COMTREND CORPORATION

CT-320

SDSL Modem

CT-520

SDSL Router

User's Manual

Preliminary 1.0

Preface

The user's manual is a preliminary version for those who take interests in Comtrend CT-320 SDSL Modem or CT-520 SDSL Router.

The user's manual provides general information about the features, functions, installation, operation and other useful messages of the mentioned product. The user reading this manual is presumed to have basic understandings of telecommunication and the relevant knowledge. This manual is subject to change without notice.

For product update, new product release, manual revision, software upgrade, technical support, etc., please visit Comtrend Corporation at http://www.comtrend.com.tw.

Copyright

Table of Content

Chapter 1 Introduction

This manual provides information about the features, installation, and operation of CT-320 SDSL modem and CT-520 SDSL router. The following topics are covered.

- Chapter 1-2: provides the features and physical installation of the device.
- Chapter 3: introduces three access methods and provides general management information
- Chapter 4-10: describes operation and configuration via console and Telnet.
- Chapter 11: describes maintenance via console and Telnet.
- Chapter 12: describes operation, configuration and maintenance via Web.

When necessary, this manual will use the screen displays captured from the CT-520 as examples to help understand.

1.1 Overview

The CT-320 SDSL modem and CT-520 SDSL router satisfy the needs of multiple users for small office/home office and remote office/branch office applications. In compliance to ITU-T G.991.2 (G,shdsl) standard, they provide symmetrical transmission at speed up to 2.3 Mbps through SDSL connection over one ordinary telephone line. In addition, they support up to 16 virtual concurrent connections to multiple destinations.

The CT-320 SDSL modem and CT-520 SDSL router can be used for variety of applications, including video conferencing, remote training, e-commerce, and other multimedia applications. Easy configuration and monitoring can be accomplished by using web browser.

The CT-520 SDSL router has full routing capabilities to segment/route IP protocol and is capable of bridging other protocols. It can be also configured in either server or client mode providing a point-to-point connectivity between two sites.

1.2 Features

CT-320 and CT-520 are featured with the following functions.

- Compact and high performance standalone units
- Bridge function
- G.shdsl
- Auto-negotiation rate adaptation
- AAL5 for ATM over SDSL
- UBR / CBR / VBR ATM services
- VC-based and LLC multiplexing
- Up to 16 VCs
- One Ethernet port for LAN connection
- One console port for local management
- Embedded SNMP agent
- Web-based management
- Configuration backup and restoration
- OAM F4/F5
- Static route/ RIP/RIP v2 routing function (CT-520 only)
- Dynamic IP assignment and Network Address Translation (CT-520 only)

1.3 Application

The CT-320/CT-520 can be applied for DSLAM and point-to-point applications.

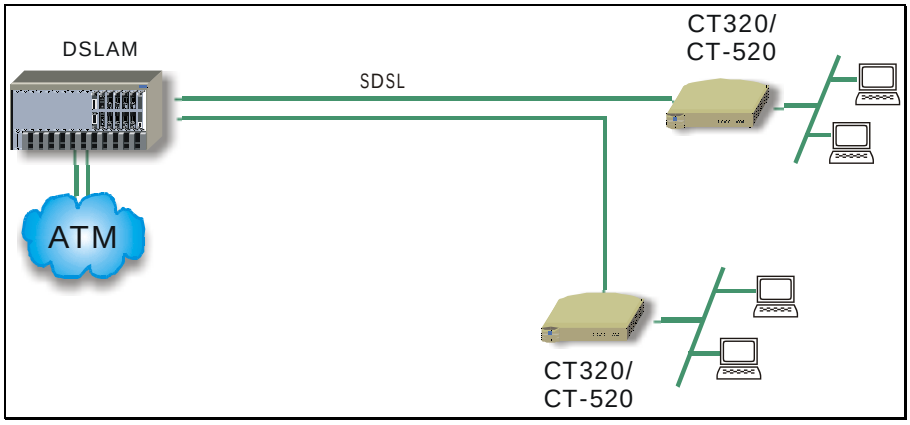


Figure 1–1 DSLAM Application

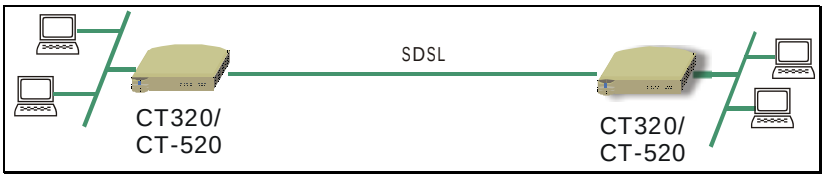


Figure 1–2 Point-to-point Application

Chapter 2 Hardware Installation

2.1 Physical Features

Identify the type by the label at the left bottom of the faceplate.

