN flag is present without an ACK flag, then the packet is filtered out. This condition is met only for the first packet of a TCP connection. It allows to control which side initiates a connection.
sourcePortStart	This is the source port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: any or optional (0), echo (7), discard (9), ftp-data (20), ftp (21), telnet (23), smtp (25), domain (53), www-http (80), pop3 (110), nntp (119), snmp (161), snmptrap (162), z39.50 (210), syslog (514), router (520), socks (1080), l2tp (1701), telindus (1728).
sourcePortEnd	
destinationPortStart	This is the destination port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: see above.
destinationPortEnd	

Start and end values

Except for the IP protocol field, it is possible to specify ranges using the start and end values. There are two special cases:

- A start value is entered, but no end value ⇒ an exact match is needed for the start value.
- Neither a start nor an end value is entered ⇒ the field is not checked.

shdslRouter/lanInterface/bridgePortInfo

Default:-
Range: structure, see below

Use this attribute to set the bridging attributes of the interface.

The bridgePortInfo structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>bridging</td><td>Enables or disables bridging on the interface.

Default:disabled
Range: enabled / disabled</td></tr>
<tr><td>priority</td><td>Each port of a bridge has a unique port identifier. The priority attribute is a part of this port identifier and allows you to change the priority of the port. It is taken as the more significant part in priority comparisons.

Default:128
Range: 0 … 255

The other part of the unique port identifier has a fixed relationship to the physical or logical port. This assures the uniqueness of the unique port identifier among the ports of a single bridge.

For more information on port priority, refer to 5.9.7 - What is Spanning Tree priority and cost? on page 98.</td></tr>
<tr><td>pathCost</td><td>This is the value that is added to the total cost of the path to the root bridge, provided that this particular port is a root port, i.e. that the path to the root goes through this port.

Default:100
Range: 1 … 65535

The total cost of the path to the root bridge should not exceed 65500.

For more information on path cost, refer to 5.9.7 - What is Spanning Tree priority and cost? on page 98.</td></tr>
<tr><td>topologyChange-Detection</td><td>Enables or disables the communication of Spanning Tree topology changes to the root bridge:

Default:enabled
Range: enabled / disabled

<table>
<tr><th>Value</th><th>If a change in topology is detected by or notified to the bridge via this port, …</th></tr>
<tr><td>enabled</td><td>then the bridge communicates this to the root bridge.</td></tr>
<tr><td>disabled</td><td>then the bridge does not communicate this to the root bridge.</td></tr>
</table>
</td></tr>
</table>

shdslRouter/lanInterface/bridgeAccessList

Default:<empty>
Range: table, see below

Use this attribute to control the access from certain hosts or networks.

The bridge access list filters bridged frames based on the source MAC address. The Telindus 1420 SHDSL Router will not forward any packets to the interface that have a source MAC addresses which is specified in the bridge access list.

shdslRouter/lanInterface/arpTimeOut

Default:00000d 02h 00m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to set the ageing time of the ARP (Address Resolution Protocol) cache.

What is the ARP cache?

The LAN interface has been allocated a fixed Ethernet address, also called MAC (Medium Access Control) address. This MAC address is not user configurable. The IP address of the LAN interface, on the other hand, is user configurable (refer to the ipAddress attribute). This means that the user associates an IP address with the predefined MAC address. The MAC address - IP address pairs are kept in a table, called the ARP cache. For an example of such a table, refer to shdslRouter/lanInterface/arpCache on page 217.

How does the ARP cache work?

Before the Telindus 1420 SHDSL Router sends an IP packet on the LAN interface, it has to know the MAC address of the destination device. If the address is not present in the ARP cache table yet, the Telindus 1420 SHDSL Router sends an ARP request on the Ethernet to learn the MAC address and associated IP address of the destination device. This address pair is then written in the ARP cache. Once the address pair is present, the Telindus 1420 SHDSL Router can reference to this pair if it has to send an IP packet to the same device later on.

The ARP cache time-out

Summarised, all the MAC address - IP address pairs from ARP requests and replies received on the LAN interface are kept in the ARP cache. However, if devices on the network are reconfigured then this MAC address - IP address relation may change. Therefore, the ARP cache entries are automatically removed from the cache after a fixed time-out. This time-out period can be set with arpTimeOut attribute.

shdslRouter/lanInterface/directedBroadcasts

Default:enabled
Range: enabled / disabled

Use this attribute to enable (forward) or disable (discard) directed broadcasts.

Directed broadcasts are IP packets destined for a complete (sub-)network. For example, a packet destined for all devices on sub-network 192.168.48.0 with subnet mask 255.255.255.0 will have destination address 192.168.48.255. I.e. all ones in the subnet area of the IP address.

shdslRouter/lanInterface/ipHelpers

Default:<empty>
Range: table, see below

Use this attribute for broadcast forwarding.

Limited IP broadcasts (address 255.255.255.255) and (sub-)network broadcasts for a directly connected network are normally not forwarded by the Telindus 1420 SHDSL Router. However, client / server applications often use these broadcasts during start-up to discover the server on the network. If the server is on a remote LAN, then the detection may fail.

Therefore, if you configure a helper IP address, the received broadcasts address is replaced by this helper IP address and the packets are re-routed using the destination address. Multiple helper IP addresses can be configured.

The Telindus 1420 SHDSL Router only substitutes addresses for the protocols which are selected in the helperProtocols attribute (refer to the configuration attribute shdslRouter/router/helperProtocols on page 178).

shdslRouter/lanInterface/sendIcmpRedirect

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP messages.

If the Telindus 1420 SHDSL Router receives an IP packet on the LAN interface for which …

- the next hop gateway is on the same interface,
- the next hop address is in the same subnet as the source,

… then it sends an ICMP message to the originator of the packet to inform him that a better (shorter) route exists.

shdslRouter/lanInterface/lanWanStatusCoupling

Default:disabled
Range: enabled / disabled

Use this attribute to enable or disable the status coupling between the LAN and the WAN interface. This is only supported for PPP and Frame Relay.

If you enable the lanWanStatusCoupling, then the WAN interface stops transmitting in case the LAN interface goes down and vice versa. This allows you, when using PPP with link monitoring or Frame Relay with LMI, to let a complete link go down in case one element of the link goes down.

shdslRouter/lanInterface/<configurationAlarmAttributes>

For more information on the configuration alarm attributes alarmMask and alarmLevel and on the alarms in general, refer to 11.2 - Introducing the alarm attributes on page 275.

For more information on the alarms of the lanInterface object, refer to 11.4 - LAN interface alarms on page 279.

8.4 WAN interface configuration attributes

Several configuration attributes of the WAN interface are the same as on the LAN interface. Therefore, they are not explained here again. These attributes are: ipAddress, ipNetMask, secondaryIpAddresses, metric, ripMode, rip2Authentication, accessList, extendedAccessList, bridgeAccessList, directedBroadcasts and ipHelpers.

For a complete description of these attributes, refer to 8.3 - LAN interface configuration attributes on page 152.

shdslRouter/wanInterface/autoInstallMode

Default:unnumbered
Range: enumerated, see below

Use this attribute to determine how the WAN interface will obtain its IP address in case you do not configure it yourself.

The autoInstallMode attribute has the following values:

Value	Description
unnumbered	The WAN interface uses the LAN IP address. In this case: • If an IP address is present on the LAN interface, then no auto-install (or any other method of automatically obtaining an IP address) is used. • If no IP address is configured on the LAN interface, then BootP is used on the LAN interface and the auto-install sequence is started on the WAN interface.
numbered	The WAN interface uses the configured IP address. If no IP address has been entered, then the interface is not present.
autoInstall	The WAN interface automatically obtains its IP address. Then it continues with the sequence: • DNS request • TFTP configuration download • activate configuration.
easyIp	The WAN interface automatically obtains its IP address. Easy IP is a new twist to auto-install over PPP. With easy IP, the WAN interface obtains its IP address through IPCP.
easyIpPat	The WAN interface automatically obtains its IP address and uses that address as PAT address. The IP address obtained through easy IP is used as PAT address to provide Internet access to all users on the local network of the router. This means that the LAN interface is fully configured (including an active DHCP server). However, each time the WAN link goes down, the WAN interface address is renegotiated.

shdslRouter/wanInterface/priorityPolicy

Default:<empty>
Range: max. 64 characters

When you want to activate the priority policy feature of the Telindus 1420 SHDSL Router, you first have to add the priority policy object to the containment tree (refer to 5.11.5 - Adding a policy object on page 108). What is more, the instance value you defined for the priorityPolicy object also has to be entered in this priorityPolicy attribute.

shdslRouter/wanInterface/trafficPolicy

Default:<empty>
Range: max. 64 characters

When you want to activate the traffic policy feature of the Telindus 1420 SHDSL Router, you first have to add the traffic policy object to the containment tree (refer to 5.11.5 - Adding a policy object on page 108). What is more, the instance value you defined for the trafficPolicy object also has to be entered in this trafficPolicy attribute.

shdslRouter/wanInterface/splitHorizon

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable split horizon operation.

Split horizon operation prevents that routing information exits the interface through which the information was received in the first place. This optimises communications among multiple routers, particularly when links are broken. It also prevents routing loops.

However, with non-broadcast networks (such as Frame Relay), situations can arise for which split horizon operation is not so ideal. If the WAN interface is connected to a Frame Relay network, it is possible that each Data Link Connection Identifier (DLCI) has its own remote router. In other words, they could be considered as individual sub-interfaces. By default, routing information received via one DLCI is not propagated to the other DLCIs (over the same physical interface). However, setting the splitHorizon attribute to disabled, allows the routing information received via one DLCI to be propagated to the other DLCIs.

shdslRouter/wanInterface/encapsulation

Default:frameRelay
Range: enumerated, see below

Use this attribute to select the encapsulation protocol on the WAN interface.

The encapsulation attribute has the following values:

Value	Description
frameRelay	Selects Frame Relay encapsulation. Frame Relay is a synchronous communication protocol.
ppp	Selects Point-To-Point encapsulation. PPP can be synchronous or asynchronous.
hdlc	Selects High-Level Data Link Control encapsulation.

shdslRouter/wanInterface/<configurationAlarmAttributes>

For more information on the configuration alarm attributes alarmMask and alarmLevel and on the alarms in general, refer to 11.2 - Introducing the alarm attributes on page 275.

For more information on the alarms of the wanInterface object, refer to 11.5 - WAN interface alarms on page 280.

8.5 WAN encapsulation configuration attributes

This section discusses the configuration attributes of the encapsulation protocols that can be used on the WAN interface.

The following gives an overview of this section:

8.5.1 Frame Relay configuration attributes

shdslRouter/wanInterface/frameRelay/dlciTable

Default:<empty>
Range: table, see below

Use this attribute to configure the Frame Relay Data Link Connection Identifiers (DLCIs).

The Telindus 1420 SHDSL Router can connect to multiple remote routers via different DLCIs using a single WAN interface. Through LMI Full Status Enquiry messages, the Telindus 1420 SHDSL Router can learn its active and inactive DLCIs. If the Frame Relay network also supports the Inverse ARP protocol, the Telindus 1420 SHDSL Router can learn the IP address of the corresponding router for each DLCI.

If however neither LMI nor Inverse ARP is supported by the Frame Relay network, then you can define which DLCI number corresponds with which remote router in the dlciTable. This is also called static routing on a WAN.

The dlciTable contains the following elements:

Element	Description
dlci	This is the DLCI number to reach a remote network. Default:16 Range: 16 … 1022 The DLCI number may have any value between 16 and 1022. However, if you set the configuration attribute lmi to q933-Annex-A, you should only use DLCIs up to 1007.
cir	This is the Committed Information Rate for the corresponding DLCI. Default:0 Range: 0 … 2048000 The CIR is expressed in bps. Any value between 0 and 2048000 (bps) can be configured. If the cir value is set to 0 (default), it means the complete bandwidth may be used (no flow control).
eir	This is the Excess Information Rate for the corresponding DLCI. Default:0 Range: 0 … 2048000 The EIR is expressed in bps. Any value between 0 and 2048000 (bps) can be configured. If the eir value is set to 0 (default), it means no excess burst is allowed. If you configure EIR, then CIR must also be configured. Else there is no flow control.
routing	Use this attribute to determine whether IP packets are treated by the bridging process or not. Default:enabled Range: enabled / disabled For more information, refer to the configuration attribute shdslRouter/lanInterface/routing on page 153.

Element	Description	
gateway	This is the corresponding IP address of the remote router.	Default:0.0.0.0 Range: up to 255.255.255.255
local	This address is used in the response on an Inverse ARP request received on the DLCI. The local attribute is optional and only needs to be defined in case secondary IP addresses are used on the Frame Relay WAN interface.	Default:0.0.0.0 Range: up to 255.255.255.255
bridgePortInfo	This sets the bridging attributes of the Frame Relay WAN interface. For more information, refer to the configuration attribute shdslRouter/lanInterface/bridgePortInfo on page 157.	Default:- Range: structure, see below

shdslRouter/wanInterface/frameRelay/lmi

Default:-
Range: structure, see below

Use this attribute to select the Local Management Interface (LMI) protocol and to fine-tune the LMI operation.

The LMI provides a status mechanism which gives an on-going status report on the DLCIs. These status reports are exchanged between the Frame Relay access device (or Frame Relay DTE) and Frame Relay node (or Frame Relay DCE).

At regular intervals, the DTE sends Full Status Enquiry messages to the DCE. The DCE answers with the status of all its DLCIs on the interface. At smaller intervals, the DTE sends Status Enquiry messages. In that case, the DCE only answers with DLCI status changes.

The lmi structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>type</td><td>This is the LMI variant. There are several standards for the LMI protocol with small variations between them. Therefore you should configure the Telindus 1420 SHDSL Router according to the standard that is used by your service provider.
Default:q933-Annex-A
Range: enumerated, see below

The type attribute has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>noLmiConfigured</td><td>No LMI is used.</td></tr>
<tr><td>lmiRev1</td><td>Set this value only for compatibility with older equipment.</td></tr>
<tr><td>ansit1-617-d</td><td>Set this value for ANSI LMI compliance.</td></tr>
<tr><td>q933-Annex-A</td><td>Set this value for ITU-T LMI compliance.</td></tr>
</table></td></tr>
<tr><td>pollingInterval</td><td>This defines the time between successive Status Enquiry messages.
Default:00000d 00h 00m 10s
Range: 00000d 00h 00m 05s - 00000d 00h 00m 30s</td></tr>
<tr><td>errorThreshold</td><td>This defines the maximum number of unanswered Status Enquiry messages that the Telindus 1420 SHDSL Router will accept before declaring the interface down. See also the attribute monitoredEvents.
Default:3
Range: 1 … 10</td></tr>
</table>

Element	Description
monitoredEvents	This defines the number of status polling intervals over which the error threshold is counted. Default:4 Range: 1 … 10 In other words, if the station receives an errorThreshold number of unanswered Status Enquiry messages within a monitoredEvents number of pollingInterval intervals, then the interface is declared down. **Example** If the station receives 3 unanswered Status Enquiry messages within 4 x 10s = 40s, then the interface is declared down.
expectedPollInterval	This defines the maximum time between two consecutive incoming Status Enquiry messages. Select the value 0 in order to disable verification. Default:00000d 00h 00m 15s Range: 00000d 00h 00m 00s - 00000d 00h 00m 30s This attribute is only relevant when using Frame Relay over a point-to-point link (no Frame Relay network): In Frame Relay language, a router is normally considered as a DTE. However, if two routers are connected to each other in Frame Relay but without a real Frame Relay network in between, then the routers also take the role of a DCE. This happens automatically, without the need of a reconfiguration. The Status Enquiry messages are sent in both directions.
fullEnquiryInterval	This defines the number of Status Enquiry intervals that have to go by before sending a Full Status Enquiry message. Default:6 Range: 1 … 255

8.5.2 PPP configuration attributes

shdslRouter/wanInterface/ppp/linkMonitoring

Default:-
Range: structure, see below

Use this attribute to enable or disable link monitoring and to fine-tune it.

The PPP protocol features link monitoring. You can use this to verify whether the WAN link is up or down.

If link monitoring is enabled, then the Telindus 1420 SHDSL Router sends an echo request packet over the line at regular intervals. If on consecutive requests no reply is given, then the PPP link is declared down. Data traffic is stopped until the PPP handshake succeeds again.

The linkMonitoring structure contains the following elements:

Element	Description
operation	Enables or disables link monitoring. Default:disabled Range: enabled / disabled
interval	This defines the time interval between two consecutive echo requests. Default:00000d 00h 00m 10s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
replyTimeOut	This defines the period that the Telindus 1420 SHDSL Router waits for a reply on the echo request. Default:00000d 00h 00m 02s Range: 00000d 00h 00m 00s - 00000d 00h 04m 15s If no reply has been received within this time-out, then the Telindus 1420 SHDSL Router considers this as a failed echo request.
failsPermitted	This defines the number of failed echo requests after which the Telindus 1420 SHDSL Router declares the WAN link down. Default:4 Range: 1 … 30 **Example** Suppose failsPermitted is set to 10. If on 10 consecutive echo requests no reply is given, then the Telindus 1420 SHDSL Router declares the WAN link down and the PPP handshake is started again.

shdslRouter/wanInterface/ppp/authentication

Default:disabled
Range: chap / disabled

Use this attribute to enable or disable CHAP authentication on the PPP link. For more information refer to What is CHAP authentication? on page 65.

The authentication attribute has the following values:

Value	Description
disabled	Authentication is disabled.
chap	This side of the link requests a CHAP authentication from the remote router.

shdslRouter/wanInterface/ppp/authenPeriod

Default:00000d 00h 00m 10s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to define the PPP authentication interval.

Normally on an authenticated PPP link, authentication is not only performed at link set-up but also at regular intervals during the data transfer. You can set this interval using the authenPeriod attribute. If you set the authenPeriod attribute to 00000d 00h 00m 00s, then authentication is only performed at link set-up and not during the data transfer.

shdslRouter/wanInterface/ppp/routing

Default:disabled
Range: enabled / disabled

Use this attribute to determine whether IP packets are treated by the bridging process or not.

For more information, refer to the configuration attribute shdslRouter/lanInterface/routing on page 153.

shdslRouter/wanInterface/ppp/bridgePortInfo

Default:-
Range: structure, see below

Use this attribute to set the bridging attributes of the PPP WAN interface.

For more information, refer to the configuration attribute shdslRouter/lanInterface/bridgePortInfo on page 157.

8.5.3 HDLC configuration attributes

shdslRouter/wanInterface/hdlc/bridgePortInfo

Default:-
Range: structure, see below

Use this attribute to set the bridging attributes of the HDLC WAN interface.

For more information, refer to the configuration attribute shdslRouter/lanInterface/bridgePortInfo on page 157.

8.6 Line configuration attributes

shdslRouter/wanInterface/line/channel

Default:central
Range: enumerated, see below

Use this attribute to determine which unit is the central unit and which the remote unit.

I.e. it determines which unit acts as master and which as slave during the synchronisation procedure. Therefore set one Telindus 1420 SHDSL Router to central and its remote counterpart to remote.

shdslRouter/wanInterface/line/speed

Default:auto
Range: enumerated, see below

Use this attribute to set the line speed.

The speed attribute has the following values:

Value	Description
auto	In auto speed mode the central and remote Telindus 1420 SHDSL Router negotiate the speed they are going to use on the line.
64Kbps … 2304Kbps	Besides auto speed, you can also select a fixed line speed ranging from 64Kbps up to 2304Kbps in steps of 64 kbps.

shdslRouter/wanInterface/line/retrain

Default:-
Range: structure, see below

Use this attribute to determine at what bit error rate (BER) a retrain cycle will be initiated in case the line quality deteriorates.

The retrain structure contains the following elements:

Element	Description
errorPersistence-Time	Period, in seconds, over which the average BER is calculated. If within this period the average BER equals or exceeds the value entered in the errorThreshold attribute, the modem will retrain. Default:30 Range: 1 … 255
errorThreshold	Bit error rate (BER), in percent, which defines when the modem should retrain. Default:100 Range: 10 … 100

shdslRouter/wanInterface/line/<configurationAlarmAttributes>

For more information on the configuration alarm attributes alarmMask and alarmLevel and on the alarms in general, refer to 11.2 - Introducing the alarm attributes on page 275.

For more information on the alarms of the line object, refer to 11.6 - Line alarms on page 281.

8.7 Routing configuration attributes

shdslRouter/router/defaultRoute

Default:-
Range: structure, see below

Use this attribute to set the default route, also called gateway address.

Besides specifying routing entries for specific networks, you can also specify a gateway address. Packets for destinations that do not match one of the routing table entries are sent to this gateway address.

The defaultRoute structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>gateway</td><td>
Default:0.0.0.0
Range: up to 255.255.255.255
This is the IP address of the next router that will route all packets for which no specific (static or dynamic) route is exists in the routing table.
Whether you can omit the gateway element or not, is linked to the following conditions:
<table>
<tr><th>If the interface element is set to …</th><th>then …</th></tr>
<tr><td>lan,</td><td>you can not omit the gateway element.</td></tr>
<tr><td>wan,</td><td>you can omit the gateway element only when using PPP encapsulation.</td></tr>
</table>
</td></tr>
<tr><td>interface</td><td>
Default:<opt>
Range: enumerated, see below
This specifies the interface through which the gateway can be reached.
The interface element has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td><opt></td><td> The interface element value is deduced from the setting of the gateway element (refer to Deducing the interface element value on page 173). Select the <opt> value for routes that use a tunnel. </td></tr>
<tr><td>lan</td><td>The gateway can be reached through the Ethernet interface.</td></tr>
<tr><td>wan</td><td>The gateway can be reached through the serial interface.</td></tr>
<tr><td>discard</td><td>Packets for this destination are discarded.</td></tr>
</table>
</td></tr>
<tr><td>preference</td><td>
Default:10
Range: 1 … 200
This defines the level of importance of the default route with respect to routes learnt via RIP.
RIP routes always have a preference of 60. Routes with a lower preference value are chosen over routes with higher preference value.
</td></tr>
</table>

Element	Description
metric	This determines with how much the metric parameter of a route is incremented. Default:1 Range: 1 … 15 If two routes exist with the same preference, then the route with the lowest metric value is chosen. This element is only important when combining static routes and RIP routes. For more information on the metric element, refer to the configuration attribute shdslRouter/lanInterface/metric on page 153.

Deducing the interface element value

If you do not specify a value for the interface element, then this value is deduced from the setting of the gateway element. Depending on the presence of an IP address on the WAN interface, the deduction is done as follows:

<table>
<tr><th>WAN IP address</th><th>Deduction</th></tr>
<tr><td>not present</td><td>In this case, the interface element value is deduced as follows:
<table>
<tr><th>If the gateway address …</th><th>then the interface element is set to …</th></tr>
<tr><td>belongs to the Ethernet interface subnet,</td><td>lan</td></tr>
<tr><td>does not belong to the Ethernet interface subnet,</td><td>wan</td></tr>
</table></td></tr>
<tr><td>present</td><td>In this case, the interface element value is deduced as follows:
<table>
<tr><th>If the gateway address …</th><th>then …</th></tr>
<tr><td>belongs to the Ethernet interface subnet,</td><td>the interface element is set to lan.</td></tr>
<tr><td>belongs to the serial interface subnet,</td><td>the interface element is set to wan.</td></tr>
<tr><td>neither belongs to the Ethernet interface subnet nor to the serial interface subnet,</td><td>the route is discarded (i.e. not used).</td></tr>
</table></td></tr>
</table>

shdslRouter/router/routingTable

Default:<empty>
Range: table, see below

Use this attribute to configure the static IP routes.