2.1.1 Front Panel LED Indicators

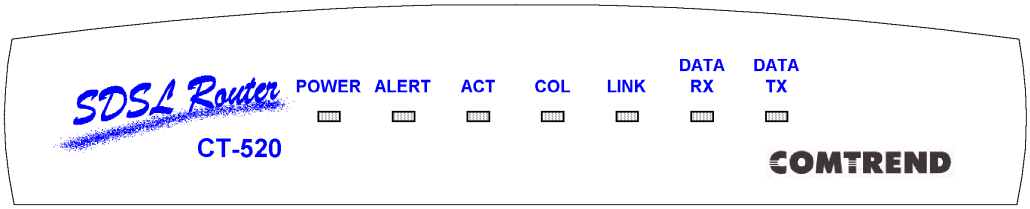


Figure 2–1 Front View of CT-520

There are nine LED indicators on the front panel. These LED indicators indicates power status, data activity, physical links and alarm conditions, etc. The description of each LED is tabulated in Table 2-1.

LED	Color	Mode	Function
Power	Green	On	12VAC power input is supplied to this unit.
		Off	Power is not connected
Alert	Red	Off	Normal status
		On	An alarm occurs
		Flash	Software downloading or self-testing
ACT	Green	On	Transmit data or receive data over Ethernet link
		Off	No data transmitted or received over the Ethernet link
COL	Yellow	On	Collision occurs over Ethernet
Link	Green	On	The physical connection between RJ11 and telephone line is established
		Flash	SDSL line is training
		Off	SDSL connection not established.
Data RX	Green	On	Receive data over SDSL link

		Off	No data received over the SDSL link
Data Tx	Green	On	Transmit data over the SDSL link
		Off	No data transmitted over the SDSL link

Table 2–1 LED Indicators

2.1.2 Rear Panel Connectors

There are seven connectors on the rear panel. They are marked **SDSL, LAN, Console,** and **Power 12 VAC** respectively. To apply these connectors, please refer to Section 2.3.

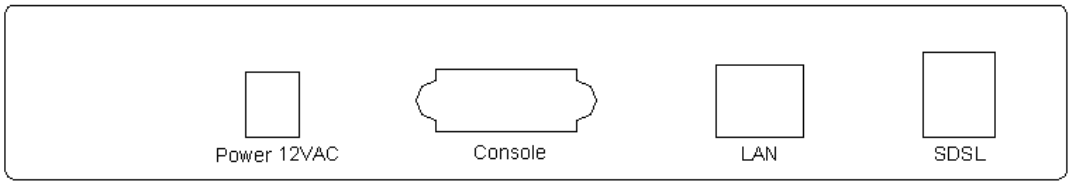


Figure 2–2 Rear View of the CT-320/CT-520

2.2 Preparing Installation

To install the SDSL device, please prepare the following accessories.

- **A Standard VT-100 Compatible Terminal** –

  This terminal is essential to perform the initial configuration of the SDSL device. Normally this is a terminal with VT-100 emulation program, such as Telix.

- **A Console Port Cable to connect to Console port** –

  An RS-232, DB9-to-DB9 straight through cable is required to connect the terminal to the unit. The following table lists the pin assignments of the DB9 console port. Only Pin2, 3 and 5 are used.

Pin	Definition	Pin	Definition
1	-	6	-
2	TD	7	-
3	RD	8	-
4	-	9	-
5	GND		

Table 2–2 Pin Assignments of Console Port

- **An AC power adapter cord to connect to the Power jack**

  A 110 VAC to 12 VAC or 220 VAC to 12 VAC power adapter cord is shipped with the unit. It is used to provide the necessary power for the unit's operation.

- **RJ45 10BaseT Ethernet connector cable to connect LAN**

  An RJ45 LAN connection cable is needed to connect the device to the Local Area Network (LAN). The pin assignments of the RJ45 connector are listed below.

Pin number	Definition	Pin number	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Table 2–3 Pin assignments of RJ45 Port

- **An RJ11 connection cable to connect to SDSL port–**

  An RJ11 connector cable is used to connect the device to the telephone line from the telephone company. The following lists the pin assignments of the RJ11 connector.

Pin	Definition	Pin	Definition
1	-	4	SDSL_TIP
2	-	5	-
3	SDSL_RING	6	-

Table 2–4 Pin Assignments of RJ11 Port

2.3 Installation

The backplane connectors of the device can be connected as follows. Figure 2-3 illustrates possible connections of these connectors.

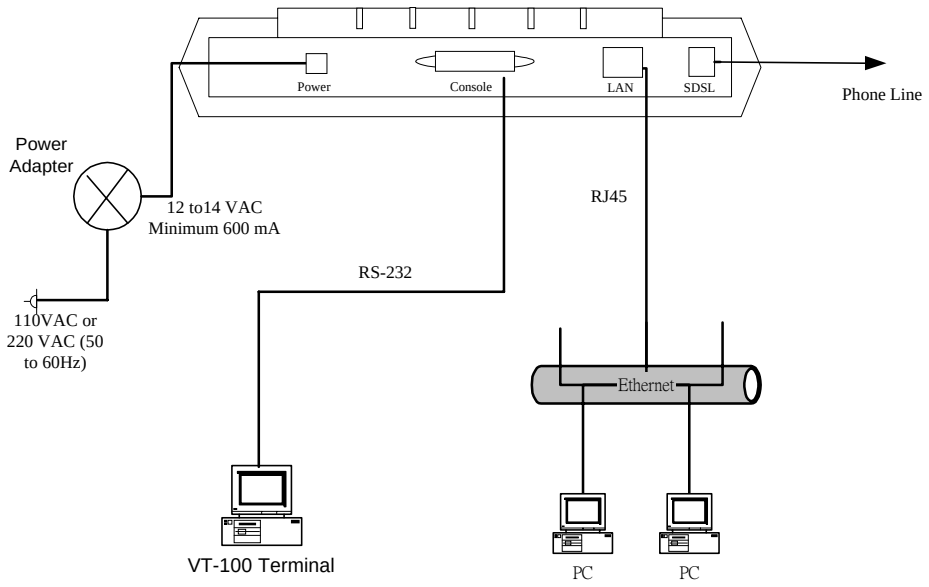


Figure 2–3 Installation

1. Connect the power jack to the AC power supply with a power adapter cord.
2. Connect the LAN port to the LAN with an RJ45 connector cable.
3. Connect the Console port to a VT-100 compatible terminal for local management with an RS-232 straight through cable.
4. Connect the SDSL port to the phone jack.

Caution 1: If the unit fails to power on, or it malfunctions, first verify the power supply is correctly connected. Then power it on again. If the symptom persists, please contact our technical support engineers.

Caution 2: Always disconnect all telephone lines from the wall outlet before servicing or disassembling this device.

Chapter 3 Management

This chapter introduces how to access and manage the device. To configure the device for user's application, it is strongly recommended that user also read Chapter 4 Initial Configuration after reading this chapter.

3.1 How to Access

Three methods are available to access, configure, operate or monitor the device. You can choose from console, Telnet, or Web. Below shows how to get accessed to the device.

3.1.1 Console

Your console PC should be installed with VT-100 emulation program, such as Telix or HyperTerminal 5. Before you manage the device, verify all the connections are made correctly.

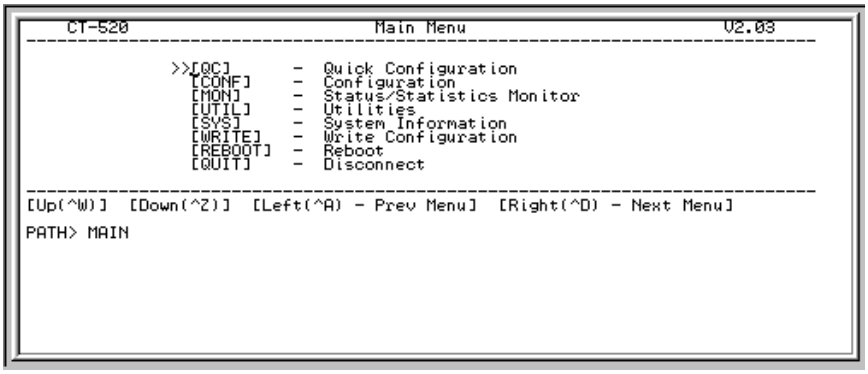
Step 1 Start a VT-100 compatible program such as ***Telix*** in the local terminal. The session parameters of the console port are:

- Baud rate: 9600
- Parity: none
- Data bits: 8
- Stop bit: 1
- Flow control: None

Step 2 After the session parameters are set up, press any key to bring up the following message.