The routingTable table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>network</td><td>This is the IP address of the destination network.
Default:0.0.0.0
Range: up to 255.255.255.255</td></tr>
<tr><td>mask</td><td>This is the network mask of the destination network.
Default:255.255.255.0
Range: up to 255.255.255.255</td></tr>
<tr><td>gateway</td><td>This is the IP address of the next router on the path to the destination network.
Default:0.0.0.0
Range: up to 255.255.255.255
Whether you can omit the gateway element or not, is linked to the following conditions:
<table>
<tr><th>If the interface element is set to …</th><th>then …</th></tr>
<tr><td>lan,</td><td>you can not omit the gateway element.</td></tr>
<tr><td>wan,</td><td>you can omit the gateway element only when using PPP encapsulation.</td></tr>
</table></td></tr>
<tr><td>interface</td><td>This specifies the interface through which the destination network can be reached.
Default:<opt>
Range: enumerated, see below
The interface element has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td><opt></td><td>The interface element value is deduced from the setting of the gateway element (refer to Deducing the interface element value on page 173).
Select the <opt> value for routes that use a tunnel.</td></tr>
<tr><td>lan</td><td>The gateway can be reached through the Ethernet interface.</td></tr>
<tr><td>wan</td><td>The gateway can be reached through the serial interface.</td></tr>
<tr><td>discard</td><td>Packets for this destination are discarded.</td></tr>
</table></td></tr>
<tr><td>preference</td><td>This defines the level of importance of the route with respect to routes learnt via RIP.
Default:10
Range: 1 … 200
RIP routes always have a preference of 60. Routes with a lower preference value are chosen over routes with higher preference value.</td></tr>
</table>

Element	Description
metric	This determines with how much the metric parameter of a route is incremented. Default:1 Range: 1 … 15 If two routes exist with the same preference, then the route with the lowest metric value is chosen. This element is only important when combining static routes and RIP routes. For more information on the metric element, refer to the configuration attribute shdslRouter/lanInterface/metric on page 153.

shdslRouter/router/routingProtocol

Default:none
Range: enumerated, see below

Use this attribute to activate or deactivate the Routing Information Protocol (RIP).

The routingProtocol attribute has the following values:

Value	Description
none	No routing protocol is used. Only static routes are used.
Rip2	The RIP version 2 routing protocol is used.

shdslRouter/router/alternativeRoutes

Default:backup
Range: enumerated, see below

Use this attribute to determine how the Telindus 1420 SHDSL Router deals with identical routes.

If more than one route to a (sub-)network is defined in the routing table, and these routes have …

- identical destination addresses, masks, preferences and metrics,
- different gateway,

… then you can use the alternativeRoutes attribute to determine which route the Telindus 1420 SHDSL Router uses to reach the (sub-)network.

The alternativeRoutes attribute has the following values:

Value	Description
backup	The Telindus 1420 SHDSL Router always uses the same route to reach the (sub-)network. Only when this route goes down, it uses the alternative route.
roundRobin	The Telindus 1420 SHDSL Router alternately uses the two possible routes to reach the (sub-)network. However, once a certain route is used to reach a specific address, this same route is always used to reach this specific address.

shdslRouter/router/ripUpdateInterval

Default:00000d 00h 00m 30s
Range: 00000d 00h 00m 05s - 00000d 00h 10m 00s

Use this attribute to set the interval the Telindus 1420 SHDSL Router transmits RIP update messages.

Normally, RIP update messages are transmitted every 30 seconds. It is possible to change this interval. However, changing this interval will also change the lifetime of routes learnt through RIP. If a RIP route is received for the last time, it is declared down after 6 times the ripUpdateInterval. After the route is down, it is deleted after 4 times the ripUpdateInterval.

shdslRouter/router/ripv2SecretTable

Default:<empty>
Range: table, see below

Use this attribute to authenticate the routing updates.

The ripv2SecretTable holds the secrets used for the RIP authentication. Authentication can be enabled or disabled on each interface (refer to the configuration attribute shdslRouter/lanInterface/rip2Authentication on page 154).

The ripv2SecretTable table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>keyId</td><td>This is a unique identifier for each secret.
Default:0
Range: 0 … 255</td></tr>
<tr><td>secret</td><td>This is a string of maximum 16 characters. It is sent with the RIP updates on the specified interface. It is also used to authenticate incoming RIP updates.
Default:<empty>
Range: max. 16 characters</td></tr>
<tr><td>interface</td><td>This specifies the interface on which the secret is used.
The interface element has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>all</td><td>The secret is used on all interfaces.</td></tr>
<tr><td>lan</td><td>The secret is used on the Ethernet interface only.</td></tr>
<tr><td>wan</td><td>The secret is used on the serial interface only.</td></tr>
</table></td></tr>
</table>

Remarks

- If authentication is enabled (either text or md5), then only updates using that authentication are processed. All other updates on that interface are discarded.
- If you use md5 and if for a certain interface multiple secrets are present in the ripv2SecretTable, then the first entry in the ripv2SecretTable is used to transmit RIP updates. Authentication of the received RIP updates is done by looking for the first secret with a matching key.
- If you use text and if for a certain interface multiple secrets are present in the ripv2SecretTable, then only the first entry in the ripv2SecretTable is used to transmit and receive RIP updates.

shdslRouter/router/sysSecret

Default:<empty>
Range: max. 64 characters

Use this attribute for the CHAP authentication process. The CHAP authenticator uses the sysSecret attribute in order to verify the peer its response. For more information, refer to the configuration attribute shdslRouter/wanInterface/ppp/authentication on page 169.

shdslRouter/router/pppSecretTable

Default:<empty>
Range: table, see below

Use this attribute for the CHAP authentication process. Enter the CHAP name and secret of the remote router in this table. For more information, refer to the configuration attribute shdslRouter/wanInterface/ppp/authentication on page 169.

The ripv2SecretTable table contains the following elements:

Element	Description
name	Enter here the CHAP name of the remote router. Default:<empty> Range: max. 64 characters If the remote router is a Telindus 1420 SHDSL Router, then the name element should correspond with the remote Telindus 1420 SHDSL Router its sysName attribute.
secret	Enter here the CHAP secret of the remote router. Default:<empty> Range: max. 64 characters If the remote router is a Telindus 1420 SHDSL Router, then the secret element should correspond with the remote Telindus 1420 SHDSL Router its sysSecret attribute.

shdslRouter/router/helperProtocols

Default:<empty>
Range: table, see below

Use this attribute to define the TCP and UDP port numbers for which broadcast forwarding is required. Use this attribute if you have specified IP addresses for one of the interfaces in the ipHelpers attribute (refer to the configuration attribute shdslRouter/lanInterface/ipHelpers on page 159).

If the helperProtocols table is empty (default), then address substitution is applied for the following protocols:

Protocol name	TCP/UDP port number
Time Server	37
IEN-116 Host Name Server	42
Domain Name Server	53
TACACS database service	65
Boot Protocol (BootP) / DHCP server	68
NetBIOS Name Server	137
NetBIOS Datagram Server	138

Specifying at least one value in the helperProtocols table clears the default helper list automatically. In that case, if you want that for instance NetBios Datagram Server broadcast is forwarded, you have to specify port number 138 again.

For BootP / DHCP broadcast packets, the Telindus 1420 SHDSL Router is also a BootP / DHCP Relay Agent. If the protocol is selected, then the Telindus 1420 SHDSL Router will write the IP address of its Ethernet interface in the BootP or DHCP gateway field and increment the hops field in addition to the address substitution.

shdslRouter/router/sendTtlExceeded

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP “TTL exceeded“ messages.

What is Time To Live (TTL)?

Each IP packet has a Time To Live (TTL) value in its header. Each device that sends an IP packet sets this parameter at some fixed or predefined value. When the packet enters a router, the router decrements the TTL value. If a router finds a value 0 after decrementing the TTL, it discards the packet. This because a value 0 means the packet has passed too many routers. Probably the packet is looping between a number of routers. This mechanism avoids that routers with configuration errors bring down a complete network.

The ICMP message “TTL exceeded”

If a router discards a packet because its TTL is exceeded, it normally sends an ICMP “TTL exceeded“ message to the originator of the packet. With the sendTtlExceeded attribute you can define whether you want the Telindus 1420 SHDSL Router to send such ICMP messages or not.

The sendTtlExceeded attribute has the following values:

Value	Description
enabled	The Telindus 1420 SHDSL Router sends "ICMP destination unreachable, reason: TTL exceeded" messages.
disabled	The Telindus 1420 SHDSL Router does not send ICMP “TTL exceeded” messages. This also implies that the router is not recognised by the UNIX or Windows traceroute feature.

shdslRouter/router/sendPortUnreachable

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP “port unreachable“ messages.

The ICMP message “port unreachable”

The Telindus 1420 SHDSL Router supports a number of higher-layer IP protocols (Telnet, SNMP and TMA) for management purposes. If an IP packet is sent to the Telindus 1420 SHDSL Router for a higher-layer protocol that it does not support, it normally sends an ICMP “port unreachable“ message to the originator of the packet. With the sendPortUnreachable attribute you can define whether you want the Telindus 1420 SHDSL Router to send such ICMP messages or not.

The sendPortUnreachable attribute has the following values:

Value	Description
enabled	The Telindus 1420 SHDSL Router sends "ICMP destination unreachable, reason: port unreachable" messages.
disabled	The Telindus 1420 SHDSL Router does not send ICMP “port unreachable” messages. This also implies that the router is not recognised by the UNIX or Windows traceroute feature.

shdslRouter/router/sendAdminUnreachable

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP “communication prohibited“ messages.

The ICMP message “communication prohibited”

If the Telindus 1420 SHDSL Router receives an IP packet that is destined for a prohibited destination (because this destination is defined in the access list or extended access list), then it sends an ICMP “communication prohibited“ message to the originator of the packet. With this attribute you can define whether you want the Telindus 1420 SHDSL Router to send ICMP packets or not:

The sendPortUnreachable attribute has the following values:

Value	Description
enabled	The Telindus 1420 SHDSL Router sends "Communication administratively prohibited by filtering, message: Destination host unreachable" messages.
disabled	The Telindus 1420 SHDSL Router does not send ICMP messages.

shdslRouter/router/patAddress

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to define the Port Address Translation address.

The PAT address is always an official IP address. Entering an address different from the default value 0.0.0.0 automatically enables PAT.

For more information on PAT, refer to 5.8 - Configuring NAT and PAT on page 77.

shdslRouter/router/portTranslations

Default:<empty>
Range: table, see below

Use this attribute to define specific port number ranges that should not be translated.

Some TCP or UDP applications do not allow port translations: these applications require a dedicated source port number. In the portTranslations table you can define UDP and TCP port ranges that should not be translated. If a packet with a source port number in such a range is received, PAT replaces only the source IP address provided it is the first device using this port number. When other devices using the same application (hence the same port number) try to send traffic to the same Internet destination address, PAT discards this traffic.

It is also possible to define port ranges that PAT should always discard. The port translation range PAT uses goes from 60928 up to 65535.

The portTranslations table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>protocol</td><td>This selects the protocol: tcp or udp.
Default:tcp
Range: tcp / udp</td></tr>
<tr><td>startPort</td><td>This defines the lowest value of the TCP or UDP port range.
Default:0
Range: 0 … 65535</td></tr>
<tr><td>endPort</td><td>This defines the highest value of the TCP or UDP port range.
Default:<Opt>
Range: 0 … 65535
If no endPort value is defined (<Opt>), then the port range is limited to the startPort value only.</td></tr>
<tr><td>action</td><td>If a packet is received with a source port number in the previously specified range, a certain action can be taken.
Default:noTranslation
Range: enumerated, see below
The action element has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>noTranslation</td><td>The port numbers that fall within the defined port range are not translated.</td></tr>
<tr><td>deny</td><td>Packets with port numbers in that fall within the defined port range are discarded.</td></tr>
</table></td></tr>
</table>

shdslRouter/router/servicesAvailable

Default:<empty>
Range: table, see below

Use this attribute to define specific port number ranges for incoming Internet traffic that should not be translated. Instead it is sent to the corresponding private IP address.

The servicesAvailable table makes it possible to have a server on the local network that can be accessed from the Internet, although it has no official IP address.

The servicesAvailable table contains the following elements:

Element	Description
protocol	This selects the protocol: tcp or udp. Default:tcp Range: tcp / udp
startPort	This defines the lowest value of the TCP or UDP port range. Default:0 Range: 0 … 65535
endPort	This defines the highest value of the TCP or UDP port range. Default:<Opt> Range: 0 … 65535 If no endPort value is defined (<Opt>), then the port range is limited to the startPort value only.
serverAddress	This sets the private server address. Default:0.0.0.0 Range: up to 255.255.255.255 If a packet is received with a source port number in the previously specified range, it is sent to the private server address.

shdslRouter/router/natAddresses

Default:<empty>
Range: table, see below

Use this attribute to define all the official IP addresses. Entering an address in the table automatically enables NAT.

The natAddresses table contains the following elements:

Element	Description
officialAddress	This is the official IP address. These addresses are used in the reverse order as they appear in the list.
privateAddress	This is the private IP address. Use this element to permanently assign an official IP address to a private address.

For more information on NAT, refer to 5.8 - Configuring NAT and PAT on page 77.

shdslRouter/router/natGateways

Default:<empty>
Range: table, see below

Use this attribute to define the gateway addresses from routes on which NAT or PAT should be applied.

shdslRouter/router/natTcpSocketTimeOut

Default:00001d 00h 00m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to define the time-out for TCP sessions that are not closed by the application.

Such sessions, whether PAT or NAT is in use, remain active for one day by default. Only decrease this attribute if some TCP applications do not close properly, filling up the available translation sessions.

shdslRouter/router/natUdpSocketTimeOut

Default:00000d 00h 03m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to define the time-out for UDP sessions that are not closed by the application.

Such sessions, whether PAT or NAT is in use, remain active for 3 minutes by default. Only decrease this attribute if some UDP applications do not close properly, filling up the available translation sessions.

shdslRouter/router/natTcpSockets

Default:1024
Range: 500 … 4500

Use this attribute to set the maximum number of TCP session that may be used simultaneously for address translation.

shdslRouter/router/natUdpSockets

Default:1024
Range: 500 … 4500

Use this attribute to set the maximum number of UDP session that may be used simultaneously for address translation.

shdslRouter/router/dhcpStatic

Default:<empty>
Range: table, see below

Use this attribute to assign a fixed IP address to a client its MAC address and this for an infinite time.

The Telindus 1420 SHDSL Router supports the DHCP server protocol. This attribute and the following two attributes describe the configuration parameters to customise the DHCP server behaviour.

The dhcpStatic table contains the following elements:

Element	Description
ipAddress	This assigns an IP address to a certain client. This client is identified with its MAC address. Default:0.0.0.0 Range: up to 255.255.255.255 If no IP address is specified, then there is no connection to the client. Therefore, all other attributes in the table are ignored for this client.
mask	This is the client its subnet mask. Default:255.255.255.0 Range: up to 255.255.255.255
gateway	This is the default gateway for the client its subnet. Default:0.0.0.0 Range: up to 255.255.255.255 If no gateway is specified, then the gateway of the LAN channel is used.
nameServer	This is the IP address of the name server that is available to the client. Default:0.0.0.0 Range: up to 255.255.255.255
tftpServer	This is the IP address of the TFTP server that is available to the client. It is the next server to use in boottrap. Default:0.0.0.0 Range: up to 255.255.255.255
MAC address	This is the client its MAC address. Default:0.0.0.0.0.0 Range: up to ff.ff.ff.ff.ff.ff If no MAC address is specified, then there is no connection to the client. Therefore, all other attributes in the table are ignored for this client.
bootFile	This is the location of the boot file. Default:<empty> Range: max. 128 characters
hostName	This is the name of the client. Default:<empty> Range: max. 20 characters
domainName	This is the name the client should use when resolving hostnames via the Domain Name System (DNS). Default:<empty> Range: max. 20 characters
netbiosNameServer	This is the IP address of the NetBios server. Default:0.0.0.0 Range: up to 255.255.255.255
netbiosNodeType	Use this element to configure the client as described in RFC 1001 / 1002. Default:<Opt> Range: enumerated, see below The netbiosNodeType element has the following values: no-node, B-node, P-node, M-node, H-node.

shdslRouter/router/dhcpDynamic

Default:<empty>
Range: table, see below

Use this attribute to specify the IP address range from which an IP address may be dynamically assigned to a client its MAC address.

The dhcpDynamic table contains the following elements:

Element	Description
ipStartAddress	This defines the start address of the IP address range. It is from this range that an IP address will be dynamically assigned to a client. Default:0.0.0.0 Range: up to 255.255.255.255 If no IP start address is specified, all other attributes on the same line in the table are ignored.
ipEndAddress	This defines the end address of the IP address range. It is from this range that an IP address will be dynamically assigned to a client. Default:0.0.0.0 Range: up to 255.255.255.255 The IP address range will only contain the ipStartAddress in case … • no ipEndAddress is specified, • the specified ipEndAddress is the same as the ipStartAddress, • the specified ipEndAddress is smaller than the ipStartAddress, • the specified ipEndAddress belongs to another subnet than the ipStartAddress. Do not include the Telindus 1420 SHDSL Router its own IP address in this range!
mask	This defines the client its subnet mask for the specified IP address range. Default:255.255.255.0 Range: up to 255.255.255.255
gateway	This is the default gateway for the client its subnet. If no gateway is specified, then the gateway of the LAN channel is used. Default:0.0.0.0 Range: up to 255.255.255.255
nameServer	This is the IP address of the name server that is available to the client. Default:0.0.0.0 Range: up to 255.255.255.255
tftpServer	This is the IP address of the TFTP server that is available to the client. It is the next server to use in bootstrap. Default:0.0.0.0 Range: up to 255.255.255.255
leaseTime	This is the maximum time a client can lease an IP address from the specified IP address range. If 00000d 00h 00m 00s (default) is specified, then the lease time is infinite. Default:00000d 00h 00m 00s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
holdTime	This is the time between two consecutive leases of an IP address. I.e. if a client has just let go of its dynamically assigned IP address, then this same IP address can not be reassigned before the holdTime has elapsed. Default:00000d 00h 00m 00s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Element	Description
bootFile	This is the location of the boot file. Default:<empty> Range: max. 128 characters
hostName	This is the name of the client. Default:<empty> Range: max. 20 characters Because the DHCP server can not give the same name to all clients of this IP address range, a number is added to the host name from the second IP address onwards. The number goes up to 99. **Example** Suppose the host name is Telindus. In that case the name for the start IP address is Telindus, for the second IP address Telindus1, and so on.
domainName	This is the name the client should use when resolving hostnames via the Domain Name System (DNS). Default:<empty> Range: max. 20 characters
netbiosNameServer	This is the IP address of the NetBios server. Default:0.0.0.0 Range: up to 255.255.255.255
netbiosNodeType	Use this element to configure the client as described in RFC 1001 / 1002. Default:<Opt> Range: enumerated, see below The netbiosNodeType element has the following values: no-node, B-node, P-node, M-node, H-node.

DHCP server reaction on a BootP request

The DHCP server reacts on a BootP request as follows: the source MAC address of the incoming BootP request packet is compared with the MAC addresses that have been entered in the dhcpStatic table. Then, there are two possibilities:

- If the source MAC address corresponds with a MAC address in the dhcpStatic table, then the DHCP server replies with a BootP reply packet. In this reply, the IP address that is linked with the MAC address in question (as defined in the dhcpStatic table) is returned.
- If the source MAC address does not correspond with a MAC address in the dhcpStatic table, then the DHCP server returns no response on that frame.

Releasing IP addresses - DHCP versus BootP

On DHCP level, it is regularly checked whether the device that has an IP address in lease is still connected to the network. If it is not, the IP address is returned to the pool of free IP addresses.

On BootP level, however, such a check (or *refresh*) does not exist. What is more, a statistic IP address lease is for an infinite time. Consequently, if the device that requested the IP address is no longer connected to the network, this is not detected by the server. In that case, the statistical information will still indicate that the IP address is leased although it is not.

shdslRouter/router/dhcpCheckAddress

Default:disabled
Range: enabled / disabled

Use this attribute to allow that the assigned IP address is probed with an ICMP Echo Request. This checks and prevents the double use of IP addresses.

The dhcpCheckAddress attribute has the following values:

Value	Description
enabled	No ICMP Echo Request is sent when an IP address is leased by a client.
disabled	An ICMP Echo Request is sent when an IP address is leased by a client. If an ICMP Echo Reply is received, it means the IP address is already in use. Therefore, another IP address is assigned.

shdslRouter/router/<configurationAlarmAttributes>

For more information on the configuration alarm attributes alarmMask and alarmLevel and on the alarms in general, refer to 11.2 - Introducing the alarm attributes on page 275.

For more information on the alarms of the router object, refer to 11.7 - Routing alarms on page 282.

8.8 L2TP tunnel configuration attributes

shdslRouter/router/tunnels/l2tpTunnels

Default:<empty>
Range: table, see below

Use this attribute to configure the Layer 2 Tunnelling Protocol tunnels you want to set up.

The l2tpTunnels table contains the following elements:

Element	Description
name	This is the name of the tunnel. Default:<empty> Range: max. 64 characters The tunnel name is used in status and performance information to distinguish the different tunnels from one another.
adminStatus	This activates (up) or deactivates the tunnel (down). Default:down Range: up / down
ip	Use this structure to assign IP addresses to the tunnel. For more information, refer to shdslRouter/router/tunnels/l2tpTunnels/ip on page 189.
bridging	Use this structure to configure the bridging feature in the tunnel. For more information, refer to the configuration attribute shdslRouter/lanInterface/bridgePortInfo on page 157. When bridging is enabled on a tunnel interface, the tunnel acts exactly as a bridge port for a physical PPP connection.
l2tp	Use this structure to configure the L2TP properties of the tunnel. For more information, refer to shdslRouter/router/tunnels/l2tpTunnels/l2tp on page 190.

shdslRouter/router/tunnels/l2tpTunnels/ip

Default:-
Range: structure, see below

Use the ip structure in the l2tpTunnels table to configure the IP addresses of the tunnel.

The ip structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>ipAddress</td><td>This is the IP address of the local side of the PPP connection inside the tunnel.
Default:<Opt>
Range: up to 255.255.255.255</td></tr>
<tr><td>ipNetMask</td><td>This is the IP subnet mask of the PPP connection inside the tunnel.
Default:<Opt>
Range: up to 255.255.255.255</td></tr>
<tr><td>ipGateway</td><td>This is the IP address of the remote side of the PPP connection inside the tunnel.
Default:<Opt>
Range: up to 255.255.255.255</td></tr>
<tr><td>rip</td><td>Use this structure to configure the RIP behaviour in the tunnel.
Default:-
Range: structure, see below
The rip structure contains the following elements:
<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>metric</td><td>This determines with how much the metric parameter of a route is incremented.
Default:1
Range: 1 … 15
For more information on the metric element, refer to the configuration attribute shdslRouter/lanInterface/metric on page 153.</td></tr>
<tr><td>mode</td><td>This modifies the RIP behaviour of the interface.
Default:disabled
Range: enumerated, see below
By default RIP updates are nor transmitted nor received on this interface. For more information on the mode element, refer to the configuration attribute shdslRouter/lanInterface/ripMode on page 154.</td></tr>
</table></td></tr>
<tr><td>routing</td><td>This determines whether IP packets are treated by the bridging process or not.
Default:enabled
Range: enabled / disabled
For more information, refer to the configuration attribute shdslRouter/lanInterface/routing on page 153.</td></tr>
</table>

shdslRouter/router/tunnels/l2tpTunnels/l2tp

Default:-
Range: structure, see below

Use the l2tp structure in the l2tpTunnels table to configure the L2TP properties of the tunnel.

The l2tp structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>localIpAddress</td><td>This is an official IP address which serves as starting point of the L2TP connection.
Default:<Opt>
Range: up to 255.255.255.255</td></tr>
<tr><td>remoteIpAddress</td><td>This is an official IP address which serves as end point of the L2TP connection.
Default:<Opt>
Range: up to 255.255.255.255
Both localIpAddress and remoteIpAddress together with the well-known port number for L2TP (i.e. 1701), make up the socket used for the L2TP session. At the moment, only one L2TP session can exist between one localIpAddress and remoteIpAddress combination.</td></tr>
<tr><td>pppAuthentication</td><td>This enables or disables CHAP authentication on the PPP connection in the tunnel.
Default:disabled
Range: enabled / disabled
For more information, refer to the configuration attribute shdslRouter/wanInterface/ppp/authentication on page 169.</td></tr>
<tr><td>type</td><td>This specifies the type of the tunnel.
Default:outgoingDial
Range: enumerated, see below
The type element has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>outgoingDial</td><td>The outgoing tunnel is not continuously open. It is opened whenever data has to be sent through the tunnel, and closed when no data is detected for a certain time.</td></tr>
<tr><td>outgoingLeasedLine</td><td>The outgoing tunnel is opened as soon as the Telindus 1420 SHDSL Router is up, and it stays open.</td></tr>
<tr><td>incoming</td><td>The tunnel is an incoming tunnel.</td></tr>
</table></td></tr>
<tr><td>dataChannelSequenceNumbering</td><td>This enables (on) or disables (off) sequence numbering on the data messages. These sequence numbers are used to detect lost packets and/or restore the original sequence of packets that may have been reordered during transport.
Default:off
Range: on / off
On control messages, sequence numbering is always enabled.
It is recommended that for connections where reordering or packet loss may occur, dataChannelSequenceNumbering is enabled.</td></tr>
<tr><td>keepAliveTimeOut</td><td>This is the amount of time (in seconds) the tunnel waits before it sends a keep alive message in case it receives no data.
Default:30
Range: 1 … 3600
If the tunnel does not receive incoming data during a certain time, it sends a keep alive message to the other side and waits for an acknowledgement.</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>l2tpType</td><td>This defines the L2TP function of the Telindus 1420 SHDSL Router.
The l2tpType element has the following values:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>lac</td><td>The Telindus 1420 SHDSL Router acts as an L2TP Access Concentrator.</td></tr>
<tr><td>lns</td><td>The Telindus 1420 SHDSL Router acts as an L2TP Network Server</td></tr>
<tr><td>auto</td><td>If both local and remote Telindus 1420 SHDSL Router are set to auto, they mutually determine who will be the LAC and who the LNS.</td></tr>
</table>
Select auto only if you use a Telindus router at both sides of the tunnel. In conjunction with routers from other vendors (e.g. Cisco), specifically select an L2TP mode (lac or lns).</td></tr>
<tr><td>tunnelAuthentication</td><td>This enables (on) or disables (off) tunnel authentication.
Default:off
Range: on / off
L2TP incorporates a simple, optional, CHAP-like tunnel authentication system during control connection establishment.
If the LAC or LNS wishes to authenticate the identity of the peer it is contacting or being contacted by, it sends a challenge packet. If the expected response and response received from a peer does not match, the tunnel is not opened.
To participate in tunnel authentication, a single shared secret has to exist between the LAC and LNS.</td></tr>
<tr><td>tunnelSecret</td><td>This is used in the tunnel authentication in order to verify the peer its response.
Default:<empty>
Range: max. 64 characters</td></tr>
<tr><td>maxNrOfRetransmissions</td><td>This sets the number of times a control message has to be retransmitted in case no acknowledgement follows, before the tunnel is closed.
Default:4
Range: 0 … 10</td></tr>
<tr><td>transmitWindowSize</td><td>This defines the window size for transmitting control messages.
Default:4
Range: 1 … 30</td></tr>
<tr><td>receiveWindowSize</td><td>This defines the window size for receiving control messages.
Default:4
Range: 1 … 30</td></tr>
<tr><td>udpChecksum</td><td>L2TP is encapsulated in IP/UDP. This enables (on) or disables (off) the UDP checksum.
Default:off
Range: on / off
It is recommended to enable the UDP checksum on lower quality links.</td></tr>
</table>

8.9 Priority policy configuration attributes

The priorityPolicy object is not present in the containment tree by default. If you want to use priority policy, then you have to add this object first. Refer to 5.11.5 - Adding a policy object on page 108.

shdslRouter/router/priorityPolicy[ ]/algorithm

Default:fifo
Range: enumerated, see below

Use this attribute to determine which mechanism is used to queue the data when the Telindus 1420 SHDSL Router experiences an overload condition.

The algorithm attribute has the following values:

Value	Description
fifo	This is a First In First Out queue. The data that enters the queue first, also leaves the queue first. This is the fastest but most superficial queuing mechanism.
roundRobin	This is a priority queuing mechanism. In this case, all queues containing data have an equal weight, disregarding the setting of the weight element in the shdslRouter/router/priorityPolicy[ ]/queueConfigurations attribute.
absolutePriority	This is a priority queuing mechanism. In this case, queues with a high priority have *absolute* priority over queues with a low priority. In other words, no lower priority queue is emptied as long as a higher priority queue contains data. The priority of the queues runs parallel to the queue number. I.e. the user configurable queue number 1 has the lowest priority, whereas the system queue (number 7) has the highest priority. For the queue numbers refer to 5.11.2 - What is a priority queue? on page 107. Note that there is a risk of *starvation*. This means that it is possible that the lower weight queues are never emptied because a higher weight queue continuously receives data.
weightedFair-Queueing	This is a priority queuing mechanism. In this case, the queues are emptied based on their weight. The weight can be configured in the shdslRouter/router/priorityPolicy[ ]/queueConfigurations attribute. **Example** Suppose queue 1 has weight 2, queue 2 has weight 1 and both queues contain data. In that case the queues are emptied in the following order: queue 1 → queue 1 → queue 2 → queue 1 → queue 1 → queue 2 → etc.

Priority queuing

The options roundRobin, absolutePriority and weightedFairQueueing are priority queuing mechanisms. In order to determine which data goes into which priority queue, use the shdslRouter/router/trafficPolicy[ ]/method attribute. The queues themselves can be configured using the shdslRouter/router/priorityPolicy[ ]/queueConfigurations attribute.

shdslRouter/router/priorityPolicy[ ]/countingPolicy

Default:bytes
Range: enumerated, see below

Use this attribute to define whether the quotum of the queues is expressed in bytes or packets.

shdslRouter/router/priorityPolicy[ ]/queueConfigurations

Default:<empty>
Range: table, see below

Use this attribute to set the relative importance of the user configurable queues.

The queueConfigurations table contains the following elements:

Element	Description
quotum	This sets the number of bytes/packets that is dequeued from the user configurable queue when the queue is addressed. Default:1500 Range: 1 … 25000 The unit of the quotum (bytes or packets) can be set with the shdslRouter/router/priorityPolicy[ ]/countingPolicy attribute.
weight	This sets the relative importance of the queue. Default:1 Range: 1 … 10 The weight element is only relevant in case the shdslRouter/router/priorityPolicy[ ]/algorithm attribute is set to absolutePriority or weightedFairQueueing.

shdslRouter/router/priorityPolicy[ ]/lowdelayQuotum

Default:50
Range: 1 … 25000

This sets the number of bytes/packets that is dequeued from the low delay queue when the queue is addressed. For more information on the low delay queue, refer to 5.11.2 - What is a priority queue? on page 107.

The unit of the quotum (bytes or packets) can be set with the shdslRouter/router/priorityPolicy[ ]/countingPolicy attribute.

8.10 Traffic policy configuration attributes

The trafficPolicy object is not present in the containment tree by default. If you want to use traffic policy, then you have to add this object first. Refer to 5.11.5 - Adding a policy object on page 108.

shdslRouter/router/trafficPolicy[ ]/method

Default:trafficShaping
Range: enumerated, see below

Use this attribute to choose a method for redirecting the data to a specific queue.

The method attribute has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>trafficShaping</td><td>The data is redirected to the queues based on the settings of the attribute shdslRouter/router/trafficPolicy[ ]/trafficShaping.</td></tr>
<tr><td>tosDiffServ</td><td>The data is redirected to the queues based on DiffServ (refer to RFC2597) regarding class and drop precedence.

This means that, depending on their Type Of Service (TOS) field, some packets are moved to other queues and/or dropped sooner than other packets in case the queue is full.

The highest 3 bits of the TOS field are mapped as follows:
<table>
<tr><th>Bit values …</th><th>are mapped to …</th></tr>
<tr><td>000 up to 100</td><td>queues 1 up to 5, respectively.</td></tr>
<tr><td>101 and higher</td><td>the low delay queue.</td></tr>
</table>
The next 2 bits define the drop precedence:
<table>
<tr><th>Bit values …</th><th>correspond with …</th></tr>
<tr><td>00 and 01</td><td>maxLength1.</td></tr>
<tr><td>10</td><td>maxLength2.</td></tr>
<tr><td>11</td><td>maxLength3.</td></tr>
</table>
For more information on drop precedence, refer to the attribute shdslRouter/router/trafficPolicy[ ]/dropPrecedence.</td></tr>
<tr><td>tosMapped</td><td>The data is redirected to the queues based on the settings of the attribute shdslRouter/router/trafficPolicy[ ]/tos2QueueMapping.</td></tr>
</table>

shdslRouter/router/trafficPolicy[ ]/dropPrecedence

Default:-
Range: table, see below

Use this attribute to define for each user configurable queue, how many packets with a certain drop level may be queued before they are dropped.

The dropPrecedence table contains the following elements:

Element	Description
maxLength1	This is the maximum length or drop level 1. Default:100 Range: 1 … 3000 In case you set the attribute shdslRouter/router/trafficPolicy[ ]/method to … • trafficShaping or tosMapped, then only this drop level is relevant. • tosDiffServ, then this drop level corresponds with the drop precendence bits value 00 and 01.
maxLength2	This is the maximum length or drop level 2. Default:100 Range: 1 … 3000 In case you set the attribute shdslRouter/router/trafficPolicy[ ]/method to … • trafficShaping or tosMapped, then this drop level is not relevant. • tosDiffServ, then this drop level corresponds with the drop precendence bits value 10.
maxLength3	This is the maximum length or drop level 3. Default:100 Range: 1 … 3000 In case you set the attribute shdslRouter/router/trafficPolicy[ ]/method to … • trafficShaping or tosMapped, then this drop level is not relevant. • tosDiffServ, then this drop level corresponds with the drop precendence bits value 11.

Example

Suppose …

- the shdslRouter/router/trafficPolicy[ ]/method is set to tosDiffServ.
- for queue 1 you set maxLength1 = 100, maxLength2 = 200 and maxLength3 = 50.

Now the following applies:

Queue 1 contains … data packets.	An incoming data packet with … is …		
	drop level[1] 1	drop level 2	drop level 3
less than 50	accepted	accepted	accepted
more than 50, less than 100	accepted	accepted	dropped
more than 100, less than 200	dropped	accepted	dropped
more than 200	dropped	dropped	dropped

1. As defined in the TOS field.

shdslRouter/router/trafficPolicy[ ]/trafficShaping

Default:<empty>
Range: table, see below

In case you have set the shdslRouter/router/trafficPolicy[ ]/method attribute to trafficShaping, then use the trafficShaping table to specify which data has to be redirected to which queue.

The trafficShaping table can be compared with an access list. You can “filter” based on several criteria (IP source and destination address, TOS value, etc.). A packet is redirected to the specified queue when the criteria are met and an overload condition occurs. When more than one entry applies to the same packet, then only the most specific one is taken in consideration. I.e. the entry covering the smallest range.

The trafficShaping table contains the following elements:

Element	Description
sourceIpStart-Address sourceIpEnd-Address	This is the IP source address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
destinationIpStart-Address destinationIpEnd-Address	This is the IP destination address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
tosStartValue tosEndtValue	This is the Type Of Service field value. Default:any(start)/optional(end) Range: 0 … 256
ipProtocol	This is the protocol field from the IP header. Default:any Range: 0 … 255 You can specify the protocol by typing the protocol number. For ease of use, some common protocols can be selected from a drop-down box: any (0), ICMP (1), IGMP (2), IPinIP (4), TCP (6), EGP (8), IGP (9), UDP (17), RSVP (46), IGRP (88), OSPFIGP (89), TCPestablished (255).
sourcePortStart sourcePortEnd	This is the source port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: any or optional (0), echo (7), discard (9), ftp-data (20), ftp (21), telnet (23), smtp (25), domain (53), www-http (80), pop3 (110), nntp (119), snmp (161), snmptrap (162), z39.50 (210), syslog (514), router (520), socks (1080), l2tp (1701), telindus (1728).

Element	Description
destinationPortStart destinationPortEnd	This is the destination port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: see above.
newTosValue	This is the new TOS field value. Default:unchanged Range: 0 … 256 When you select a new TOS field value, then a packet that matches an entry in the trafficShaping table its TOS field value is changed and the packet is redirected to a queue. Selecting unchanged, leaves the TOS field value as it is.
priority	This is the destination queue for a packet matching an entry in the trafficShaping table. Default:Queue1 Range: enumerated, see below The priority element has the following values: Queue1, Queue2, Queue3, Queue4, Queue5, lowDelayQueue.

Start and end values

Except for the ipProtocol, newTosValue and priority elements, it is possible to specify ranges using the start and end values. There are two special cases:

- A start value is entered, but no end value ⇒ an exact match is needed for the start value.
- Neither a start nor an end value is entered ⇒ the field is not checked.

shdslRouter/router/trafficPolicy[ ]/tos2QueueMapping

Default:<empty>
Range: table, see below

In case you have set the shdslRouter/router/trafficPolicy[ ]/method attribute to tosMapped, then use the tos2QueueMapping table to specify which data has to be redirected to which queue.

The tos2QueueMapping table contains the following elements:

Element	Description
startTos endTos	Traffic that has a Type Of Service field value within the specified range is redirected to the specified queue. Default:0 (start) / 255 (end) Range: 0 … 255
targetQueue	This is the destination queue for a packet matching an entry in the tos2QueueMapping table. Default:Queue1 Range: enumerated, see below The targetQueue element has the following values: Queue1, Queue2, Queue3, Queue4, Queue5, lowDelayQueue.

8.11 Bridging configuration attributes

shdslRouter/bridge/spanningTree

Default:-
Range: structure, see below

Use this attribute to set the bridging configuration attributes.

Whereas the bridgePortInfo attribute groups the bridging attributes that are applicable on an individual interface, the spanningTree attribute groups the bridging attributes that are applicable on the bridge as a whole.

The spanningTree structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>spanningTree-
Protocol</td><td>This sets the spanning tree protocol.

Default:none
Range: enumerated, see below

The spanningTreeProtocol element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>none</td><td>The Telindus 1420 SHDSL Router uses the self-learning principle.

This means that the bridge itself learns which data it has to forward and which data it has to block. I.e. it builds its own bridging table.</td></tr>
<tr><td>IEEE p802.1D</td><td>The Telindus 1420 SHDSL Router uses the self-learning principle in conjunction with the Spanning Tree protocol.

Because Spanning Tree bridging is somewhat more complicated than self-learning bridging, an introduction is given in 5.9.3 - What is Spanning Tree? on page 93.</td></tr>
</table>

When using Frame Relay encapsulation on the WAN interface together with the Spanning Tree protocol, every DLCI is considered as a separate bridge port. Each DLCI link is than considered as a special kind of LAN with only both end points connected.</td></tr>
<tr><td>bridgePriority</td><td>The bridge its MAC address together with the bridgePriority element form a unique bridge identifier. This identifier is used to determine which bridge becomes the root bridge.

Default:32768
Range: 0 … 65535

The bridge with the lowest bridgePriority value becomes the root bridge. If two bridges have the same bridgePriority value, then the bridge with the lowest MAC address becomes the root bridge.</td></tr>
</table>

Element	Description
bridgeMaxAge	This changes the time the bridge retains bridging information before discarding it. Default:00000d 00h 00m 20s Range: 00000d 00h 00m 06s - 00000d 00h 00m 40s
bridgeHelloTime	The root bridge regularly sends Configuration BPDUs, also called Hello messages. This element changes the Hello message interval. Default:00000d 00h 00m 02s Range: 00000d 00h 00m 01s - 00000d 00h 00m 10s
bridgeForwardDelay	This changes … • the delay a bridge port applies to move from listening state to learning state or from learning state to forwarding state. For more information on the possible states of a bridge port, refer to Bridge port states on page 200. • the time-out (or ageing) for purging MAC addresses from the bridge cache in case a topology change is detected. Default:00000d 00h 00m 15s Range: 00000d 00h 00m 04s - 00000d 00h 00m 30s

shdslRouter/bridge/bridgeTimeOut

Default:00000d 00h 05m 00s
Range: 00000d 00h 00m 00s- 24855d 03h 14m 07s

Use this attribute to change the time-out (or ageing) for MAC addresses learned by the Telindus 1420 SHDSL Router.

When this time-out expires, the MAC address is purged from the address database (also called bridge cache). This in case no topology change is detected, otherwise the time-out is equal to the value of the shdslRouter/bridge/spanningTree/bridgeForwardDelay element.

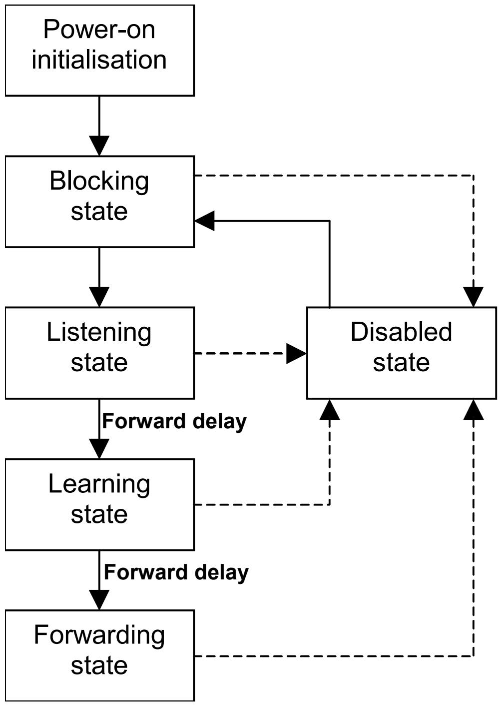
Bridge port states

There are four possible states a bridge port can be in:

State	A port in this state …
blocking	• does no frame forwarding. • does not incorporate station location into its address database (There is no learning on a blocking port, so there is no MAC address database update.). • receives BPDUs, but does not process or propagate them. A bridge always enters the blocking state following bridge initialisation.
listening	• does no frame forwarding. • does not incorporate station location into its address database (There is no learning on a listening port, so there is no MAC address database update.). • receives and processes BPDUs, but does not propagate them.
learning	• does no frame forwarding. • incorporates station location into its MAC address database. • receives, processes and propagates BPDUs.
forwarding	• forwards frames. • incorporates station location into its MAC address database. • receives, processes and propagates BPDUs.

Bridge port state transition diagram

The following figure shows how a bridge port moves through the different states when the bridge is powered:



When you enable Spanning Tree, every bridge in the network goes through the transitory states of listening and learning at power up. If properly configured, each port stabilises to the forwarding or blocking state.

When the spanning-tree algorithm places a port in the forwarding state, the following process occurs:

1. The port is put into the listening state while it waits for protocol information that suggests it should go to the blocking state.
2. The port waits for the expiration of the forward delay timer, moves the port to the learning state, and resets the forward delay timer.
3. In the learning state, the port continues to block frame forwarding as it learns station location information for the forwarding database.
4. The port waits for the expiration of the forward delay timer and then moves the port to the forwarding state, where both learning and forwarding are enabled.

8.12 SNMP proxy configuration attributes

shdslRouter/snmpProxy/trapDestinations

Default:<empty>
Range: table, see below

Use this attribute to define to which IP address the SNMP traps have to be sent.

The Telindus 1420 SHDSL Router translates all alarm status changes into SNMP traps. These traps can then be sent to a management system. To enable this, configure in the trapDestinations table the IP addresses to which the traps have to be sent. If the trapDestinations table is empty then no traps are sent.

The trapDestinations table contains the following elements:

Element	Description
address	This is the IP address of the management station to which the SNMP trap messages have to be sent. Default:0.0.0.0 Range: up to 255.255.255.255
community	This is the community string which is included in the SNMP traps that are sent to the management station. It is used as a password in the SNMP communication. Give it the same value as on your SNMP management station. Default:public Range: max. 20 characters

shdslRouter/snmpProxy/mib2Traps

Default:off Range: on / off

Use this attribute to enable (on) or disable (off) the sending of SNMP traps as MIB2 traps.

If you want to send the SNMP traps as MIB2 traps, proceed as follows:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Select the trapDestinations attribute. Add an entry to this table for each network management station that should receive SNMP traps.</td></tr>
<tr><td>2</td><td>In the trapDestinations table, define the IP address of the management stations that should receive the SNMP traps.</td></tr>
<tr><td>3</td><td>In the trapDestinations table, configure the community element associated with each trap destination.</td></tr>
<tr><td>4</td><td>Configure the mib2Traps attribute:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>on</td><td>Select this value if the management station is any SNMP station (without the TMA for HP OpenView application). In that case, the Telindus 1420 SHDSL Router sends the alarms coldBoot, warmBoot and linkDown as MIB2 traps instead of enterprise specific (private) MIB traps.</td></tr>
<tr><td>off</td><td>Select this value if the management system is the TMA for HP OpenView application. In that case the Telindus 1420 SHDSL Router sends all alarms as enterprise specific (private) MIB traps.</td></tr>
</table></td></tr>
<tr><td>5</td><td>Set for each object of the Telindus 1420 SHDSL Router:
• the alarms that you want to send using the attribute alarmMask.
• the importance of each alarm using the attribute alarmLevel.
By default only the most important alarms are enabled.</td></tr>
</table>

8.13 Management configuration attributes

shdslRouter/management/cms2Address

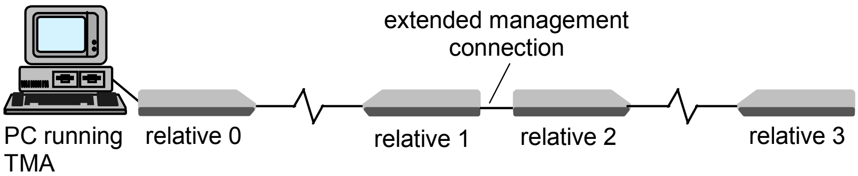
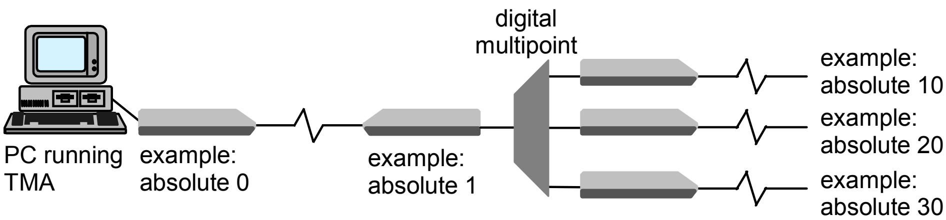
Default:0	
Range: 0 … 65535	

Use this attribute to assign an absolute address to the Telindus 1420 SHDSL Router.