"Press ESC key to enter console mode configuration".

Step 3 Press **ESC** key to display the main menu.



Step 4 You can start operating this device now.

Step 5 Use the arrow keys to select the utility item and enter the menu you want to configure.

To configure the device for Telnet and Web access, further complete the procedures to change the necessary parameters. Or you can skip them by using the following default values.

- LAN IP address: 210.65.231.206
- Read-write access

  Login: root

  Password: root

Step 6 To change a LAN IP address, enter the **MAIN/QC/LAN** menu.

Step 7 To change a WAN IP address, enter the ATM interface menu, e.g., **MAIN/QC/ATM/ATM1** (refer to Section 4.2.2 ATM Interface for more details).

Step 8 Hold down CTRL-S keys to save the IP address.

Step 9 To change the passwords, enter the **MAIN/CONF/SYSTEM** menu.

Step 10 You can enable the console password check function in the Console Password Check field. Then, a visitor will be requested to enter the password.

Step 11 Enter ADMINISTRATOR password in the New Administrator Password field and retype the password to confirm.

Step 12 Enter USER password in the New User Password field and retype the password to confirm.

Step 13 Hold down CTRL-S keys to save the passwords.

Step 14 Return to the main menu and select **WRITE** to write configurations to flash memory.

Step 15 Reboot the system.

Step 16 In less than one minute, the sentence ***"Press ESC key to enter console mode configuration"*** displays on your screen.

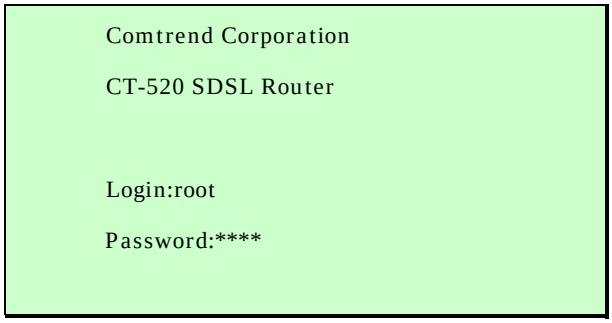
Note 1: If you use HyperTerminal, it is recommended to install the Edition 5.0.
2: After adjusting the parameters, make sure you save them in the flash memory and then reboot the system before you quit, or you will lose the new parameters after restart.

3.1.2 Telnet

Maximum one administrator and two common users can use Telnet to access the device from different locations at the same time.

Step 1 Telnet the device with the LAN IP address or WAN IP address (refer to Section 3.1.1 Step 5-8 on setting LAN/WAN IP address). The default LAN IP address is 210.65.231.206.

Step 2 You will be prompted to enter user name and password.



To have full access privilege as an ADMINISTRATOR, type **root** in the Login field, and type the password that is set in console (refer to Section 3.1.1 Step 9-13).

To have read-only access as a common USER, type **user** in the Login field and type the password that is set in console (refer to Section 3.1.1 Step 9-13).

Or if the default password is not changed, type **root** for ADMINISTRATOR password or **user** for common USER password.