What is relative and absolute addressing?

If you want to connect with TMA to a Telindus device, you have to specify the address of the device in the *Connect…* window. Refer to 4 - Managing the Telindus 1420 SHDSL Router on page 37.

There are two different address types: relative and absolute. The following table explains the difference between these address types:

Type	Description
relative	This type of addressing is meant for a network topology where the Telindus devices are connected in-line on management level. I.e. with extended management links between two Telindus devices. An extended management link is realised with a cross connect cable between the auxiliary connectors of two Telindus devices.  To enable relative addressing, no address has to be specified in the modem.
absolute	This type of addressing is meant for a network topology where the Telindus devices are not connected in-line on management level. I.e. when there is a digital multi-point device present.  To enable absolute addressing, an address has to be specified in the Telindus 1420 SHDSL Router. Do this with the cms2Address attribute.

shdslRouter/management/accessList

Default:<empty>
Range: table, see below

Use this attribute to control the access from certain hosts or networks.

The access list filters *incoming* traffic for the Telindus 1420 SHDSL Router, based on the source IP address. You can specify multiple entries within the access list. When more than one entry applies to the same packet, then only the most specific one is taken in consideration. I.e. the entry covering the smallest range. If not one entry matches, then the packet is dropped. If the access list is empty, then all packets are forwarded.

The accessList table contains the following elements:

Element	Description
sourceAddress	This is the IP source address of the packet. The address may be a (sub)network address. Default:0.0.0.0 Range: up to 255.255.255.255
mask	This is the IP subnet mask for the sourceAddress. By combining an IP address with a mask you can uniquely identify a range of addresses. Before comparing IP addresses, a logical AND function is made between both addresses and the mask. Default:255.255.255.255 Range: up to 255.255.255.255
action	This defines which action has to be taken when a packet arrives with a source IP address that falls within the specified address range. Default:deny Range: enumerated, see below The possible actions are: **Value** – **Description** deny – The packet is dropped. allow – The packet is forwarded.

If you specify one entry or multiple entries for which the action is set to deny, then also specify at least one entry for which the action is set to allow. Else all packets are dropped!

shdslRouter/management/snmp

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enable) or discard (disable) SNMP requests.

shdslRouter/management/telnet

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enable) or discard (disable) Telnet sessions.

Use this attribute also to accept (enable) or discard (disable) HTTP (Web Interface) sessions.

shdslRouter/management/tftp

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enable) or discard (disable) TFTP sessions.

shdslRouter/management/consoleNoTrafficTimeOut

Default:00000d 00h 30m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to automatically close a management session if there is no user interaction during a certain time-out period. This time-out period can be set with the consoleNoTrafficTimeOut attribute.

The purpose of such a timer is to protect the Telindus 1420 SHDSL Router against unauthorised access in case the last user did not close his session.

shdslRouter/management/ctrlPortProtocol

Default:console
Range: enumerated, see below

Use this attribute to define what purpose the auxiliary connector of the Telindus 1420 SHDSL Router has to serve.

The ctrlPortProtocol attribute has the following values:

Value	Description
management	Select this value if you want to connect the auxiliary connector of the Telindus 1420 SHDSL Router to … • the Orchid 1003 LAN for management purposes. • the auxiliary connector of another Telindus 1420 SHDSL Router using a crossed cable (i.e. they are connected back-to-back) in order to create an extended management link. For more information on extended management links, refer to What is relative and absolute addressing? on page 204. When connecting the auxiliary connector of the Telindus 1420 SHDSL Router to a COM port of your computer, you can still open a TMA session on the Telindus 1420 SHDSL Router. You can however not open a CLI or ATWIN session.
console	Select this value if you want to connect the auxiliary connector of the Telindus 1420 SHDSL Router to a COM port of your computer in order to manage the Telindus 1420 SHDSL Router using TMA, CLI or ATWIN.

shdslRouter/management/alarmFilter

Default:0	Range: 0 … 50000

Use this attribute to selectively ignore / drop alarms in TMA for HP Open-View if these alarms are below a certain level.

The filter number that you define using the alarmFilter attribute, has to correspond with a filter that you have to define in the Alarm Manager of TMA for HP OpenView. In the Alarm Manager, it is possible to specify a minimum alarm level that is needed before alarms are logged in HP OpenView. This can be specified for each filter number.

shdslRouter/management/loopback/ipAddress

Default:0.0.0.0	Range: up to 255.255.255.255

Use this attribute to assign an IP address to the loop-back interface.

The loop-back interface is a software interface which can be used for management purposes. This interface is always up, regardless of the state of the physical interfaces. This means the router will always respond to ICMP echo requests sent to this address. In every other respect the loop-back address behaves the same as an IP address of a physical interface.

If the loop-back address is used and RIPv2 is active, then a host route to the loop-back address is included in the RIP updates.

9 Status attributes

This chapter discusses the status attributes of the Telindus 1420 SHDSL Router. The following gives an overview of this chapter:

9.1 Status attribute overview

> shdslRouter
- sysDescr
- sysObjectID
- sysUpTime
- sysServices
- flash1Version
- flash2Version
- activeFlash
- bootVersion
- flashVersions
- messages
- deviceId
- configurationSaving

>> lanInterface
- ipAddress
- ipNetMask
- secondaryIpAddresses
- ifDescr
- ifType
- ifSpeed
- ifMtu
- ifOperStatus
- ifLastChange
- macAddress
- arpCache
- ipAdEntBcastAddr
- ipAdEntReasmMaxSize
- bridgePortStatus
- Action: clearArpCache

>> wanInterface
- ipAddress
- ipNetMask
- secondaryIpAddresses
- ifDescr
- ifType
- ifMtu
- ifOperStatus
- ifLastChange

>>> frameRelay
- lmi
- dlciTable
- cllmLastCongestionCause

>>> ppp
- lcpState
- ipcpState
- bcpState
- lcpMyOptions
- lcpHisOptions
- ipcpMyOptions
- ipcpHisOptions
- bcpMyOptions
- bcpHisOptions
- myAuthenState
- hisAuthenState
- bridgePortStatus

>>> hdlc
- bridgePortStatus

>>> line
- ifDescr
- ifType
- ifSpeed
- ifOperStatus

>>>> linePair [1]
- timeSinceLastRetrain
- status
- lineAttenuation
- noiseMargin

>> router
- routingTable
- natAddresses
- dhcpBinding
- dhcpStatistics

>>> tunnels
- l2tpTunnels

>> bridge
- bridgeCache
- spanningTree
- Action: clearBridgeCache

>> management
- cms2Address

>>> loopback

ipAddress
ifDescr
ifType
ifSpeed
ifMtu
ifOperStatus

>> operatingSystem

taskInfo

9.2 General status attributes

shdslRouter/sysDescr

This attribute is a textual description of the device. It is an SNMP MIB2 parameter.

Example: Telindus 1420 SHDSL Router Txxxx/xxxxx 01/01/00 12:00

In this example the following parameters are visible:

- Telindus 1420 SHDSL Router is the device name.
- Txxxx/xxxxx is the firmware code and version.
- 01/01/00 12:00 is the firmware release date and time.

shdslRouter/sysObjectID

This attribute is the SNMP identification string. This is an SNMP MIB2 parameter.

shdslRouter/sysUpTime

This attribute displays the elapsed time since the last power-on or cold boot of the Telindus 1420 SHDSL Router.

shdslRouter/sysServices

This attribute is the SNMP service identification. This is an SNMP MIB2 parameter.

shdslRouter/flash1Version

This attribute displays the code and version of the firmware currently stored in flash memory bank 1. If this value is empty then flash memory bank 1 does not contain firmware.

Example: Txxxx/xxxxx 01/01/00 12:00

In this example the following parameters are visible:

- Txxxx is the firmware code for this device.
- /xxxxx is the firmware version.
- 01/01/00 is the firmware release date.
- 12:00 is the firmware release time.

shdslRouter/flash2Version

This attribute displays the code and version of the firmware currently stored in flash memory bank 2. If this value is empty then flash memory bank 2 does not contain firmware or the Telindus 1420 SHDSL Router is equipped with one flash memory bank only.

shdslRouter/activeFlash

This attribute displays which flash memory bank is currently active. If the Telindus 1420 SHDSL Router is equipped with one flash memory bank only, then this value is always flash1.

shdslRouter/bootVersion

This attribute displays the code and version of the boot software currently used in the Telindus 1420 SHDSL Router.

shdslRouter/flashVersions

This attribute indicates how many flash memory banks are present in the Telindus 1420 SHDSL Router. Hence it indicates how many firmware versions can be stored in the Telindus 1420 SHDSL Router. Possible values are 1 and 2.

shdslRouter/messages

This attribute displays informative and error messages, e.g. Reconfigured, Cold Boot, … The messages table displays maximum 20 messages.

If you open a TMA session on the Telindus 1420 SHDSL Router over IP, i.e. not through the auxiliary port, then the messages are also sent to the auxiliary port. This means that if you open a terminal emulation session on the auxiliary port, you can monitor these messages. If you hit the ENTER key, the messages stop and you get the (CLI) password prompt.

shdslRouter/deviceId

This attribute displays a unique code. This code is programmed into the Telindus 1420 SHDSL Router before it leaves the factory. You can use this code for inventory purposes.

shdslRouter/configurationSaving

This attribute indicates when the Telindus 1420 SHDSL Router is writing its (new) configuration to the flash memory. Possible values are:

Value	Description
busy	The Telindus 1420 SHDSL Router is busy writing its configuration to the flash memory. During this state, do not power-down or reboot the Telindus 1420 SHDSL Router else the new configuration will be lost.
done	The Telindus 1420 SHDSL Router has finished writing its configuration to the flash memory.

9.3 LAN interface status attributes

shdslRouter/lanInterface/ipAddress

This attribute displays the IP address of the LAN interface. It is either configured with the configuration attribute ipAddress or automatically retrieved with BootP.

shdslRouter/lanInterface/ipNetMask

This attribute displays the IP subnet mask of the LAN interface. It is either configured with the configuration attribute ipNetMask or automatically retrieved with BootP.

shdslRouter/lanInterface/secondaryIpAddresses

This attribute displays the secondary IP addresses as you configured them with the configuration attribute secondaryIpAddresses.

shdslRouter/lanInterface/ifDescr

This attribute is the interface description. This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifType

This attribute is the interface type. This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifSpeed

This attribute displays the LAN interface speed in bits per second (bps), e.g. 10000000.

shdslRouter/lanInterface/ifMtu

This attribute displays the interface its Maximum Transfer Unit, i.e. the maximum number of bytes that one packet can contain on this interface.

This is an SNMP MIB2 parameter.

The Telindus 1420 SHDSL Router never fragments packets, since both its LAN and WAN interfaces have the same MTU value (being 1520).

shdslRouter/lanInterface/ifOperStatus

This attribute displays the current operation status of the LAN interface. Possible values are:

Value	Description
up	The LAN interface is up, data transfer is possible.
down	The LAN interface is down, data transfer is not possible.

shdslRouter/lanInterface/ifLastChange

This attribute shows the system-up time on the moment the interface entered its current operation state. I.e. the moment the value of the ifOperStatus status attribute changes (from up to down or vice versa), the system-up time value is written into the ifLastChange status attribute.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/macAddress

This attribute displays the MAC address of the Telindus 1420 SHDSL Router its LAN interface, e.g. 00:C0:89:00:8E:23.

The LAN interface has been allocated a fixed Ethernet address, also called MAC (Medium Access Control) address. The MAC address is globally unique and can not be modified. It is a 6 byte code, represented in hexadecimal format. Each byte in the code is separated by a colon.

For more information on the MAC address, refer to the configuration attribute shdslRouter/lanInterface/arpTimeOut on page 158.

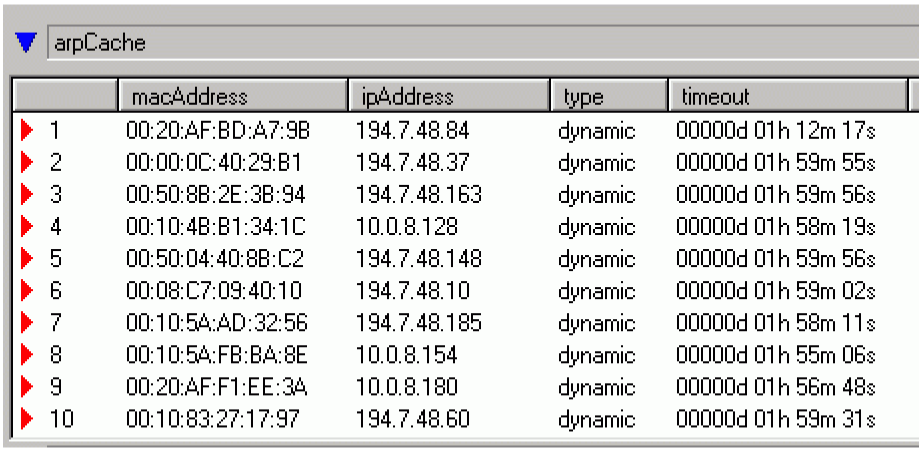
shdslRouter/lanInterface/arpCache

This attribute displays all the MAC address - IP address pairs from ARP requests and replies received on the LAN interface. For more information on the ARP cache, refer to the configuration attribute shdslRouter/lanInterface/arpTimeOut on page 158.

The arpCache table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>macAddress</td><td>This is the corresponding MAC address, e.g. 00:C0:89:00:0F:ED.</td></tr>
<tr><td>ipAddress</td><td>This is the IP address.</td></tr>
<tr><td>type</td><td>This is the ARP cache entry type. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>dynamic</td><td>The MAC - IP address pair is retrieved from an ARP request or reply message.</td></tr>
<tr><td>static</td><td>The MAC - IP address pair is configured.
There is only one static entry, i.e. the Telindus 1420 SHDSL Router its own IP and MAC address.</td></tr>
</table></td></tr>
<tr><td>timeOut</td><td>This is the time the entry will remain in the ARP cache. For the static entry, this value is 0.</td></tr>
</table>

The following figure shows part of an ARP cache table as an example:


arpCache

	macAddress	ipAddress	type	timeout
1	00:20:AF:BD:A7:9B	194.7.48.84	dynamic	00000d 01h 12m 17s
2	00:00:0C:40:29:B1	194.7.48.37	dynamic	00000d 01h 59m 55s
3	00:50:8B:2E:3B:94	194.7.48.163	dynamic	00000d 01h 59m 56s
4	00:10:4B:B1:34:1C	10.0.8.128	dynamic	00000d 01h 58m 19s
5	00:50:04:40:8B:C2	194.7.48.148	dynamic	00000d 01h 59m 56s
6	00:08:C7:09:40:10	194.7.48.10	dynamic	00000d 01h 59m 02s
7	00:10:5A:AD:32:56	194.7.48.185	dynamic	00000d 01h 58m 11s
8	00:10:5A:FB:BA:8E	10.0.8.154	dynamic	00000d 01h 55m 06s
9	00:20:AF:F1:EE:3A	10.0.8.180	dynamic	00000d 01h 56m 48s
10	00:10:83:27:17:97	194.7.48.60	dynamic	00000d 01h 59m 31s

shdslRouter/lanInterface/ipAdEntBcastAddr

This attribute displays the value of the least-significant bit in the IP broadcast address. This address is used for sending packets on the interface which is associated with the IP address of this entry. The value applies to both the general broadcast, the subnet and network broadcasts.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ipAdEntReasmMaxSize

This attribute displays the size of the largest IP packet which this entity can re-assemble from incoming IP fragmented packets received on this interface. Value 0 means there is no re-assembly.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/bridgePortStatus

This attribute displays the bridging status of the LAN interface.

The bridgePortStatus structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>state</td><td>This displays the current state of the port. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled[1]</td><td>The port is not in use because of a management action.</td></tr>
<tr><td>blocking</td><td>The port does not participate in frame forwarding.</td></tr>
<tr><td>listening</td><td>The port prepares to participate in frame forwarding, but it does not update its MAC address database (also called bridge cache).</td></tr>
<tr><td>learning</td><td>The port prepares to participate in frame forwarding, and it learns the present MAC addresses.</td></tr>
<tr><td>forwarding[1]</td><td>The port participates in frame forwarding.</td></tr>
</table>
1. These are the only possible port states for a bridge that is not running the Spanning Tree protocol (IEEE p802.1D).

For more detailed information on port states, refer to Bridge port states on page 200.</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>subState</td><td>This gives additional information on the port state. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>root</td><td>This is the port through which the root bridge can be reached. Consequently, the root bridge itself does not have a root port. All other bridges must have a root port.</td></tr>
<tr><td>designated</td><td>This is the designated port for this (virtual) LAN. All ports of the root bridge are designated ports.</td></tr>
<tr><td>alternate</td><td>This port is not active. Either because of a management action, or through protocol intervention.</td></tr>
</table></td></tr>
<tr><td>designatedPriority
designatedMac</td><td>Together, these two attributes form a unique bridge identifier. Depending whether the current port is a designated port or not, these two attributes display the unique bridge identifier of …
• the bridge to which this port belongs, in case of a designated port.
• the bridge believed to be the designated bridge for the LAN that is currently connected to this port, in all other cases.
This bridge identifier is used …
• together with the designatedPortPriority and designatedPortId attributes to determine whether this port should be the designated port for the LAN that is currently connected to this port.
• to test the value of the bridge identifier parameter conveyed in received Configuration BPDUs.</td></tr>
<tr><td>designatedPort-Priority
designatedPortId</td><td>Together, these two attributes form a unique port identifier. They display the unique port identifier of the bridge port through which the designated bridge transmits the configuration message information stored by this port.
This port identifier is used …
• together with the designatedPriority and designatedMac attributes to determine whether this port should be the designated port for the LAN that is currently connected to this port.
• by the management system to determine the topology of the bridged LAN.</td></tr>
<tr><td>topologyChangeAck</td><td>This displays the value of the Topology Change Acknowledgement flag in the next Configuration BPDU that will be transmitted on this port.
This attribute is used to assess the need to set the Topology Change Acknowledgement flag in response to a received Topology Change Notification BPDU.</td></tr>
<tr><td>configurationPend-ing</td><td>This is used to determine whether a Configuration BPDU should be transmitted on this port after expiry of the hold timer. This avoids that Configuration BPDUs are transmitted too often, although ensuring that up-to-date information is transmitted.</td></tr>
</table>

shdslRouter/lanInterface/clearArpCache

If you execute this action, the ARP cache table is cleared.

9.4 WAN interface status attributes

Several status attributes of the WAN interface are the same as on the LAN interface. Therefore, they are not explained here again. These attributes are: ipAddress, ipNetMask, secondaryIpAddresses, ifDescr, ifType, ifMtu and ifLastChange.

For a complete description of these attributes, refer to 9.3 - LAN interface status attributes on page 215.

The attribute ifOperStatus is also present on the LAN interface, but behaves somewhat differently on the WAN interface.

shdslRouter/lanInterface/ifOperStatus

This attribute displays the current operation status of the WAN interface. Possible values are:

Value	Description
up	The WAN interface is up, data transfer is possible. The following table shows you in which case the value of the ifOperStatus attribute is up: **Protocol** — **The ifOperStatus attribute is up (i.e. the alarm wanInterface/alarmInfo/linkDown = off) in case …** Frame Relay — LMI is up. PPP — LCP is open.
down	The WAN interface is down, data transfer is not possible.

Important remarks

- Whether the Telindus 1420 SHDSL Router is configured in bridging or routing has no effect on the value of the attributes shdslRouter/wanInterface/ifOperStatus:Status and shdslRouter/wanInterface/alarmInfo/linkDown:Alarms.
- In case of Frame Relay, if the configuration attribute element shdslRouter/wanInterface/frameRelay/lmi/type is set to noLmiConfigured, then the value of the attribute shdslRouter/wanInterface/frameRelay/lmi/state:Status is always up. However, the other conditions as stated in the table above remain.
- In case of PPP, if the configuration attribute element shdslRouter/wanInterface/ppp/linkMonitoring/operation is set to disabled, then it is possible that the ifOperStatus value does not go down even if the link quality is too bad for a proper data link. This because the link monitoring mechanism is the only PPP mechanism that will start a renegotiation of the LCP layer.

9.5 WAN encapsulation status attributes

This section discusses the status attributes of the encapsulation protocols that can be used on the WAN interface.

The following gives an overview of this section:

9.5.1 Frame Relay status attributes

shdslRouter/lanInterface/frameRelay/lmi

This attribute gives a complete LMI status information overview.

The lmi structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>type</td><td>This displays the LMI variant. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>noLmiConfigured</td><td>No LMI is in use.</td></tr>
<tr><td>lmiRev1</td><td>LMI revision 1 is in use.</td></tr>
<tr><td>ansit1-617-d</td><td>ANSI LMI is in use.</td></tr>
<tr><td>q933-Annex-A</td><td>ITU-T LMI is in use.</td></tr>
</table></td></tr>
<tr><td>state</td><td>This displays the current state of LMI. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>up</td><td>LMI messages can and are exchanged.</td></tr>
<tr><td>down</td><td>No LMI messages can be exchanged.</td></tr>
</table></td></tr>
<tr><td>lastStateChange</td><td>This is the system-up time when the LMI state entered its current state. I.e. the moment the value of the state element changes (from up to down or vice versa), the system-up time value is written into the lastStateChange element.</td></tr>
<tr><td>subState</td><td>This is a bit string indicating the following LMI sub-states:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>startup</td><td>This is a transient state at start-up. It remains in this state if no LMI has been configured.</td></tr>
<tr><td>wait response</td><td>This bit is set if the DTE is waiting on a response on a Status Enquiry message.</td></tr>
<tr><td>usr error</td><td>This bit is set in case the DTE …
• has not received a response on a (Full) Status Enquiry message within the given pollingInterval.
• has received an error message.</td></tr>
<tr><td>expect poll</td><td>This bit is set if the DCE is waiting on a response on a Status Enquiry message.</td></tr>
<tr><td>net error</td><td>This bit is set in case the DCE …
• has not received a response on a (Full) Status Enquiry message within the given pollingInterval.
• has received an error message.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>lastError</td><td>This displays the last error condition reported by LMI. Possible values are: none, protocol error, unknown information element, sequence error, unknown report, timer expired, invalid report type, unsolicited status.</td></tr>
<tr><td>netTxSeqNr</td><td>This is the sequence number of the last LMI response frame sent towards the network.</td></tr>
<tr><td>netRxSeqNr</td><td>This is the sequence number of the last LMI command frame received from the network.</td></tr>
<tr><td>netErrors</td><td>This is the number of errors on LMI commands issued by the network during the last monitoredEvents period.</td></tr>
<tr><td>userTxSeqNr</td><td>This is the sequence number of the last LMI command frame sent towards the router.</td></tr>
<tr><td>userRxSeqNr</td><td>This is the sequence number of the last LMI response frame received from the router.</td></tr>
<tr><td>userErrors</td><td>This is the number of errors on LMI commands issued by the router during the last monitoredEvents period.</td></tr>
<tr><td>userWaitFullEnquiry</td><td>This is the number of LMI frames still to be sent before a Full Status Enquiry will be requested.</td></tr>
<tr><td>userLastReport-TypeSent</td><td>This displays the type of the most recent report that was sent. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>full status</td><td>The last report contained the full status.</td></tr>
<tr><td>link integrity</td><td>The last report only contained the link integrity information.</td></tr>
</table>
</td></tr>
</table>

shdslRouter/lanInterface/frameRelay/dlciTable

This attribute gives the complete status information of all known DLCIs.

The dlciTable table contains the following elements:

Element	Description
dlci	This is the DLCI identification number.
committedBurst	Displays the current CIR value for the corresponding DLCI. When no BECNs (Backward Explicit Congestion Notifications) are received, then this value is the same as the initialised value. For dynamically added DLCIs no CIR values are known.
excessBurst	Displays the initialised EIR value. For dynamically added DLCIs no EIR values are known.
gateway	This is the IP address of the corresponding gateway.
local	This is the address used in the response on an Inverse ARP request received on this DLCI.
active	This indicates whether the corresponding DLCI is active (on) or not (off).
new	This is set to on if the DLCI has just been created, else it is off.
deleted	This is set to on if the DLCI has been deleted, else it is off.
rr	This element is only relevant for LMI revision 1. It is the flow control flag. If it is on, then no traffic can be sent on this DLCI. Else it is off.
bandwidth	This is the available bandwidth on this DLCI as it is communicated by the Frame Relay network.
cllmLastCongestion-Cause	CLLM (Consolidated Link Layer Management) is a Frame Relay protocol used for traffic management. The cllmLastCongestionCause element indicates the last reason, which was received from the network, for congestion on the corresponding DLCI. For possible values, refer to the status attribute shdslRouter/lanInterface/frameRelay/cllm-LastCongestionCause on page 225.
bridgePortStatus	This displays the bridging status of the Frame Relay WAN interface. For more information, refer to the status attribute shdslRouter/lanInterface/bridgePortSta-tus on page 218.

shdslRouter/lanInterface/frameRelay/cllmLastCongestionCause

This attribute indicates the last reason, which was received from the network, for congestion on any of the DLCIs. Possible values are:

- none
- short term, excessive traffic
- long term, excessive traffic
- short term, equipment failure
- long term, equipment failure
- short term, maintenance action
- long term, maintenance action
- short term, unknown cause
- long term, unknown cause
- unknown cause

9.5.2 PPP status attributes

shdslRouter/lanInterface/ppp/lcpState

This attribute reflects the status of the LCP (Link Control Protocol) protocol. Possible values are:

Value	Description
Initial	LCP handshake has not started yet.
Starting, Closed, Stopped, Closing, Stopping	These values correspond with the transient states in the LCP state diagram.
Req-Sent	The local side of the PPP link has sent an LCP request. The remote side did not answer yet.
Ack-Rcvd	The local side of the PPP link has received an LCP acknowledge from the remote side. This is a transient state.
Ack-Sent	The local side of the PPP link has acknowledged the LCP request from the remote side.
Opened	The LCP handshake succeeded.

shdslRouter/lanInterface/ppp/ipcpState

This attribute reflects the status of the IPCP (Internet Protocol Control Protocol) protocol. The possible values are the same as those of shdslRouter/lanInterface/ppp/lcpState.

shdslRouter/lanInterface/ppp/bcpState

This attribute reflects the status of the BCP (Bridging Control Protocol) protocol. The possible values are the same as those of shdslRouter/lanInterface/ppp/lcpState.

shdslRouter/lanInterface/ppp/lcpMyOptions

During the LCP handshake, a number of options can be exchanged between the local and remote side of the link. This attribute lists the LCP options for the router at this side (local side) of the link.

The lcpMyOptions table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>option</td><td>The Telindus 1420 SHDSL Router supports the following LCP options:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>3</td><td>This is the Authentication-Protocol option.</td></tr>
<tr><td>5</td><td>This is the Magic-Number option.</td></tr>
</table>
For more information on the LCP configuration options, refer to RFC 1661.</td></tr>
<tr><td>length</td><td>This is the length of the option field.</td></tr>
<tr><td>value</td><td>This is the option value represented as an octet string (hexadecimal ASCII representation).</td></tr>
</table>

shdslRouter/lanInterface/ppp/lcpHisOptions

This attribute lists the LCP options for the router at the other side (remote side) of the link. The lcpMyOptions table contains the same elements as the shdslRouter/lanInterface/ppp/lcpMyOptions table.

Other option values than the ones supported by the Telindus 1420 SHDSL Router may be present.

shdslRouter/lanInterface/ppp/ipcpMyOptions

During the IPCP handshake, a number of options can be exchanged between the local and remote side of the link. This attribute lists the IPCP options for the router at this side (local side) of the link.

The ipcpMyOptions table contains the following elements:

Element	Description
option	The Telindus 1420 SHDSL Router supports the following IPCP option: • 3 : the IP-Address option. For more information on the IPCP configuration options, refer to RFC 1332.
length	This is the length of the option field.
value	This is the option value represented as an octet string (hexadecimal ASCII representation).

shdslRouter/lanInterface/ppp/ipcpHisOptions

This attribute lists the IPCP options for the router at the other side (remote side) of the link. The ipcpHisOptions table contains the same elements as the shdslRouter/lanInterface/ppp/ipcpMyOptions table.

Other option values than the ones supported by the Telindus 1420 SHDSL Router may be present.

shdslRouter/lanInterface/ppp/bcpMyOptions

During the BCP handshake, a number of options can be exchanged between the local and remote side of the link. This attribute lists the BCP options for the router at this side (local side) of the link.

The bcpMyOptions table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>option</td><td>The Telindus 1420 SHDSL Router supports the following LCP options:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>1</td><td>This is the Bridge-Identification option.</td></tr>
<tr><td>2</td><td>This is the Line-Identification option.</td></tr>
<tr><td>3</td><td>This is the MAC-Support option.</td></tr>
<tr><td>4</td><td>This is the Tinygram-Compression option.</td></tr>
<tr><td>5</td><td>This is the LAN-Identification option.</td></tr>
<tr><td>6</td><td>This is the MAC-Address option.</td></tr>
<tr><td>7</td><td>This is the Spanning-Tree-Protocol option.</td></tr>
</table>
For more information on the LCP configuration options, refer to RFC 2878.</td></tr>
<tr><td>length</td><td>This is the length of the option field.</td></tr>
<tr><td>value</td><td>This is the option value represented as an octet string (hexadecimal ASCII representation).</td></tr>
</table>

shdslRouter/lanInterface/ppp/bcpHisOptions

This attribute lists the BCP options for the router at the other side (remote side) of the link. The bcpMyOptions table contains the same elements as the shdslRouter/lanInterface/ppp/bcpMyOptions table.

Other option values than the ones supported by the Telindus 1420 SHDSL Router may be present.

shdslRouter/lanInterface/ppp/myAuthenstate

This attribute displays the authentication state of the router at this side (local side) of the link. I.e. the state of the authenticator. Possible values are:

Value	Description
No-Authentication	The local side does not request PPP authentication or still has to start the CHAP authentication (LCP handshake is busy).
Wait-On-Response	The local side has sent a challenge packet and is waiting for an answer.
Authen-Successful	The response packet is found to be correct. This is the state when authentication succeeded.
Authen-Failure	The response packet is found to be incorrect. This is a transient state since the router starts the LCP handshake again after a failing authentication.

shdslRouter/lanInterface/ppp/hisAuthenstate

This attribute displays the authentication state of the router at the other side (remote side) of the link. I.e. the state of the peer. Possible values are:

Value	Description
No-Authentication	This is the start-up state.
Wait-On-Challenge	During the LCP handshake the authenticator already indicates it wants to authenticate. From that moment on, the peer awaits a challenge packet.
Wait-On-Success	Once the peer has sent a response, it awaits a success or failure message.
Authen-Successful	The peer has received a success packet. It remains in this state during data transfer.
Authen-Failure	The peer has received a failure packet. This is a transient state since the router starts the LCP handshake again after a failing authentication.
Authen-Not-Allowed	This state only occurs when the peer does not accept the authentication request during the LCP handshake. A possible reason might be that the peer router does not support CHAP.

shdslRouter/lanInterface/ppp/bridgePortStatus

This attribute displays the bridging status of the PPP WAN interface.

For more information, refer to the status attribute shdslRouter/lanInterface/bridgePortStatus on page 218.

9.5.3 HDLC status attributes

---

shdslRouter/lanInterface/hdlc/bridgePortStatus

This attribute displays the bridging status of the HDLC WAN interface.

For more information, refer to the status attribute shdslRouter/lanInterface/bridgePortStatus on page 218.

9.6 Line status attributes

shdslRouter/wanInterface/line/ifDescr

This is the interface description. This is an SNMP MIB2 parameter.

shdslRouter/wanInterface/line/ifType

This is the interface type. This is an SNMP MIB2 parameter.

shdslRouter/wanInterface/line/ifSpeed

In case the attribute ifOperStatus is …

- up, the attribute ifSpeed displays the current line speed in bits per second (bps), e.g. 1152000.
- down, the attribute ifSpeed becomes 0.

shdslRouter/wanInterface/line/ifOperStatus

This attribute displays the current operation status of the line. Possible values are:

Value	Description
up	The line is up, data transfer is possible. This is in case the value of the attribute linePair [1]/status is dataState.
down	The line is down, data transfer is not possible.
testing	A line test is active.

shdslRouter/wanInterface/line/linePair [1]/timeSinceLastRetrain

This attribute displays the elapsed time since the last retrain cycle.

shdslRouter/wanInterface/line/linePair [1]/status

This attribute displays the status of the line. Possible values are:

Value	Description
idle	No link is present.
training	A training cycle is in progress.
dataState	A data link is present.

shdslRouter/wanInterface/line/linePair [1]/lineAttenuation

This attribute displays the current line attenuation in dB, e.g. 11.0.

shdslRouter/wanInterface/line/linePair [1]/noiseMargin

This attribute displays the current noise margin of the line in dB, e.g. 2.5.

9.7 Routing status attributes

shdslRouter/router/routingTable

This attribute lists all known routes with their operating status. This information is retrieved from the configured IP addresses, the static routes and the interface status.

The routingTable contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>network</td><td>This is the IP address of the destination network.</td></tr>
<tr><td>mask</td><td>This is the network mask of the destination network.</td></tr>
<tr><td>gateway</td><td>This is the IP address of the next router on the path to the destination network.</td></tr>
<tr><td>interface</td><td>This is the interface through which the destination network can be reached. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>internal</td><td>The own protocol stack is used.</td></tr>
<tr><td>lan</td><td>The destination network can be reached through the Ethernet interface.</td></tr>
<tr><td>wan</td><td>The destination network can be reached through the serial interface.</td></tr>
<tr><td>discard</td><td>Packets for this destination are discarded.</td></tr>
</table></td></tr>
<tr><td>encapsulation</td><td>This indicates the used encapsulation. It is related to the interface for this route. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>none</td><td>The IP packets are not encapsulated.</td></tr>
<tr><td>ethernet</td><td>The IP packets are encapsulated with the ARPA MAC header.</td></tr>
<tr><td>frameRelay</td><td>The IP packets are encapsulated in Frame Relay (RFC 1490).</td></tr>
<tr><td>ppp</td><td>The IP packets are encapsulated in PPP.</td></tr>
<tr><td>x25</td><td>The IP packets are encapsulated in X.25.</td></tr>
</table></td></tr>
<tr><td>status</td><td>This is the route status. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>up</td><td>The route can be used.</td></tr>
<tr><td>down</td><td>The route is currently not in use.</td></tr>
<tr><td>discard</td><td>Packets for this destination are discarded.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>preference</td><td>This displays the route preference.

If more than one route matches the IP destination address, this attribute determines which route is used. The route with the lowest preference value will be used.</td></tr>
<tr><td>type</td><td>This is the type of the route. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>host</td><td>This is a host route, i.e. a route to a single IP address instead of a complete network. This is also used for the router its own IP address.</td></tr>
<tr><td>internal</td><td>A route with this status is irrelevant.</td></tr>
<tr><td>local</td><td>This route is for directly connected networks.</td></tr>
<tr><td>rip</td><td>This route has been received by a RIP update.</td></tr>
<tr><td>static</td><td>This route has been configured, i.e. it is a static route.</td></tr>
</table></td></tr>
<tr><td>metric</td><td>If two routes exist with the same preference, then the route with the lowest metric value is chosen. The metric attribute serves as a cost for using the route. In most cases it indicates the number of hops (= routers) required to reach a destination.</td></tr>
<tr><td>timeOut</td><td>In case of a RIP route, the timeOut attribute displays the time the route will remain in the routing table if no RIP updates are received anymore. For other routes this attribute always displays 00000d 00h 00m 00s.</td></tr>
</table>

shdslRouter/router/natAddresses

This attribute displays the status of each official IP address which is configured in the natAddresses configuration attribute.

The natAddresses table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>officialAddress</td><td>This is the official IP address you entered it in the natAddresses configuration attribute.</td></tr>
<tr><td>privateAddress</td><td>This is the private IP address that is currently linked with the official IP address.</td></tr>
<tr><td>status</td><td>This is the status of the official IP address. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>free</td><td>This official IP address is currently not in use.</td></tr>
<tr><td>fixed</td><td>This address has a pre-configured mapping between the official and private IP address.</td></tr>
<tr><td>allocated</td><td>This official IP address is currently assigned to a private IP address, but it is not fixed.</td></tr>
</table></td></tr>
<tr><td>uses</td><td>This indicates how many sessions are currently used by this official IP address.
If the attribute value becomes zero, the assigned official IP address becomes free again and can be assigned to another private IP address.</td></tr>
</table>

shdslRouter/router/dhcpBinding

This attribute contains a list of dynamically assigned (i.e. leased) IP addresses.

The dhcpBinding table contains the following elements:

Element	Description
ipAddress	This is the IP address that is dynamically assigned to a client.
macAddress	This is the MAC address of the client.
leaseTime	This is the remaining lease time.

shdslRouter/router/dhcpStatistics

This attribute contains the statistics of all IP address ranges that have been specified in the configuration attribute dhcpDynamic.

The dhcpStatistics table contains the following elements:

Element	Description
startRange	Displays the IP start address of an IP address range.
endRange	Displays the IP end address of an IP address range.
free	For the corresponding IP address range, this displays the number of IP addresses that are still free.
lease	For the corresponding IP address range, this displays the number of IP addresses that are leased.
hold	For the corresponding IP address range, this displays the number of IP addresses that are on hold.

During power-down of the DHCP server, some leased IP addresses can still be active. Because the duration of the power-down can not be known, all timer information about lease and hold time becomes meaningless. Therefore, the DHCP server incorporated in the Telindus 1420 SHDSL Router sends a ping to all leased addresses after a warm boot. When the client responds to this ping, the DHCP server resets all timers to their default value and keeps the lease with this client.

9.8 L2TP tunnel status attributes

shdslRouter/router/tunnels/l2tpTunnels

This attribute gives you status information on the L2TP tunnels.

The l2tpTunnels table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>name</td><td>This is the name of the tunnel as you defined it in the configuration attribute l2tpTunnels.</td></tr>
<tr><td>ifOperStatus</td><td>This displays the operational status of the tunnel. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>up</td><td>The tunnel is up, data transfer is possible.</td></tr>
<tr><td>down</td><td>The tunnel is down, data transfer is not possible.</td></tr>
<tr><td>dormant</td><td>The tunnel is "stand-by". As soon as data has to be sent over the tunnel, control connect messages are exchanged and operational status of the tunnel becomes up.</td></tr>
</table></td></tr>
<tr><td>ifLastChange</td><td>This is the system-up time on the moment the interface entered its current operation state. I.e. the moment the value of the ifOperStatus status attribute changes (from up to down or vice versa), the system-up time value is written into the ifLastChange status attribute.</td></tr>
<tr><td>ip</td><td>This structure displays the IP address information of the tunnel. The ip structure contains the following elements:
<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>ipAddress</td><td>This is the IP address of the local side of the PPP connection inside of the tunnel as you configured it in the configuration structure l2tpTunnels/ip.</td></tr>
<tr><td>ipNetMask</td><td>This is the IP subnet mask of the local side of the PPP connection inside of the tunnel as you configured it in the configuration structure l2tpTunnels/ip.</td></tr>
</table></td></tr>
</table>

Element	Description
bridging	This structure displays the bridging information of the tunnel. For more information, refer to the status attribute shdslRouter/lanInterface/bridgePortStatus on page 218.
l2tp	This structure displays the L2TP information of the tunnel. For more information, refer to the shdslRouter/router/tunnels/l2tpTunnels/l2tp on page 238.
ppp	This structure displays the PPP information of the tunnel. For more information, refer to the status attributes shdslRouter/lanInterface/ppp/lcpState, shdslRouter/lanInterface/ppp/ipcpState, shdslRouter/lanInterface/ppp/bcpState, shdslRouter/lanInterface/ppp/myAuthenstate and shdslRouter/lanInterface/ppp/hisAuthenstate.

shdslRouter/router/tunnels/l2tpTunnels/l2tp

The l2tp structure in the l2tpTunnels table displays the L2TP information of the tunnel.

The l2tp structure contains the following elements:

Element	Description
sendingSeqNr	In case sequence numbering on the data messages is enabled (dataChannelSequenceNumbering = on), then this displays the transmit data sequence numbers.
receivingSeqNr	In case sequence numbering on the data messages is enabled (dataChannelSequenceNumbering = on), then this displays the receive data sequence numbers.
l2tpType	This displays which L2TP server type the Telindus 1420 SHDSL Router currently is: LAC or LNS. If you set the configuration attribute l2tpType to auto, then the status attribute l2tpType displays the auto value until the Telindus 1420 SHDSL Routers have mutually decided who will be the LAC and who the LNS.
controlState	This displays the states associated with the LNS or LAC control connection establishment. For more information, refer to L2TP status - control states on page 239.
callState	This displays the states associated with the LNS or LAC incoming or outgoing calls. For more information, refer to L2TP status - call states on page 240.
deliveryState	This displays the states associated with the LNS or LAC packet delivery. For more information, refer to L2TP status - delivery states on page 241.
authenState	This displays the states associated with the LNS or LAC authentication. For more information, refer to L2TP status - authentication states on page 242.

L2TP status - control states

The states associated with the LNS or LAC for control connection establishment are:

Value	Description
idle	No control connection is present. Both initiator and recipient start from this state. An initiator transmits a Start Control Connection Request, while a recipient remains in the idle state until receiving a Start Control Connection Request.
waitCtlReply	This is the state where a Start Control Connection Reply is awaited.
waitCtlConn	This is the state where a Start Control Connection Connected is awaited. Upon receipt, the challenge response is checked. The tunnel either is established, or is torn down if an authorisation failure is detected.
established	The control connection is established. An established connection may be terminated by either a local condition or the receipt of a Stop Control Connection Notification. The session then returns to the idle state.

L2TP status - call states

The states associated with the LNS or LAC incoming or outgoing calls are:

Value	Description
idle	No data is exchanged over the tunnel.
waitTunnel	This is the state in which is waited … • either for the control connection to be opened, • or for verification that the tunnel is already open. Once an indication is received that the tunnel has/was opened, session control messages may be exchanged. The first of these is the Incoming Call Request.
waitReply	This is the state where an Incoming or Outgoing Call Reply message is awaited. If an Incoming or Outgoing Call Reply message is received, an incoming or Outgoing Call Connected message is sent and the session moves to the established state.
waitConnect	This is the state where an Incoming or Outgoing Call Connected message is awaited. If an Incoming or Outgoing Call Connected message is received, the call was successful and the session moves to the established state.
established	Data is exchanged over the tunnel. The session is terminated when receiving or sending a Call Disconnect Notify message. The session then returns to the idle state.

L2TP status - delivery states

The states associated with the packet delivery are:

Value	Description
operating	The Telindus 1420 SHDSL Router has sent a packet, but has not received an acknowledgement on this packet yet.
idle	All transmitted packets have been acknowledged.

L2TP status - authentication states

The states associated with the LNS or LAC authentication are:

Value	Description
noAuthentication	Authentication is not enabled. This is also the start-up state for the authentication process.
authenSuccessful	Authentication was successful. The Telindus 1420 SHDSL Router remains in this state during data transfer.
authenFailure	Authentication failed. This is a transient state since the Telindus 1420 SHDSL Router starts the handshake again after a failing authentication.

9.9 Bridging status attributes

shdslRouter/bridge/bridgeCache

When a port of the bridge enters the learning state, it stores the MAC addresses of the stations situated on the LAN that is connected to this port. The MAC addresses are stored in a MAC address database or bridge cache. The bridgeCache attribute visualises this address database.

The bridgeCache table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>interface</td><td>This is the interface through which the station with the MAC address as displayed in the macAddress element can be reached.</td></tr>
<tr><td>macAddress</td><td>This is the MAC address of a station on the bridged LAN.</td></tr>
<tr><td>type</td><td>This displays whether the corresponding MAC address is static or dynamic:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>dynamic</td><td>The corresponding MAC address is learned on one of the interfaces.</td></tr>
<tr><td>static</td><td>There are only two static entries:
• the Telindus 1420 SHDSL Router its own MAC address
• a MAC address used for Spanning Tree.</td></tr>
</table></td></tr>
<tr><td>age</td><td>This is the elapsed time since a frame was received from the station with the MAC address as displayed in the macAddress element.</td></tr>
</table>

shdslRouter/bridge/spanningTree

This attribute gives you status information on the Spanning Tree.

The spanningTree structure contains the following elements:

Element	Description
designatedPriority	Together, these two elements form the unique bridge identifier. They display the unique bridge identifier of the root bridge as it is indicated in the root identifier parameter of the Configuration BPDUs. These BPDUs are transmitted by the designated bridge for the LAN that is currently connected to this port. This bridge identifier is used to test the value of the root identifier parameter conveyed in received Configuration BPDUs.
designatedMAC	
rootPathCost	This is the cost of the path from this bridge to the root bridge. If this bridge is the root bridge, the rootPathCost value equals 0. Else, the rootPathCost value equals the sum of … • the path cost as it is up to the designated bridge for the LAN that is currently connected to this port (this cost is transmitted in Configuration BPDUs by the designated bridge) and • the path cost as it is configured for the root port. The rootPathCost element is used … • to test the value of the root path cost parameter conveyed in received Configuration BPDUs. • as the value of the root path cost parameter in transmitted Configuration BPDUs. The total cost of the path to the root bridge should not exceed 65500.
rootPort	This is the port identifier of the port that offers the lowest cost path to the root. If two or more ports offer equal least cost paths to the root bridge, then the root port is selected to be that with the highest designatedPriority (i.e. the lowest numerical value). If two or more ports offer equal least cost paths to the root bridge and the same designatedPriority, then the root port is selected to be that with the highest designatedPortPriority (i.e. the lowest numerical value).
bridgePriority	Together, these two attributes form the unique bridge identifier of this bridge.
bridgeMAC	
maxAge	This is the time-out value to be used by all bridges in the bridged LAN for discarding bridging information. The maxAge element displays the value as it is set by the root bridge. This information is conveyed by the root bridge to ensure that each bridge in the bridged LAN has a consistent value against which to test the age of stored configuration information.