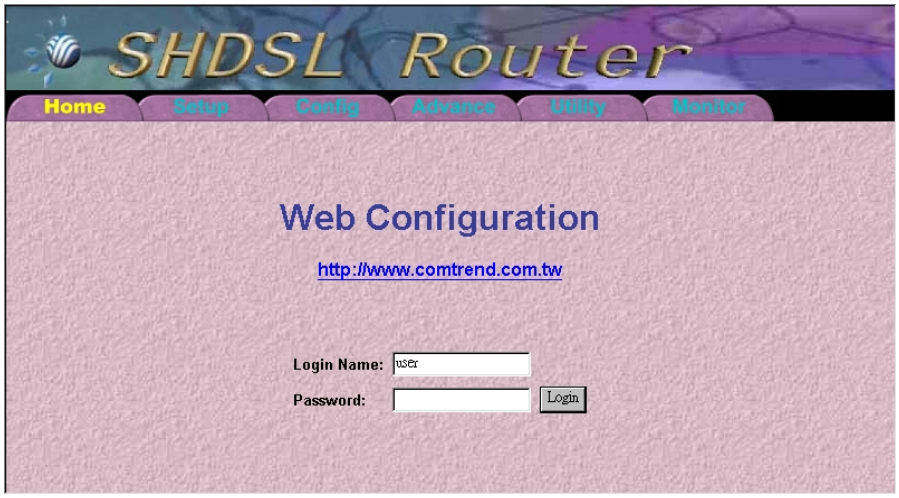
Step 3 The main menu displays. The menus and operations of Telnet are the same as those of the console.

3.1.3 Web

Web-based management can be used by only one person at any one time. It is ENABLED by factory default. To disable it, enter the MAIN/CONF/HTTPD menu from console or Telnet.

Step 1 Browse the device with the LAN IP address or WAN IP address (refer to Section 3.1.1 Step 5-8 on setting LAN/WAN IP address). The default LAN IP address is 210.65.231.206.

Step 2 You will be requested to enter login name and password.



To have the full access privilege as an ADMINISTRATOR, type **root** in the Login field, and type the password that is set in console (refer to Section 3.1.1 Step 9-13).

To have read-only access as a common USER, type **user** in the Login Name field and type the password that is set in console (refer to Section 3.1.1 Step 9-13).

Or if the default password is not changed, type **root** for ADMINISTRATOR password or **user** for common USER password.

Step 3 The main page displays.

Step 4 For more operation instructions, please refer to Chapter 12.

Note: when a user has entered the system via the Web, a second user (neither administrator nor user) cannot access the device via Web at the same time. The second user should enter the console or Telnet.

3.2 General Configuration in Console/Telnet

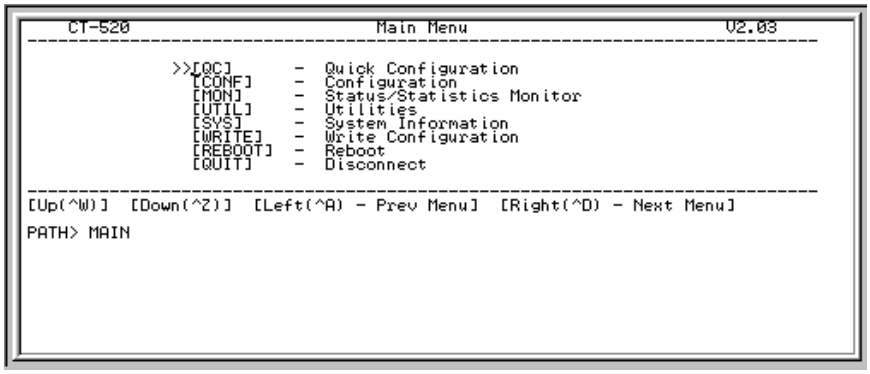
3.2.1 Configuration Steps

The device should be configured from the main menu, branch menu to leaf menu in order. To explain conveniently in this document, we denote each menu's operating sequence by path prompts. You can easily find the directory of the menu, branch menu, or leaf menu via the path prompt.

For example, if you want to configure the LAN interface of the SDSL device, please complete the following procedures.

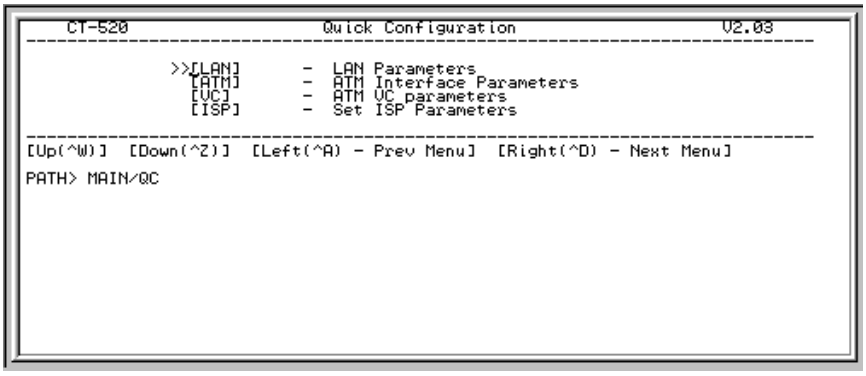
Step 1 Enter the main menu.