Element	Description
helloTime	This is the interval between the generation of Configuration BPDUs by the root bridge. The helloTime element displays the value as it is set by the root bridge. This attribute is not directly used by the Spanning Tree algorithm, but it is conveyed by the root bridge to facilitate the monitoring of protocol performance by the management system.
forwardDelay	This is the time-out value to be used by all bridges in the bridged LAN for … • a bridge port applies to move from listening state to learning state or from learning state to forwarding state. • time-out (or ageing) for purging MAC addresses from the bridge cache in case a topology change is detected. The forwardDelay element displays the value as it is set by the root bridge. This information is conveyed by the root bridge to ensure that each bridge in the bridged LAN has a consistent value for the forward delay timer.
topologyChange	This is a Boolean value (0 or 1) to report … • for a bridge that is not a root bridge, whether or not the most recently accepted Configuration BPDU indicates a change in the active topology. • for the root bridge, whether or not a change in topology has been detected within the preceding topologyChangeTime period. The topologyChange element is used to … • propagate the topology change indication in transmitted Configuration BPDUs. • determine whether the short (bridgeForwardDelay) or long (bridgeTimeOut) time-out (or ageing) value is used to purge dynamic MAC addresses from the bridge cache.
topologyChange-Detection	This is a Boolean value (0 or 1) to report that a topology change has been detected by or notified to the bridge.
topologyChange-Time	This displays the time during which the root bridge transmits Configuration BPDUs indicating a topology change, after it detected this topology change. The topologyChangeTime element value is equal to the sum of the root bridge its bridgeMaxAge element value and bridgeForwardDelay element value. For more information on the latter two elements, refer to the configuration attribute shdslRouter/bridge/spanningTree on page 198.

shdslRouter/bridge/clearBridgeCache

If you execute this action, the bridge cache table is cleared.

9.10 Management status attributes

shdslRouter/management/cms2Address

This attribute displays the absolute device address as you configured it.

shdslRouter/management/loopback/ipAddress

This attribute displays the IP address of the loop-back interface as you configured it.

shdslRouter/management/loopback/ifDescr

This attribute displays the interface description. It is an SNMP MIB2 parameter.

shdslRouter/management/loopback/ifType

This attribute displays the interface type. It is an SNMP MIB2 parameter.

shdslRouter/management/loopback/ifMtu

This attribute displays the interface its Maximum Transfer Unit, i.e. the maximum number of bytes that one packet can contain on this interface. It is an SNMP MIB2 parameter.

shdslRouter/management/loopback/ifOperStatus

This attribute displays the current operation status of the loop-back interface. The loop-back interface is always up.

9.11 Operating system status attributes

shdslRouter/operatingSystem/taskInfo

This attribute displays status information about the operating system.

The taskInfo table contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>taskName</td><td>This is the name of the task.</td></tr>
<tr><td>taskStatus</td><td>This is the current status of the task. Possible values are:
<table><tr><th>Value</th><th>Description</th></tr><tr><td>awake</td><td>This task is actually running.</td></tr><tr><td>asleep</td><td>This task is waiting on an event.</td></tr><tr><td>inactive</td><td>This task slot is not active, i.e. no task has been assigned to this slot.</td></tr></table></td></tr>
<tr><td>load30s (%)</td><td>This is the relative load on the processor during the last 30 seconds.</td></tr>
<tr><td>load5m (%)</td><td>This is the relative load on the processor during the last 5 minutes.</td></tr>
<tr><td>runningInMedium (%)</td><td>Each task can be running with a low, medium or high priority. This element gives the percentage of time this task has been running with medium priority during the last 30 seconds.</td></tr>
<tr><td>runningInHigh (%)</td><td>Each task can be running with a low, medium or high priority. This element gives the percentage of time this task has been running with high priority during the last 30 seconds.
The percentage of time this task has been running with low priority can be calculated using the following formula:
running in low priority = 100% - runningInMedium (%) - runningInHigh (%)</td></tr>
<tr><td>programCounter</td><td>This is the current value of the program counter. The program counter is the memory address for the current instruction of this task.</td></tr>
</table>

10 Performance attributes

This chapter discusses the performance attributes of the Telindus 1420 SHDSL Router. The following gives an overview of this chapter:

10.1 Performance attributes overview

> shdslRouter

>> lanInterface
- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors
- ifOutQLen
- bridgeAccessList
- h2Performance
- h24Performance

>> wanInterface
- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors
- ifOutQLen
- bridgeAccessList
- h2Performance
- h24Performance

>>> frameRelay
- lmi
- dlciTable
- cllmInFrames

>>> line
- h2Line
- h24Line
- d7Line
- line

>>>> linePair [1]
- h2LineParameters
- h2Performance
- h24LineParameters
- h24Performance
- d7LineParameters
- d7Performance
- lineParameters
- performance

>> router
- routingTable
- natSocketsFree
- natAllocFails
- natDiscards
- natAddressesAvailable
- natTcpSocketsUsed
- natUdpSocketsUsed
- natIcmpSocketsUsed
- natTcpAllocs
- natUdpAllocs
- natIcmpAllocs
- pingResults
- Action: startPing
- Action: stopPing
- Action: resetNat

>>> tunnels
- l2tpTunnels

>> bridge
- bridgeCache
- bridgeDiscards
- bridgeFloods

>> management
- cms2SessionCount
- tftpSessionCount
- cliSessionCount
- tcpSessionCount

>> operatingSystem

currUsedProcPower (%)
usedProcPower
freeDataBuffers
totalDataBuffers
largestFreeBlockSize
freeBlockCount
freeMemory
totalMemory
taskInfo

10.2 LAN interface performance attributes

shdslRouter/lanInterface/ifInOctets

This attribute displays the number of octets (bytes) received on this interface.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifInUcastPkts

This attribute displays the number of unicast packets received on this interface and delivered to a higher-layer protocol. Unicast packets are all non-multicast and non-broadcast packets.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifInNUcastPkts

This attribute displays the number of non-unicast packets received on this interface and delivered to a higher-layer protocol. Non-unicast packets are all the multicast and broadcast packets.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifInDiscards

This attribute displays the number of incoming packets that were discarded, to prevent their deliverance to a higher-layer protocol. This even though no errors were detected in these packets.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifInErrors

This attribute displays the number of incoming packets that could not be delivered to a higher-layer protocol because they contained errors.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifInUnknownProtos

This attribute displays the number of incoming packets that were discarded because they contained an unknown or unsupported protocol.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifOutOctets

This attribute displays the total number of octets (bytes) transmitted by the interface, including framing characters.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifOutUcastPkts

This attribute displays the total number of packets that higher-level protocols requested to be transmitted to a unicast address, including those that were discarded or not sent.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifOutNUcastPkts

This attribute displays the number of non-unicast packets that higher-level protocols requested to be transmitted to a non-unicast (i.e. a broadcast or multicast) address, including those that were discarded or not sent.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifOutDiscards

This attribute displays the number of outgoing packets that were discarded, to prevent they are transmitted by the interface. This could be due to, for instance, the presence of an access list.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifOutErrors

This attribute displays the number of outgoing packets that could not be transmitted by the interface because they contained errors.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/ifOutQLen

This attribute displays the length of the output packet queue, expressed in packets, on the interface.

This is an SNMP MIB2 parameter.

shdslRouter/lanInterface/bridgeAccessList

This attribute shows information on the use of the bridge access list.

The bridgeAccessList table contains the following elements:

Element	Description
macAddress	This is the MAC address as configured in the configuration attribute bridgeAccessList.
uses	This indicates the number of times a packet has been discarded because of the specific MAC address entry in the access list.

shdslRouter/lanInterface/h2Performance

This attribute displays the 2 hours performance summary of the LAN interface.

The h2Performance table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
ifUpTime	the time during which the interface was up.
ifStatusChanges	the amount of times the ifOperStatus value of the interface has changed (from up to down or vice versa).
ifInOctets	the number of octets (bytes) received on this interface.
ifInPackets	the number of packets received on this interface.
ifInErrors	the number of packets received on this interface that could not be delivered to a higher-layer protocol because they contained errors.
ifOutOctets	the number of octets (bytes) transmitted by the interface, including framing characters.
ifOutPackets	number of packets transmitted by the interface.
ifOutDiscards	the number of outgoing packets that were discarded, to prevent they were transmitted by the interface. This could be due to, for instance, the presence of an access list.
ifOutErrors	the number of packets that could not be transmitted by the interface because they contained errors.

shdslRouter/lanInterface/h24Performance

This attribute displays the 24 hours performance summary of the LAN interface. The h24Performance table contains the same elements as the shdslRouter/lanInterface/h2Performance table.

10.3 WAN interface performance attributes

The WAN interface performance attributes are the same as the LAN interface performance attributes. For a complete description of these attributes, refer to 10.2 - LAN interface performance attributes on page 252.

10.4 WAN encapsulation performance attributes

shdslRouter/wanInterface/frameRelay/lmi

This attribute gives a complete LMI performance overview.

The lmi structure contains the following elements:

Element	Description
inStatusEnquiry	This is the number of Status Enquiries received from the network.
inStatus	This is the number of Status Reports received from the network.
inStatusUpdate	This is the number of unsolicited Status Updates received from the network.
outStatusEnquiry	This is the number of Status Enquiries sent to the network.
outStatus	This is the number of Status Reports sent to the network.
outStatusUpdate	This is the number of unsolicited Status Updates sent to the network.
netPollNotRcvd	This is the number of times the expectedPollInterval expired without an incoming status enquiry.
userNoResponse-Rcvd	This is the number of times a response was not received.
userBadResponses-Rcvd	This is the number of times an invalid response was received.

shdslRouter/wanInterface/frameRelay/dlciTable

This attribute lists the complete performance information of all known DLCIs.

The dlciTable table contains the following elements:

Element	Description
dlci	This is the DLCI identification number.
inFecn	This is the number of frames received from the network indicating forward congestion and this since the virtual circuit was created.
inBecn	This is the number of frames received from the network indicating backward congestion and this since the virtual circuit was created.
inDe	This is the number of frames received with the Discard Eligibility bit set
inOctets	This is the number of octets received over this virtual circuit since it was created.
inFrames	This is the number of frames received over this virtual circuit since it was created.
outFecn	This is the number of frames sent to the network indicating forward congestion and this since the virtual circuit was created.
outBecn	This is the number of frames sent to the network indicating backward congestion and this since the virtual circuit was created.
outDe	This is the number of frames sent to the network with the Discard Eligibility bit set.
outOctets	This is the number of octets sent over this virtual circuit since it was created.
outFrames	This is the number of frames sent over this virtual circuit since it was created.

shdslRouter/wanInterface/frameRelay/cllmInFrames

This attribute displays the total number of received CLLM frames.

10.5 Line performance attributes

shdslRouter/wanInterface/line/h2Line

This attribute displays the 2 hours information summary of the line.

The h2Line table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
linkDownCount	the number of times the link went down.
linkDownTime	the total amount of time the link was down.

shdslRouter/wanInterface/line/h24Line

This attribute displays the 24 hours information summary of the line. The h24Line table contains the same elements as the shdslRouter/wanInterface/line/h2Line table.

shdslRouter/wanInterface/line/d7Line

This attribute displays the 7 days information summary of the line. The d7Line table contains the same elements as the shdslRouter/wanInterface/line/h2Line table.

shdslRouter/wanInterface/line/line

This attribute displays the line information summary of the line since the last cold boot. Except for the sysUpTime, the line structure contains the same elements as the shdslRouter/wanInterface/line/h2Line table.

shdslRouter/wanInterface/line/linePair [1]/h2LineParameters

This attribute displays the 2 hours parameter summary of the line.

The h2LineParameters table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
lineAttenuationMin (dB)	the minimum line attenuation that was measured.
lineAttenuationAvrg (dB)	the average line attenuation that was calculated
lineAttenuationMax (dB)	the maximum line attenuation that was measured.
noiseMarginMin (dB)	the minimum noise margin that was measured.
noiseMarginAvrg (dB)	the average noise margin that was calculated.
noiseMarginMax (dB)	the maximum noise margin that was measured.

shdslRouter/wanInterface/line/linePair [1]/h2Performance

This attribute displays the 2 hours performance summary of the line.

The h2Performance table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
codeViolations	the number of line errors that was counted.
erroredSeconds	the number of erroneous seconds that was counted.
sevErroredSeconds	the number of severely erroneous seconds that was counted.
unavailableSeconds	the number of unavailable seconds that was counted.
loswSeconds	the number of lost synchronisation words that was counted.

For the correct and unambiguous definition of code violations, errored and severely errored seconds, unavailability and lost sync words, refer to the recommendation G.826.

shdslRouter/wanInterface/line/linePair [1]/h24LineParameters

This attribute displays the 24 hours parameter summary of the line. The h24LineParameters table contains the same elements as the shdslRouter/wanInterface/line/linePair [1]/h2LineParameters table.

shdslRouter/wanInterface/line/linePair [1]/h24Performance

This attribute displays the 24 hours performance summary of the line. The h24Performance table contains the same elements as the shdslRouter/wanInterface/line/linePair [1]/h2Performance table.

shdslRouter/wanInterface/line/linePair [1]/d7LineParameters

This attribute displays the 7 days parameter summary of the line. The d7LineParameters table contains the same elements as the shdslRouter/wanInterface/line/linePair [1]/h2LineParameters table.

shdslRouter/wanInterface/line/linePair [1]/d7Performance

This attribute displays the 7 days performance summary of the line. The d7Performance table contains the same elements as the shdslRouter/wanInterface/line/linePair [1]/h2Performance table.

shdslRouter/wanInterface/line/linePair [1]/lineParameters

This attribute displays the parameter summary of the line since the last cold boot. Except for the sysUpTime, the lineParameters table contains the same elements as the shdslRouter/wanInterface/line/linePair [1]/h2LineParameters table.

shdslRouter/wanInterface/line/linePair [1]/performance

This attribute displays the performance summary of the line since the last cold boot. Except for the sysUpTime, the performance table contains the same elements as the shdslRouter/wanInterface/line/linePair [1]/h2Performance table.

10.6 Routing performance attributes

shdslRouter/router/routingTable

This attribute lists all known routes and how many times they are used.

The routingTable contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>network</td><td>This is the IP address of the destination network.</td></tr>
<tr><td>mask</td><td>This is the network mask of the destination network.</td></tr>
<tr><td>gateway</td><td>This is the IP address of the next router on the path to the destination network.</td></tr>
<tr><td>interface</td><td>This is the interface through which the destination network can be reached. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>internal</td><td>The own protocol stack is used.</td></tr>
<tr><td>lan</td><td>The destination network can be reached through the Ethernet interface.</td></tr>
<tr><td>wan</td><td>The destination network can be reached through the serial interface.</td></tr>
<tr><td>discard</td><td>Packets for this destination are discarded.</td></tr>
</table></td></tr>
<tr><td>uses</td><td>This lists how many times the route has been used since it is listed in the routing table.
For each IP packet that matches this route, the attribute value is incremented by one. RIP routes may disappear from the routing table, and re-appear afterwards. The attribute value is reset when a RIP route disappears from the routing table.</td></tr>
</table>

shdslRouter/router/natSocketsFree

This attribute shows the remaining number of new connections (i.e. sockets) that can be initiated. A socket is a set of source and destination IP addresses and port numbers.

Initially, 2048 simultaneous sockets can be initiated. Sockets are freed using a garbage mechanism. This means that every five minutes all sockets are checked. If a socket has been released by PAT or NAT, then this socket is returned to the pool of free sockets.

ICMP and UDP sockets are released when they have no data traffic during five minutes. TCP sockets are released after the TCP session has been closed or when the session has been idle for 24 hours.

shdslRouter/router/natAllocFails

If no sockets are available anymore but an attempt to set up a new connection is being made, then the natAllocFails attribute value is incremented by 1.

Because the sockets are distributed using a hashing function, it is possible that natAllocFails increases even though natSocketsFree still indicates free sockets.

ICMP requires a new socket for each transmitted packet. This implies that, for instance, a permanent ping or trace-route command may eventually use all free sockets.

shdslRouter/router/natDiscards

This attribute indicates how many times a packet has been discarded for reasons other than a lack of free sockets. This could be, for instance, because an attempt was made to connect from the Internet to a service that was not present in the servicesAvailable table.

shdslRouter/router/natAddressesAvailable

This attribute displays the number of NAT addresses that are currently free.

shdslRouter/router/natTcpSocketsUsed

This attribute displays the number of sockets currently in use by PAT and NAT for TCP applications.

shdslRouter/router/natUdpSocketsUsed

This attribute displays the number of sockets currently in use by PAT and NAT for UDP applications.

shdslRouter/router/natIcmpSocketsUsed

This attribute displays the number of sockets currently in use by PAT and NAT for ICMP applications.

shdslRouter/router/natTcpAllocs

This attribute indicates how many TCP sockets have been allocated since cold boot. Together with the performance attributes natUdpAllocs and natIcmpAllocs it gives an indication of the type of traffic that is being routed.

shdslRouter/router/natUdpAllocs

This attribute indicates how many UDP sockets have been allocated since cold boot. Together with the performance attributes natTcpAllocs and natIcmpAllocs it gives an indication of the type of traffic that is being routed.

shdslRouter/router/natIcmpAllocs

This attribute indicates how many ICMP sockets have been allocated since cold boot. Together with the performance attributes natTcpAllocs and natUdpAllocs it gives an indication of the type of traffic that is being routed.

shdslRouter/router/pingResults

It is possible to send a ping to a distant IP address (only one ping at a time). You can start and stop pinging with the ping actions startPing and stopPing. The pingResults attribute lists the results of the transmitted ping.

The routingTable contains the following elements:

Element	Description
ipAddress	This is the IP address being pinged.
nbrOfTxPackets	This is the number of transmitted pings.
nbrOfRxPackets	This is the number of correct received answers on the transmitted pings.
minReplyTime	This is the lowest reply time of all correct received answers.
maxReplyTime	This is the highest reply time of all correct received answers.
avrgReplyTime	This is the average reply time of all correct received answers.

shdslRouter/router/startPing

Execute this actions to start transmitting pings to an IP address. Several arguments can be set:

Argument	Description
ipAddress	This is the IP address you want to ping. Default:0.0.0.0 Range: up to 255.255.255.255
iterations	This is the number of pings. Default:5 Range: 0 … If you enter 0, the IP address will be pinged an indefinite number of times. The only way to stop the ping session is by executing the stopPing action.
interval	This is the interval, in seconds, between consecutive pings. Default:1 Range: 0 … 100
dataLength	This is the length of the data transmitted in a ping. Default:31 Range: 0 … 1300
timeOut	If a ping is sent, the system will wait for a certain period on the answer. I.e. the system expects the answer within this period. Use the timeOut argument to set this period. Default:00000d 00h 00m 05s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

shdslRouter/router/stopPing

Stops the pending pings.

shdslRouter/router/resetNAT

Use this action to release all sockets currently in use and return them to the free socket pool.

In other words, executing this action resets all NAT/PAT sessions that are currently established. It also releases all official IP addresses that are dynamically assigned to a private IP address. If any TCP sessions are still active, these sessions will be aborted.

Take care when using this action! All TCP information is lost when the sockets are released with this action. Any TCP sessions in use at the time of the reset will go into a hang-up state. These applications will need to restart.

10.7 L2TP tunnel performance attributes

shdslRouter/router/tunnels/l2tpTunnels

This attribute gives you performance information on the L2TP tunnels.

The l2tpTunnels table contains the following elements:

Element	Description
name	This is the name of the tunnel as you defined it in the l2tpTunnels configuration attribute.
mibCounters	This structure displays the following SNMP MIB2 parameters of the L2TP tunnels: ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifInDiscards, ifInErrors, ifInUnknownProtos, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifOutErrors, ifOutQLen. For more information on these performance attributes, refer to 10.2 - LAN interface performance attributes on page 252.

10.8 Bridging performance attributes

shdslRouter/bridge/bridgeCache

When a port of the bridge enters the learning state, it stores the MAC addresses of the stations situated on the LAN that is connected to this port. The MAC addresses are stored in a MAC address database or bridge cache. The bridgeCache attribute visualises this address database.

The bridgeCache table contains the following elements:

Element	Description
interface	This is the interface through which the station with the MAC address as displayed in the macAddress element can be reached.
macAddress	This is the MAC address of a station on the bridged LAN.
rxCount	This is the number of frames received from the corresponding MAC address.
txCount	This is the number of frames forwarded to the corresponding MAC address.

shdslRouter/bridge/bridgeDiscards

This attribute displays the number of times a frame was discarded because …

- it was received on the same interface as the one through which the destination address can be reached.
- it was received on an interface that is not in the forwarding state.

shdslRouter/bridge/bridgeFloods

This attribute displays the number of times a frame was flooded on all interfaces because …

- it was a broadcast / multicast.
- the position of the station with the destination MAC address was not known.

10.9 Management performance attributes

shdslRouter/management/cms2SessionCount

This attribute displays the number of CMS2 sessions that are currently active on the Telindus 1420 SHDSL Router.

There are always minimum two fixed sessions active. Connecting with TMA, TMA CLI, Telnet, etc. opens additional sessions. This is explained in the following table:

Session count	Purpose
1 fixed session	A fixed session for SNMP.
1 fixed session	A fixed session for O10.
+ 2 sessions	When connecting with TMA.
+ 1 session	When connecting with TMA for HP OpenView or the Alarm Manager.
+ 1 session	When connecting with TMA CLI.
+ 2 sessions	When downloading a config.cli or config.cms file.
+ 1 session	When connecting with Telnet.
+ 1 session	When downloading firmware.
+ 1 session	When connecting with the Web Interface.

shdslRouter/management/tftpSessionCount

This attribute displays the number of TFTP sessions that are currently active on the Telindus 1420 SHDSL Router.

shdslRouter/management/cliSessionCount

This attribute displays the number of CLI sessions that are currently active on the Telindus 1420 SHDSL Router.

There are always minimum two fixed sessions active. Connecting with TMA CLI, the Web Interface, etc. opens additional sessions. This is explained in the following table:

Session count	Purpose
1 fixed session	A fixed session for the auxiliary (control) port.
1 fixed session	A fixed session for Web Interface.
+ 1 session	When connecting with TMA CLI or starting a CLI session.
+ 1 session	When connecting with the Web Interface.

shdslRouter/management/tcpSessionCount

This attribute displays the number of TCP sessions that are currently active on the Telindus 1420 SHDSL Router. The following table shows when a TCP session opens:

Session count	Purpose
+ 1 session	When connecting with Telnet.
+ 1 session	When connecting with the Web Interface.

10.10 Operating system performance attributes

shdslRouter/operatingSystem/currUsedProcPower (%)

This attribute displays the amount of processing power used during the last 650 milliseconds, expressed as a percentage of the total available processing power.

shdslRouter/operatingSystem/usedProcPower

This attribute lists the used processing power for the 11 most recent 30 seconds intervals. The processing power is expressed as a percentage of the total processing power.

The usedProcPower table contains the following elements:

Element	Description
sysUpTime	This is the elapsed time since the last cold boot. The next values are for the 30 seconds period before this relative time stamp.
min (%)	This is the minimum percentage of processing power in use during the last 30 seconds.
average (%)	This is the average percentage of processing power in use during the last 30 seconds.
max (%)	is the maximum percentage of processing power in use during the last 30 seconds.

shdslRouter/operatingSystem/freeDataBuffers

The processor uses buffers for storing the packets during processing and/or queuing. Each buffer has a 256 byte size, headers included. This attribute is the number of data buffers currently not in use and available for e.g. incoming data.

shdslRouter/operatingSystem/totalDataBuffers

This attribute displays the total number of available data buffers.

shdslRouter/operatingSystem/largestFreeBlockSize

The processor uses RAM memory for storing internal information and buffering. The different tasks allocate RAM memory on request. Tasks may also free memory again. In this way the total RAM memory becomes fragmented. This attribute gives the size of the largest contiguous free memory block expressed in bytes.

shdslRouter/operatingSystem/freeBlockCount

This attribute displays the number of free contiguous memory blocks.

shdslRouter/operatingSystem/freeMemory

This attribute displays the total free memory expressed in bytes.

shdslRouter/operatingSystem/totalMemory

This attribute displays the total RAM memory expressed in bytes.

shdslRouter/operatingSystem/taskInfo

This attribute contains status information concerning the different tasks running on the processor. It is a table grouping up to 31 task slots, which is the maximum number of parallel tasks running on the processor's operating system.

This attribute contains the same elements as the status attribute shdslRouter/operatingSystem/taskInfo on page 247.

11 Alarm attributes

This chapter discusses the alarm attributes of the Telindus 1420 SHDSL Router. The following gives an overview of this chapter:

11.1 Alarm attributes overview

> shdslRouter
- totalAlarmLevel
- alarmInfo
  - notResponding
  - alarmSyncLoss
  - configChanged
  - access
  - unknownState
  - coldBoot
  - warmBoot
  - codeConsistencyFail
  - configConsistencyFail

>> lanInterface
- alarmInfo
  - linkDown

>> wanInterface
- alarmInfo
  - linkDown

>>> line
- alarmInfo
  - linkDown

>> router
- alarmInfo
  - pingActive

11.2 Introducing the alarm attributes

Before discussing the alarm attributes of the Telindus 1420 SHDSL Router in detail, some general information on the alarm attributes of the Telindus 1420 SHDSL Router is given.

The following gives an overview of this chapter:

11.2.1 Configuration alarm attributes

shdslRouter/.../alarmMask

Use this attribute to enable or disable for each alarm of the corresponding object, whether it is communicated to the central management system (e.g. HP OpenView) or not.

Alarms are always seen in the alarmInfo alarm attribute of an object, regardless of the masking of the alarm. I.e. even if an alarm is set to disabled in the alarmMask of an object, if the alarm condition is fulfilled then the alarm will be set to on in the alarmInfo of that object. However, because this alarm is disabled:

- it will not be sent to the central management system (e.g. HP OpenView).
- it will not be shifted towards the previousAlarms element of the alarmInfo attribute (refer to the alarm attribute shdslRouter/.../alarmInfo on page 277).

shdslRouter/.../alarmLevel

Use this attribute to assign a priority level to each alarm of the corresponding object. The alarm level range goes from 0 to 254, where 0 is the lowest and 254 is the highest priority level.

The alarmLevel of an unmasked, active alarm is sent to the totalAlarmLevel alarm attribute of the top object shdslRouter.

11.2.2 General alarm attributes

shdslRouter/totalAlarmLevel

This attribute is only present in the top object of the containment tree of the Telindus 1420 SHDSL Router, being shdslRouter.

It displays the priority level of an unmasked, active alarm. When several alarms are generated at the same time, the highest priority level is shown. If the alarm levels are set in a structured manner, one look at the totalAlarmLevel attribute enables the operator to make a quick estimation of the problem.

The value of the totalAlarmLevel attribute is also communicated to the central management system (e.g. HP OpenView) where it determines the colour of the icon. This colour is an indication of the severity of the alarm.

shdslRouter/…/alarmInfo

This attribute contains the actual alarm information of the corresponding object.

The alarmInfo structure contains the following elements:

Element	This element displays for the corresponding object …
discriminator	the total alarm count since the last cold boot.
currentAlarms	the current alarms.
previousAlarms	the second most recent alarms.
alarmMask	the alarmMask as you configured it.
alarmLevel	the alarmLevel as you configured it.

11.3 General alarms

For general information on the alarm attributes, refer to 11.2 - Introducing the alarm attributes on page 275.

shdslRouter/alarmInfo

The different alarms related to the shdslRouter object together with their explanation and default alarmMask and alarmLevel value are given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	**alarmLevel**
notResponding	by the Alarm Manager (TMA for HP OpenView) when the Telindus 1420 SHDSL Router does not respond on its polling session.	enabled	4
alarmSyncLoss	when the internal alarm buffer overflows.	enabled	4
configChanged	when the local configuration has been changed.	disabled	1
access	when a management session is active. This alarm is not activated when connecting via one of the ports of the Orchid 1003 LAN.	disabled	1
unknownState	- For future purposes. -	disabled	0
coldBoot	each time the Telindus 1420 SHDSL Router performs a cold boot.	disabled	1
warmBoot	each time the Telindus 1420 SHDSL Router performs a warm boot.	disabled	1
codeConsistency-Fail	- For future purposes. -	disabled	1
configConsistency-Fail	- For future purposes. -	disabled	1

11.4 LAN interface alarms

For general information on the alarm attributes, refer to 11.2 - Introducing the alarm attributes on page 275.

shdslRouter/lanInterface/alarmInfo

The alarms related to the lanInterface object together with their explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	**alarmLevel**
linkDown	when no valid LAN data is detected. I.e. when the connection between the interface and the LAN is down.	enabled	3

11.5 WAN interface alarms

For general information on the alarm attributes, refer to 11.2 - Introducing the alarm attributes on page 275.

shdslRouter/wanInterface/alarmInfo

The alarms related to the wanInterface object together with their explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	**alarmLevel**
linkDown	when an error situation is detected in the encapsulation protocol (Frame Relay, PPP, X.25 or HDLC). For instance, an error condition in the Frame Relay LMI, a failed authentication in PPP, …	enabled	3

11.6 Line alarms

For general information on the alarm attributes, refer to 11.2 - Introducing the alarm attributes on page 275.

shdslRouter/wanInterface/line/alarmInfo

The alarms related to the line object together with their explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	**alarmLevel**
linkDown	when the line is down. I.e. no data can be transmitted over the line.	enabled	3

11.7 Routing alarms

For general information on the alarm attributes, refer to 11.2 - Introducing the alarm attributes on page 275.

shdslRouter/router/alarmInfo

The alarms related to the router object together with their explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	**alarmLevel**
pingActive	in case of a pending ping (for example, an indefinite ping). This notification is necessary because you can only transmit one ping at a time. Furthermore, there is no protection when a new ping is started before the previous is stopped.	enabled	3

12 TMA sub-system picture

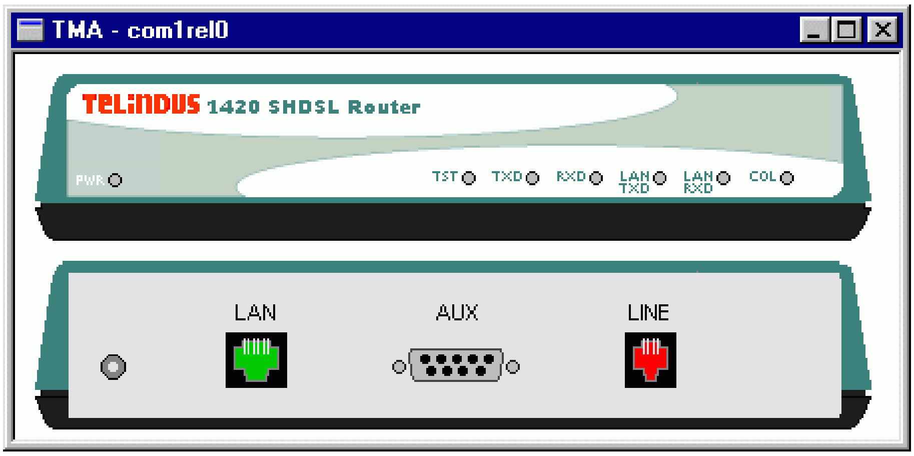
The sub-system picture is a TMA tool that visualises the status information of the Telindus 1420 SHDSL Router. This chapter explains how to display the sub-system picture, and how to interpret the visual indications.

How to display the sub-system picture?

To display the sub-system picture of the Telindus 1420 SHDSL Router, click on the sub-system picture button located in the TMA toolbar: .

Structure of the sub-system picture

This paragraph displays and labels the different elements of the sub-system picture. It also explains how the visual indications should be interpreted. Below, the Telindus 1420 SHDSL Router sub-system picture is displayed:



The following table gives an overview of the sub-system picture elements and what they indicate:

Element	Description
LED indicators	These reflect the actual status of the device. The LED indication on the sub-system picture corresponds with the LED indication on the Telindus 1420 SHDSL Router itself. For more information on the interpretation of the LEDs, refer to 2.6 - The front panel LED indicators on page 26.
interfaces	This reflects the status of the interfaces. The possible indications are: <table><tr><th>Colour</th><th>Explanation</th></tr><tr><td>green</td><td>There is no alarm active in the corresponding interface object.</td></tr><tr><td>red</td><td>An alarm is active in the corresponding interface object.</td></tr></table>The colours of the interfaces only change if the alarms related to the interface object are set to *enabled* in the alarmMask.

13 Auto installing the Telindus 1420 SHDSL Router

Auto install includes a number of features that allow you to partially or completely configure the Telindus 1420 SHDSL Router without on-site intervention. This can be particularly useful since the Telindus 1420 SHDSL Router is located at the edge of the access network. Its configuration can be retrieved over the WAN from a central server.

Auto install is made possible by using a number of standardised protocols as there are BootP, DHCP, TFTP and Frame Relay LMI.

The following gives an overview of this chapter:

13.1 What is BootP and DHCP?

BootP and DHCP are very similar protocols. IP devices without IP address use them to obtain an IP address.

Compliance:

- BootP complies with RFC 951.
- DHCP complies with RFCs 2131 and 2132.

In both protocols, the client IP device sends a limited broadcast request on its interfaces requesting an IP address. The request contains the client its MAC address, which is a unique identifier (refer to the status attribute shdslRouter/lanInterface/macAddress).

BootP

A workstation with a BootP server interprets incoming BootP requests. You can configure a file on the server with MAC address and IP address/subnet mask pairs for all devices in the network you want to service. If the MAC address in the BootP request matches a MAC address in this file, the BootP server replies with the corresponding IP address and subnet mask.

Assigning an IP address in this way is done through a simple request - response handshake.

The Telindus 1420 SHDSL Router, being a router, always requests a static IP address.

DHCP

A workstation with a DHCP server works in a similar way as with a BootP server. The difference with BootP is that you can additionally configure a list of IP addresses on the server. These IP addresses are dynamically assigned to the IP devices requesting an IP address, independently of their MAC address. Those address assignments are limited in time.

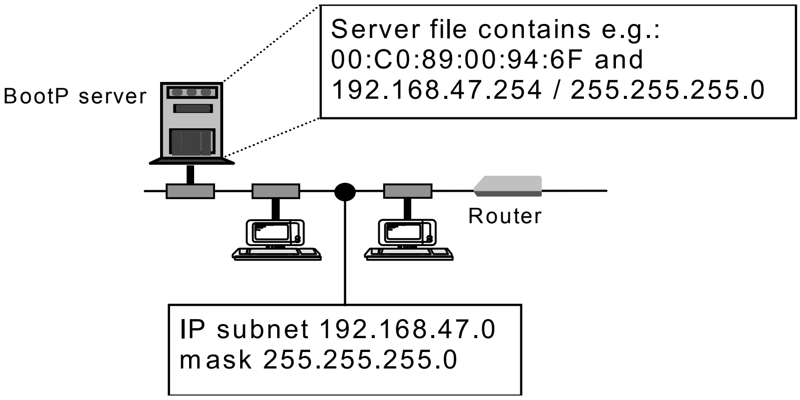
Assigning an IP address in this way is done through a 4-way handshake and with regular renewals.

The Telindus 1420 SHDSL Router as relay agent

Being broadcast packets, BootP and DHCP requests can cross a router using IP helper addresses. The Telindus 1420 SHDSL Router is a BootP and DHCP relay agent. This means it adds additional information to the request packets allowing servers on distant networks to send back the answer. This feature is not used in the auto install procedure.

13.2 Getting the IP address over the LAN interface

The following figure shows how the Telindus 1420 SHDSL Router obtains its LAN IP address from a BootP server on its Ethernet interface:



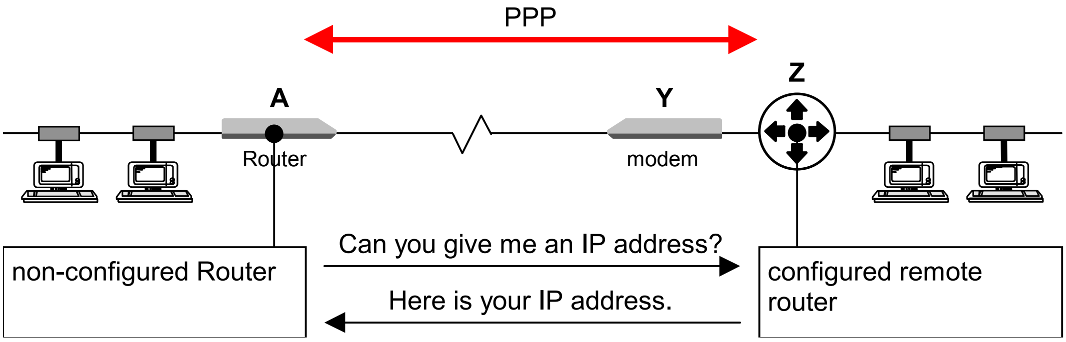
The IP address is obtained as follows:

Phase	Description
1	In case on the LAN interface no ipAddress or ipNetMask is configured (i.e. still at their default value), then the Telindus 1420 SHDSL Router starts sending BootP requests containing its MAC address on the LAN interface every 10 seconds.
2	The BootP server looks in its MAC address - IP address file. If the MAC address in the BootP request matches a MAC address in this file, the BootP server replies with the corresponding IP address and subnet mask. **Example** In the example above, the Telindus 1420 SHDSL Router its MAC address is 00:C0:89:00:94:6F. The server replies with IP address 192.168.47.254 and corresponding subnet mask 255.255.255.0.
3	The Telindus 1420 SHDSL Router uses this received IP address as its LAN IP address. However, it does not store it in non-volatile memory.

13.3 Getting the IP address over a PPP WAN link

The figure below shows the following set-up:

- a Telindus 1420 SHDSL Router (A) is connected over a line to modem (Y),
- modem (Y) its serial interface is connected to a remote router (Z) (alternatively, modem (Y) and the remote router (Z) can be replaced by another Telindus 1420 SHDSL Router),
- the protocol used between the two routers is PPP.



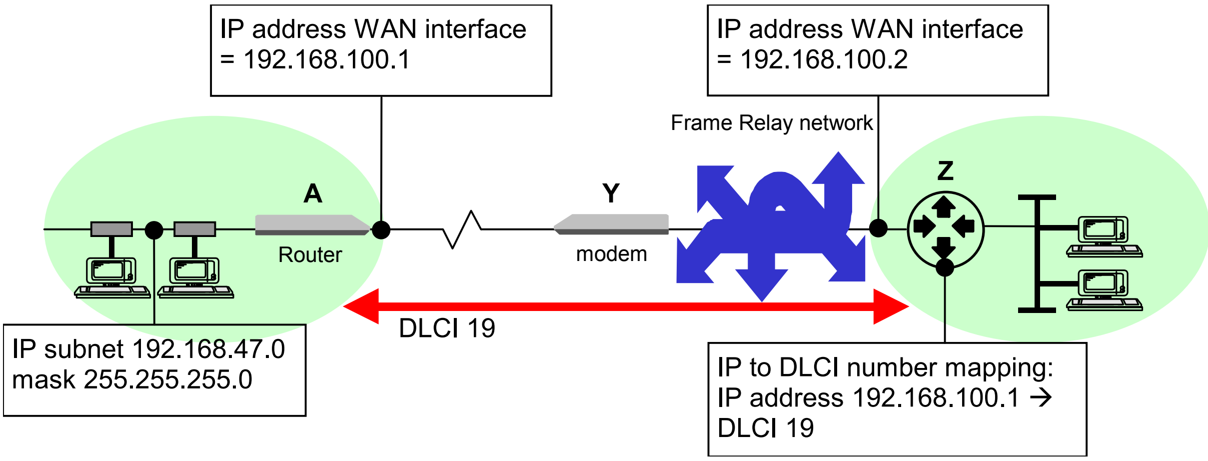
The IP address is obtained as follows:

Phase	Description
1	In case … • on the WAN interface no ipAddress is configured (i.e. still at its default value), AND • the configuration attribute autoInstallMode is set to … - unnumbered and on the LAN interface no ipAddress or ipNetMask is configured (i.e. still at their default value), OR - any other value, … then the Telindus 1420 SHDSL Router (A) requests an IP address during the IPCP handshake.
2	• If the remote router (Z) supports the IPCP option *IP address*, then it sends an IP address to the Telindus 1420 SHDSL Router (A). • If the remote router (Z) is also a Telindus 1420 SHDSL Router, then it looks in its routing table and replies with the gateway address of the first route which passes the WAN interface.
3	The Telindus 1420 SHDSL Router uses this received IP address as its WAN IP address. Possibly, it also uses this as its LAN IP address depending on the setting of the autoInstallMode configuration attribute (refer to shdslRouter/wanInterface/autoInstallMode on page 160). The IP address is assigned to both interfaces since the Telindus 1420 SHDSL Router can operate with a numbered or unnumbered WAN interface. However, it does not store the IP address in non-volatile memory.

13.4 Getting the IP address over a Frame Relay WAN link

The figure below shows the following set-up:

- a Telindus 1420 SHDSL Router (A) is connected over a line to modem (Y),
- modem (Y) is connected to a Frame Relay network,
- the Frame Relay network terminates in a central router (Z) (this can be e.g. a Cisco router or another Telindus router),
- suppose the central router (Z) belongs to an ISP,
- suppose the Telindus 1420 SHDSL Router (A) belongs to a customer.



The IP address is obtained as follows:

Phase	Description
1	The ISP asks the Frame Relay service provider to set up a Permanent Virtual Circuit (PVC) to the customer. This means a complete path is set up between the ISP and the customer. To this path, a DLCI number is assigned in the Frame Relay node closest to modem (Y). In the example above, this DLCI number is 19.
2	The Telindus 1420 SHDSL Router (A) learns this DLCI number from the Frame Relay node closest to modem (Y) through LMI PVC status inquiries.
3	In case … • on the WAN interface no ipAddress is configured (i.e. still at its default value), AND • the configuration attribute autoInstallMode is set to … - unnumbered and on the LAN interface no ipAddress or ipNetMask is configured (i.e. still at their default value), OR - any other value, … then the Telindus 1420 SHDSL Router (A) starts sending BootP requests on the Frame Relay DLCI.

Phase	Description
4	The central router (Z) answers these requests, acting as a BootP server. The answer is based on its static IP address to DLCI mapping. The central router (Z) looks for the IP address that maps the DLCI number where the BootP request was received. It sends this IP address back as the IP address for the Telindus 1420 SHDSL Router (A). This implementation is compatible with another Telindus 1420 SHDSL Router or a Cisco router starting from IOS 10.3 as central router. The Cisco router, however, must have an IP helper address on its WAN interface before it will reply.
5	The Telindus 1420 SHDSL Router uses this received IP address as its WAN IP address. Possibly, it also uses this as its LAN IP address depending on the setting of the autoInstall-Mode configuration attribute (refer to shdslRouter/wanInterface/autoInstallMode on page 160). The IP address is assigned to both interfaces since the Telindus 1420 SHDSL Router can operate with a numbered or unnumbered WAN interface. However, it does not store the IP address in non-volatile memory.

13.5 Getting the configuration with TFTP

Once the Telindus 1420 SHDSL Router has obtained an IP address, it is reachable over …

- its LAN interface in case it received a LAN IP address from a BootP server on the local LAN.
- its WAN interface in case it received a WAN IP address via the PPP or Frame Relay link.

Now you can start a TMA or a Telnet session on the Telindus 1420 SHDSL Router and configure it.

Alternatively the Telindus 1420 SHDSL Router can retrieve its complete configuration without any user intervention. As long as the previously obtained IP addresses are not stored in non-volatile memory, the Telindus 1420 SHDSL Router tries to get a complete configuration file from a TFTP server.

The configuration file and TFTP

The Trivial File Transfer Protocol is typically used in combination with BootP to obtain the configuration of a device from a TFTP server. The configuration file on this TFTP can be in a binary or an ASCII format. How to build such files is explained in 13.6 - Creating configuration files on page 294.

Getting the configuration file with TFTP

The Telindus 1420 SHDSL Router asks for its configuration file as follows:

Phase	Description
1	The Telindus 1420 SHDSL Router sends a DNS request on the interface for which it received an IP address. This request is a local broadcast message.
	If it sent over the WAN link, the peer router should have an IP helper address for the DNS server.
	If no reply is received within 10 seconds, this phase is repeated once more.
2	If a DNS reply is received, it contains the domain name. The Telindus 1420 SHDSL Router only uses the hostname part of the domain name: *host-name.domain.toplevel_domain*.

<table>
<tr><th>Phase</th><th>Description</th></tr>
<tr><td>3</td><td>Now there are two possibilities:
<table>
<tr><th>If the host name is …</th><th>then …</th></tr>
<tr><td>known,</td><td>the router requests the file hostname.cms as a limited broadcast. hostname.cms is the router its configuration file in binary format.

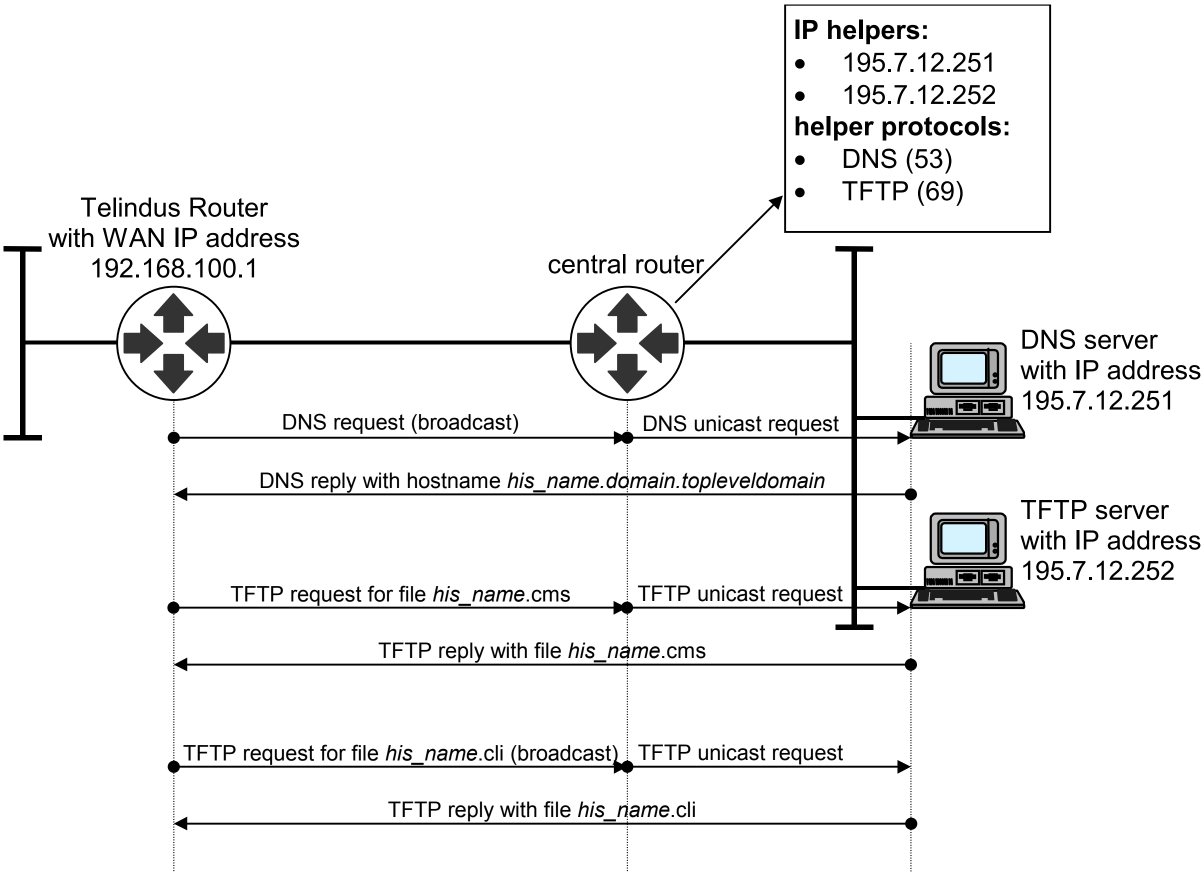
If this request is sent over the WAN link, the peer router should have an IP helper address for the TFTP server.