The path prompts **"MAIN"** to indicate the directory of current operating menu.



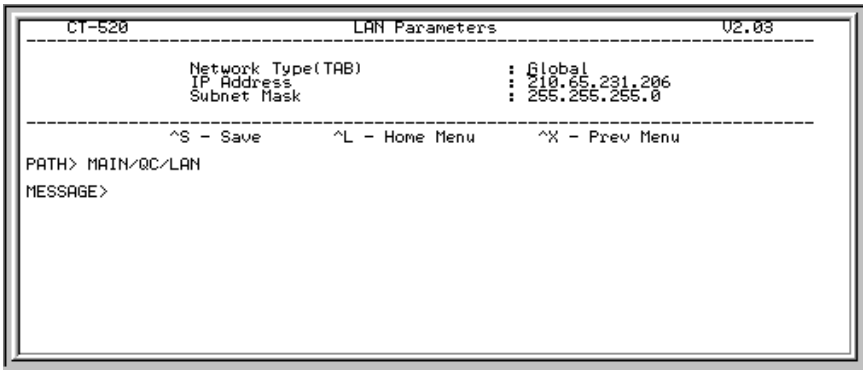
Step 2 Use the up or down arrow key to select an item. In this case, select **QC**. Press right arrow key to go to **MAIN/QC** branch menu.

The path prompts **MAIN/QC** to indicate the directory of current operating menu.



Step 3 Use the up or down arrow key to select an item. In this case, select **LAN** and press right arrow key to enter the leaf menu.

The path prompts **MAIN/QC/LAN**.



Step 4 Enter a parameter in each field. For some fields indicating TAB, press the TAB key to make a selection among the pre-defined values, e.g., Network Type (TAB). Then save the settings into RAM by holding down CTRL-S keys.

Step 5 Return to the main menu and enter **WRITE** menu to save the configurations from RAM to flash memory. Also refer to Section 11.3.

Step 6 Reboot the system by entering **REBOOT** menu from the main menu. The system then powers on with new parameters. Also refer to Section 11.4.

Note: before you exit the Console/Telnet, be sure you have saved the changes to the flash memory and reboot the device. If you do not, or you only write the changes without rebooting the device, or even you reboot the system without writing the parameters into the flash memory, the changes will be lost after you exit the system.

3.2.2 Menu Layout

The menu follows a tree-structured design and is divided into 3 categories, main menu, branch menu and leaf menu. You can select each utility item across configuration path using the up, down, left and right arrow keys in main and branch menus. The leaf menu is used to program each parameter and should be saved when a new parameter is set.

The layout of a menu includes messages like utility items, firmware version, model name, and keyboard instructions.

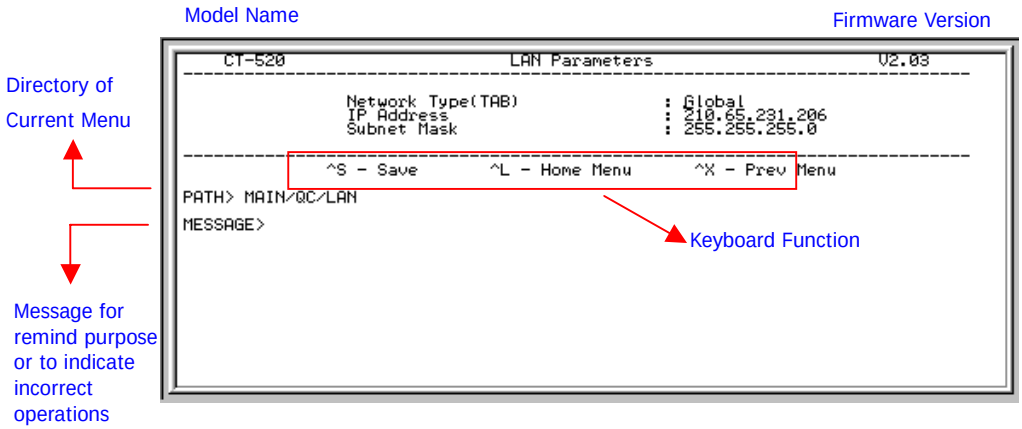


Figure 3-1 General Information in Each Menu

3.2.3 Keyboard Operations

1. UP	**Up arrow key.** The cursor moves up one field in the configuration menu.
2. Down	**Down arrow key**. The cursor moves down one field in the configuration menu.
3. Left-Prev Menu	**Left arrow key.** It returns to previous menu.
4. Right-Next Menu	**Right arrow key.** It skips to next menu.
5. ^S	Hold down CTRL-S keys simultaneously to perform different actions in some menu such as “Save”, “Add”, “Delete” and “go”.
6. ^X	Hold down CTRL-X keys simultaneously to return to previous menu.
7. ^L	Hold down CTRL-L keys simultaneously to return to Home Menu
8. ^W = Up	Hold down CTRL-W keys simultaneously to move the cursor a space upward. This function is equal to the up arrow key.
9. ^Z = Down	Hold down CTRL-Z keys simultaneously to move the cursor a space downward. This function is equal to the down arrow key.
10. ^A = Left	Hold down CTRL-A keys simultaneously to enter the previous menu. This function is equal to the left arrow key.
11. ^D = Right	Hold down CTRL-D keys simultaneously to enter the selected menu. This function is equal to the right arrow key.
12. ^T	Hold down CTRL-T keys simultaneously to reset the value or statistics counted.
13. ^R	**Hold down CTRL-R keys simultaneously to refresh or restore the menu.**
14. Q	It stops certain action, such as software download.
15. Tab	In the leaf menu, you can input parameters in each field or select the pre-defined options (such as Enabled/ Disabled) by pressing the TAB key.

Note 1: ^S is defined as “Save” in some menu, which can store all configurations into the system RAM. If you want to keep the configurations permanently, please perform the Write function by entering the MAIN/WRITE menu and reboot the system by entering the MAIN/REBOOT menu.

Note 2: ^W, ^Z, ^A, and ^D are used when the arrow keys are not available or ineffective.

Chapter 4 Initial Configuration (Console/Telnet)

This chapter guides you how to configure the SDSL device for the first time. It includes initial configuration, quick configuration, and SHDSL characteristics parameters. For further configurations, please refer to Chapter 5~11.

- Initial setup: to configure the security and basic features of the device
- Quick configuration: to configure the LAN, ATM, ATM VC, ISP parameters
- SHDSL characteristics: min/max base rate/subrate, power back off, remote

4.1 Initial Setup

4.1.1 Console Password Check

Normally, a local user does not have to enter the password when accessing the device. If password check function is required during console access, enter the **MAIN/CONF/SYSTEM** menu and enable it in the Console Password Check field. Then, a visitor who attempts to access the device from console will be prompted for password. Also refer to Section 4.1.2.

4.1.2 Login Name & Passwords

There are two types of login names, root and user. Root is for the ADMINISTRATOR with full read-write privilege, and user is for the common USERS with read only. The login names are preset in the factory and cannot be changed.

Each login name comes with a password. The default password for root, the system administrator, is **root** and for user, the common user, is **user**. The passwords can be changed in the **MAIN/CONF/SYSTEM** menu.

4.1.3 Bridge and Router Mode

The CT-520 supports both bridge and router modes and CT-320 supports bridge mode only. The default value of CT-520 is bridge mode with ATM interface 1 enabled. To change the mode, enter the **MAIN/CONF/SYSTEM** menu. In the **Operation Mode** field, select **bridge** or **router**. If bridge mode is selected, the IP address of LAN interface is considered as the bridge IP, and the IP address of the ATM interfaces are considered meaningless.

4.1.4 Terminal Mode

The SDSL device can be used for DSLAM or peer-to-peer application. When it is connected to DSLAM, select CPE in the Terminal mode field. When two SDSL devices are used, configure one of them as the CO and the other as the CPE.

4.1.5 LAN IP Address

Enter the **MAIN/CONF/INTERFACE/LAN** menu to set up a LAN IP address for the device. The default IP address is 210.65.231.206. This procedure is also described in Section 3.1.1.

4.2 Quick Configuration

This section describes how to configure the basic environment (the interface and ISP) for the device via console or Telnet. The device supports two interfaces, Ethernet and WAN Interface. It can connect to a local area network via Ethernet interface and to wide area network via WAN interface.