If no reply is received within 5 seconds, the router requests the file hostname.cli as a local broadcast. hostname.cli is the router its configuration file in ASCII format. Again there is a reply time-out of 5 seconds.

If still no valid answer is received, the router alternatively repeats both requests up to four times.</td></tr>
<tr><td>not known,</td><td>the procedure described above is executed with the file name hostname replaced by the concatenation of the decimal representation for each byte in the IP address, with leading zeroes and without dots in between the bytes.

Example, a router with IP address 192.168.100.1 requests the file 192168100001.cms or 192168100001.cli.</td></tr>
</table></td></tr>
<tr><td>4</td><td>If the Telindus 1420 SHDSL Router received a valid configuration file, then it stores the configuration and possibly reboots. Else it restarts with phase 1.</td></tr>
</table>

The following figure illustrates the procedure as described in the table above. It shows the procedure over a WAN link. The IP address of the router is 192.168.100.1 and its hostname is *his_name*. In this example, the DNS server and TFTP server are on different machines. However, in reality these two services often reside on the same machine.



13.6 Creating configuration files

In 13.5 - Getting the configuration with TFTP on page 291, you have seen how you can get a configuration file with TFTP. This section explains how to create such configuration files. First, it explains the two different configuration file formats.

The following table gives an overview of this section.

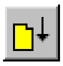
13.6.1 Configuration file formats

The two possible configuration file formats used by TFTP are:

File type	Extension	How to create the configuration file
binary	.cms	Use the TMA export utility and choose the CMS file type. This is the most compact format.
ASCII	.cli	Use the CLI user interface. When you download an ASCII (*.cli) configuration file to the Telindus 1420 SHDSL Router, make sure that each line in this file contains no more than 500 characters.

13.6.2 Creating a binary configuration file

To create a configuration file in binary (*.cms) format, proceed as follows:

Step	Action
1	Start a TMA session on the Telindus 1420 SHDSL Router.
2	Make changes to its configuration (if necessary) in order to obtain the desired configuration. You do not have to send these configuration changes to the Telindus 1420 SHDSL Router.
3	Click on the *Export data to file* button: .
4	In the *Export configuration parameters* window, select the following: • Choose a directory where to save the file. • Enter a name for the file. • Make sure the file type is CMS. • Make sure the *Full configuration* option is selected.
5	Click on the *Save* button. The edited configuration of the Telindus 1420 SHDSL Router is stored on the PC in binary format. The file contains the complete configuration including the *Activate Configuration* command. As a result, the configuration is immediately activated when downloaded with TFTP.

13.6.3 Creating an ASCII configuration file

To create a configuration file in ASCII format, you can use the CLI syntax as explained in the Maintenance Tools manual. However, for the first time user it is easier to retrieve the configuration in the CLI format from the Telindus 1420 SHDSL Router.

There are two possible ways to create a configuration file in ASCII (*.cli) format:

- 13.6.4 - Creating an ASCII file using the TFTP get command on page 298
- 13.6.5 - Creating an ASCII file using the CLI get command on page 299

Do not use the TMA export utility for creating an ASCII type configuration file (not even when saving it as a TXT file). The resulting format is not compatible with the CLI format.

13.6.4 Creating an ASCII file using the TFTP *get* command

To create a configuration file in ASCII (*.cli) format using the TFTP *get* command, proceed as follows:

Step	Action
1	Start a TFTP session on the Telindus 1420 SHDSL Router. For example by typing `tftp 10.0.11.1` at the command prompt of your UNIX station, where 10.0.11.1 is the LAN IP address of the Telindus 1420 SHDSL Router.
2	Get the configuration file of the Telindus 1420 SHDSL Router. **Example** `tftp> get CONFIG.CLI dest_file.cli` Where … • `get` is the TFTP command to retrieve a file, • `CONFIG.CLI` is the Telindus 1420 SHDSL Router configuration file, • `dest_file.cli` is the destination file.
3	When the file transfer is finished, close the TFTP session.

13.6.5 Creating an ASCII file using the CLI *get* command

To create a configuration file in ASCII (*.cli) format using the CLI *get* command and Telnet logging, proceed as follows:

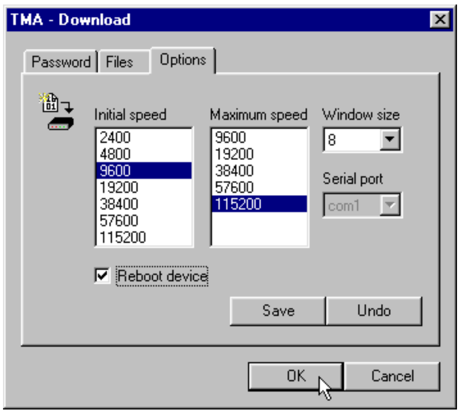
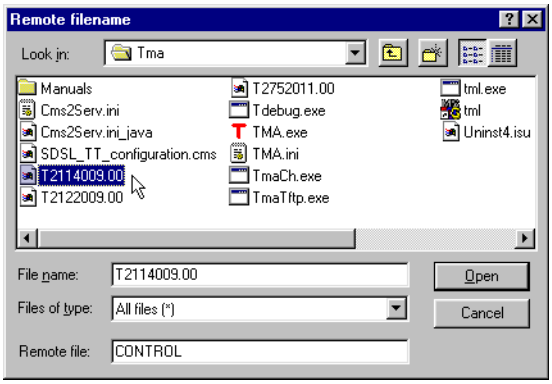
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Start a Telnet session on the Telindus 1420 SHDSL Router. You are automatically in CLI mode.</td></tr>
<tr><td>2</td><td>Redirect the CLI output or log it to a file.</td></tr>
<tr><td>3</td><td>Make sure you are in the top object (shdslRouter) and in the "Edit Configuration" group.</td></tr>
<tr><td>4</td><td>Execute the <code>get -r</code> command.</td></tr>
<tr><td>5</td><td>Stop output redirection or logging.</td></tr>
<tr><td>6</td><td>In the redirected or logged file you now obtained, remove all input and output logging before the get -r command. Also remove the get -r command itself.</td></tr>
<tr><td>7</td><td>Now, modify the configuration file:
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Change the string GET, now located at the beginning of the file, into SET.</td></tr>
<tr><td>2</td><td>Type the string Load Default Configuration at the beginning of the file.</td></tr>
<tr><td>3</td><td>Type the string Activate Configuration at the end of the file.</td></tr>
</table></td></tr>
<tr><td>8</td><td>Save this file to a file with an extension *.cli.</td></tr>
</table>

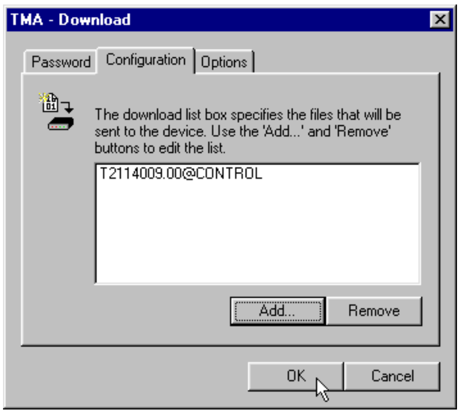
14 Downloading firmware

This chapter explains how to download new firmware into the flash memory of the Telindus 1420 SHDSL Router. The following gives an overview of this chapter:

14.1 Downloading firmware using TMA

To download firmware to the Telindus 1420 SHDSL Router using TMA, proceed as follows:

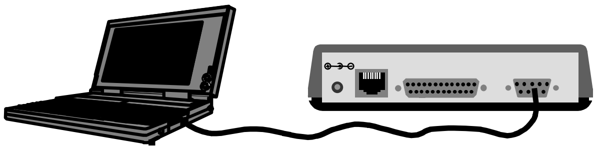
Step	Action
1	Establish a link between TMA and the Telindus 1420 SHDSL Router either over a serial or an IP link. Refer to 4 - Managing the Telindus 1420 SHDSL Router on page 37. Downloading firmware over an IP link is only possible when the Telindus 1420 SHDSL Router is equipped with two flash memory banks. Check the status attribute shdslRouter/flashVersions to find out how many flash banks your Telindus 1420 SHDSL Router contains.
2	In the TMA window select *Tools* → *Download…*
3	In case you made … • an IP connection, skip this step. • a serial connection, select the *Options* tab in the *TMA - Download* window. Then do the following: - Set the initial transfer speed to 9600 bps. - If you set the maximum transfer speed to 115200 bps, the actual transfer speed will be negotiated between 9600 bps and 115200 bps. - If your Telindus 1420 SHDSL Router is equipped with one flash bank only, tick the *Reboot* device box. Check the status attribute shdslRouter/flashVersions to find out how many flash banks your Telindus 1420 SHDSL Router contains. 
4	In the *TMA - Download* window, select the *Configuration* tab and click on *Add…*
5	In the *Remote filename* window, do the following: 1. Select the file you want to download (e.g. T1234001.00). 2. Type CONTROL in the *Remote file* field. 3. Click on *Open*. 
6	If you are currently connected to the Telindus 1420 SHDSL Router without write access, then you can enter a password in the *Password* tab which gives you write access. Else leave the *Password* tab blank.

Step	Action	
7	When the *TMA - Download* window reappears, click on *OK*. ⇒ A window opens and shows the download progress.	

14.2 Downloading firmware using TML

When downloading with TMA over a serial link, you actually evoke TML (Telindus Memory Loader) through TMA. You can also use TML without opening TMA.

To download firmware to the Telindus 1420 SHDSL Router using TML, proceed as follows:

Step	Action
1	Connect a serial port of your computer (e.g. COM1) through a straight DB9 male - female cable with the auxiliary connector of the Telindus 1420 SHDSL Router. 
2	Open a DOS window on your computer.
3	Go to the directory where the TML executable is located. Typically this is *C:\Program Files\TMA*.
4	Place the firmware file you want to download in this directory.
5	Type the following command: `tml -c1 -v -b -fTxxxxxxx.00@CONTROL?my_pwd` where … • `tml` is the executable (Telindus Memory Loader) to download files to the Telindus devices through their auxiliary port. • `-c1` specifies the COM port of the computer connected to the Telindus 1420 SHDSL Router (in this example COM1). • `-v` returns graphical information on the download status. • `-b` puts the Telindus 1420 SHDSL Router in boot mode. This is only necessary when your Telindus 1420 SHDSL Router is equipped with one flash bank only. Check the status attribute shdslRouter/flashVersions to find out how many flash banks your Telindus 1420 SHDSL Router contains. • `-fTxxxxxxx.00` is the firmware file you want to download (e.g. T1234001.00). • `CONTROL` (in capitals!) specifies that the destination is a flash bank of the Telindus 1420 SHDSL Router. • `?my_pwd` is the write access password as configured in the Telindus 1420 SHDSL Router. If no password has been configured, you may omit the ? and the password. To see a list of all the possible TML options: type `TML` in your DOS windows and press the ENTER key.
6	If you press the ENTER key, the firmware download begins. If you used the *-v* option together with the TML command, a graphical bar shows the download progress.

14.3 Downloading firmware using TML in boot mode

When a firmware download has failed or when a flash memory error occurs, it may be possible that the Telindus 1420 SHDSL Router becomes inaccessible to TMA. In that case, new software can still be downloaded by forcing the Telindus 1420 SHDSL Router in boot mode. Do this by means of the *start-up mode* DIP switch:

DIP switch name	DS1 no.	Setting	Function
start-up mode	1	**on**	Start up from flash memory.
		off	Start up in boot mode.

To download firmware to a Telindus 1420 SHDSL Router in boot mode, proceed as follows:

Step	Action
1	Disconnect the power supply and open the housing as described in 3.4 - Changing DIP switch and strap settings on page 35.
2	Set DIP switch bank DS1 position 1 to *off*. To locate this DIP switch bank, refer to 3 - DIP switches and straps of the Telindus 1420 SHDSL Router on page 31.
3	Replace the cover without fastening the screws and reconnect the power supply. ⇒ The Telindus 1420 SHDSL Router is now in boot mode.
4	Now proceed as explained in the previous section, 14.2 - Downloading firmware using TML on page 304.
5	When the download is finished, disconnect the power supply and open the housing again.
6	Reset DIP switch bank DS1 position 1 to *on*.
7	Properly replace the cover and reconnect the power supply.

14.4 Downloading firmware using TFTP

When downloading with TMA over an IP link, you actually evoke TFTP (Trivial File Transfer Protocol) through TMA. You can also use TFTP without opening TMA.

Downloading firmware using TFTP is only possible when the Telindus 1420 SHDSL Router is equipped with two flash memory banks. Check the status attribute shdslRouter/flashVersions to find out how many flash banks your Telindus 1420 SHDSL Router contains.

To download firmware to the Telindus 1420 SHDSL Router using TFTP, proceed as follows:

Step	Action
1	Start a TFTP session on the Telindus 1420 SHDSL Router. For example by typing `tftp 10.0.11.1` at the command prompt of your UNIX station, where 10.0.11.1 is the LAN IP address of the Telindus 1420 SHDSL Router.
2	Set the following TFTP parameters: • Set the retransmission time-out to at least 20 seconds. The syntax to do this is typically `rexmt 20`. • Set the total TFTP time-out sufficiently large (e.g. 40 seconds). The syntax to do this is typically `timeout 40`. • Set the transfer mode to binary (octet) format. The syntax to do this is typically `binary` or `octet`.
3	Type the following command: `tftp> put Txxxxxxx.00@CONTROL?my_pwd` Where … • `put` is the TFTP command to send a file. • `Txxxxxxx.00` is the firmware file (e.g. T1234001.00). • `CONTROL` (in capitals!) is the destination (flash memory). • `?my_pwd` is the write access password as configured in the Telindus 1420 SHDSL Router. If no password has been configured, you may omit the ? and the password.
4	When the file transfer is finished, close the TFTP session.

15 Technical specifications

This chapter gives the technical specifications of the Telindus 1420 SHDSL Router. The following gives an overview of this chapter:

15.1 Router features

The router features are as follows:

Feature	Description
routing	static routing & RIP version 2
access	access lists on each interface
WAN encapsulation	PPP encapsulation: RFC 1661 (LCP) and RFC 1332 (IPCP), with PPP CHAP authentication: RFC 1994
	Frame Relay encapsulation: RFC 1490, with … • LMI : CCITT, ANSI T1.617 D and revision 1 • PVCs only • inverse ARP • auto install
NAT & PAT	NAT and PAT with private addresses on the LAN interface and public addresses on the WAN interface or vice versa.

15.2 Line specifications

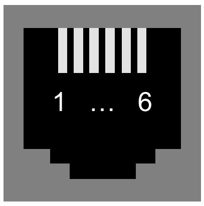
Specifications

The line specifications are as follows:

Parameter	Description
connector	RJ12
impedance	135 Ω
line speeds	from 64 kbps up to 2304 kbps in steps of 64 kbps
throughput delay	300 msec compliant to ETSI DTR/tm-3036
transmit level	13.5 dBm compliant to ETSI DTR/tm-3036
coding	TC PAM compliant to G.991.2 (G.SHDSL)
handshaking	compliant to G.994.1
performance (distance covered noise free)	conform to the following standard noise margin specifications: • Bellcore TA-NWT-001210 • ANSI T1E1.4/94-006 • ETSI ETR 152

The line connector lay-out

The following table shows the connector layout of the RJ12 line connector:

Pin	Signal	Figure
1	not used	
2	not used	
3	line	
4	line	
5	not used	
6	not used	

Maximum covered distance

The following table gives the maximum covered distance over a noise-free line:

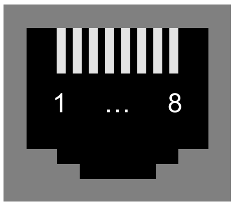
Line speed (kbps)	Maximum covered distance (km) for a given wire diameter					
	0.4 mm 26AWG	0.5 mm 24AWG	0.6 mm	0.8 mm 20AWG	1.0 mm 18AWG	1.2 mm
128	7.9	10.8	15.5	19.5	27.3	30.5
192	6.5	8.9	12.7	16.1	22.5	25.1
384	6.0	8.2	11.8	14.8	20.8	23.2
512	5.7	7.8	11.2	14.1	19.7	22.0
768	5.3	7.3	10.4	13.1	18.3	20.5
1024	5.1	7.0	10.0	12.6	17.6	19.7
1152	4.8	6.6	9.4	11.9	16.6	18.5
1536	4.2	5.8	8.2	10.4	14.5	16.2
2048	3.9	5.3	7.6	9.6	13.5	15.1
2304	3.8	5.2	7.4	9.4	13.1	14.7

15.3 Ethernet LAN interface

The LAN interface specifications are as follows:

Parameter	Description
connector	8 pins RJ45, female
operation	10BaseT Ethernet

The following table shows the connector layout of the RJ45 Ethernet LAN interface connector:

Pin	Signal	I/O	Figure
1	transmit (positive)	output	
2	transmit (negative)	output	
3	receive (positive)	input	
4	not used	-	
5	not used	-	
6	receive (negative)	input	
7	not used	-	
8	not used	-	

15.4 Management interface

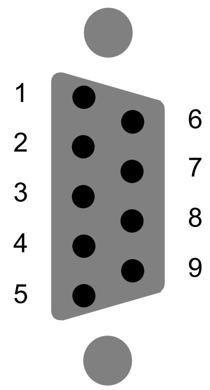
The possible management interfaces are:

Management interface	Connector type	Speed
LAN interface	RJ45	10 Mbps
asynchronous through the auxiliary connector	9 pins subD	9600 bps, 8+N

15.5 Auxiliary connector

The auxiliary connector (sometimes also called NMS or control port) is a 9 pins subD connector labelled AUX. The signals on these connector are V.24 / V.28 signals.

The auxiliary connector has the following pin layout:

Pin	Signal	DCE	Figure
1	-	output	
2	NMS RxD	output	
3	NMS TxD	input	
4	not used	-	
5	GND	-	
6	not used	-	
7	NMS RTS	input	
8	NMS CTS	output	
9	-	output	

15.6 Power requirements

The power requirements are as follows:

- 9 Vdc, 1000 mA

15.7 Mechanical dimensions

The power requirements are as follows:

- height : 38 mm
- width : 150 mm
- depth : 250 mm
- weight : 1 kg

15.8 Safety compliance

- EN60950
- Class 1 equipment for Table Tops with 115/230 Vac internal power supply.
- Class 3 equipment for …
  - Table Tops with 115/230 Vac external power supply adapter
  - Table Tops with -48 Vdc internal power supply
  - Card Versions.

15.9 Over-voltage and over-current protection compliance

The over-voltage and over-current protection complies with ITU-T K.44 and ETSI ETS 300 386-2 recommendations.

15.10 EMC compliance

- EN55022 B Emissions
- EN55024 Immunity
- EN61000-3-2 Harmonics
- EN61000-3-3 Voltage fluctuations and flicker
- EN61000-4-2 ESD
- EN61000-4-3 Radiated immunity
- EN61000-4-4 EFT/burst
- EN61000-4-5 Surge
- EN61000-4-6 Conducted immunity
- EN61000-4-8 Power magnetic field immunity
- EN61000-4-11 Voltage dips & drops
- ENV50204 Radiated immunity against digital radio telephone

15.11 Environmental compliance

- Storage conditions: ETSI ETS 300 019-1-1 Class 1.1. In addition, the storage temperature has to be between -25 to +70°C
- Transport conditions : ETSI ETS 300 019-1-2 Class 2.3
- Stationary use conditions: ETSI ETS 300 019-1-3 Class 3.2. In addition, the requirements below apply:
  - relative humidity 5 to 95% non-condensing and ambient operational temperature -5 to 45°C or
  - relative humidity 0 to 95% non-condensing and ambient operational temperature -10 to 50°C
- Maximum altitude: 3000m
- International protection (IP) class of protection against solid and liquids: IP40

Annex

Annex A: common TCP and UDP numbers

The following table shows the port numbers for a number of common protocols using TCP and UDP as transport protocol. As far as possible, the same port numbers are used for TCP as for UDP. A complete list can be found in the RFCs (Requests For Comment).

Port No	Protocol	UDP/TCP	Description
20	ftp-data	TCP	File Transfer (Default Data)
21	ftp	TCP	File Transfer (Control)
23	telnet	TCP	Telnet
25	smtp	TCP	Simple Mail Transfer Protocol
37	time	UDP/TCP	Time Server
42	nameserver	UDP	Host Name Server
53	domain	UDP/TCP	Domain Name Server
65	tacacs-ds	UDP/TCP	TACACS-Database Service
67	bootps	UDP	Bootstrap Protocol Server
68	bootpc	UDP	Bootstrap Protocol Client
69	tftp	UDP	Trivial File Transfer
80	www-http	TCP	World Wide Web HTTP
119	nntp	TCP	Network News Transfer Protocol
137	netbios-ns	UDP	NETBIOS Name Service
138	netbios-dgm	UDP	NETBIOS Datagram Service
139	netbios-ssn	UDP	NETBIOS Session Service
161	snmp	UDP	SNMP
162	snmptrap	UDP	SNMPTRAP
1728	telindus	UDP	Telindus Protocol used by TMA

Annex B: product information

The following table displays the product information of the Telindus 1420 SHDSL Router:

Sales code	Product name	Description
172729	TELINDUS 1420 SHDSL ROUTER 230VAC	IP router with 1pair SHDSL line interface. For LAN-LAN connections. Management over IP via TMA, TMA CLI, telnet, SNMP & TFTP. Includes European 230VAC power adapter.
172730	TELINDUS 1420 SHDSL ROUTER NPWR	IP router with 1pair SHDSL line interface. For LAN-LAN connections. Management over IP via TMA, TMA CLI, telnet, SNMP & TFTP. Delivered without power adapter.
172899	MANUAL TELINDUS 1420 SHDSL ROUTER (E)	Manuals are delivered with the product in electronic format (CD-ROM) for environmental reasons. If however a hardcopy (print-out) of the manual is required, this sales item can be used. Between brackets an indication of the language.
175590	PWR-PLUG (EUR VERSION)230VAC >9VDC	Wallplug power module European type, 230Vac -> 9Vdc for Desktop units delivered without power adapter.
175592	PWR-PLUG (UK VERSION) 230VAC->9VDC	Wallplug power module UK type, 230Vac -> 9Vdc for Desktop units delivered without power adapter.
171304	PWR-PLUG 48VDC->7,5/9VDC	Wallplug power module 48Vdc -> 7,5 / 9Vdc for Desktop units delivered without power adapter.

Index

A