To complete the quick configuration, enter the **MAIB/QC** screen. It includes settings for LAN, ATM, VC, and ISP parameters. The device can operate normally after the quick configuration is completed. The sub-menus of the QC are also repeated in those of the CONF (configuration).

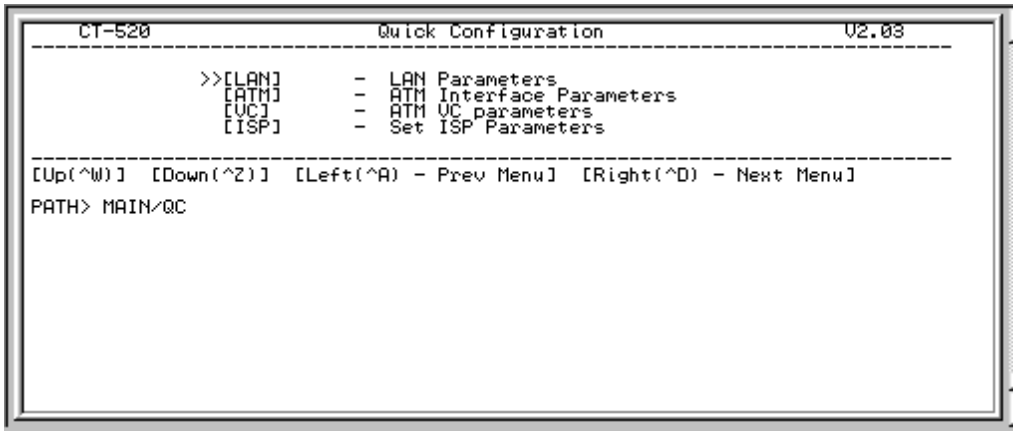


Figure 4–1 Quick Configuration Menu

4.2.1 LAN Interface

Step 1 Enter the **MAIN/QC/LAN** menu.

Step 2 Enter a parameter in each field.

- **IP address:** Enter the address of the IP network
- **Subnet Mask:** Enter the mask of the IP network
- **Network Type:** Select **Virtual** mode to enable the network address translation function. Or, select **Global** mode to disable it.

Step 3 Hold down Ctrl-S keys to save the parameters.

4.2.2 ATM Interface

A network service defines the data encapsulation and protocol characteristics for the connection between two packet switching devices. The device supports PPP and RFC 1483 network services. The device and the remote ISP should use the same network service to establish the session.

For PPP network service, the device supports two authentication protocols, PAP and CHAP. It can identify the server's authentication protocol and will auto-adjust itself to the same protocol.

Follow the steps to set the ATM interface. There are 16 ATM interfaces. The default values of these 16 interfaces are ATM1 enabled with the others disabled.

Step 1 Enter an ATM interface leaf menu from the **MAIN/QC/ATM** menu.

Step 2 Enter a parameter in each field.

- **Interface:** Enable or disable the ATM interface
- **Protocol**

  Ethernet (RFC1483 Bridge): This is the factory default. It is not necessary to configure the ATM VC field.

  PPP (PPP over ATM), **PPPOE** (PPP Over Ethernet), **IP Over ATM**

  1. Also configure the IPCP and ISP fields.
  2. Enter the ATM VC leaf menu and select an option in the AAL5 encapsulation field (also mentioned in Section 4.2.3).
- **IPCP:** static or dynamic **(for PPP)**

  Static –a local IP address is assigned manually during PPP session establishment.

  Dynamic –a local IP address is obtained dynamically from the remote PPP server during the PPP session establishment.
- **ISP:** Assign this ATM interface to one of the eight ISPs. Also, you should enter the selected ISP menu to assign the required authentication user name and password for PAP and CHAP. For example, you have selected ISP1 in this field. Then, enter the MAIN/QC/ISP/ISP1 menu to configure the ISP1 parameters (Section 4.2.4)
- **Network Type:** If NAT (Network Address Translation) function is required, select **Virtual** mode. Otherwise, select **Global** mode.
- **ATM VC:** this is correspondent to the ATM interface, e.g., ATM1 to VC1 or ATM2 to VC2. Also enter the ATM VC menu to configure the VC parameters (Section 4.2.3).
- **IP address:** Valid in the router mode only. Enter address of the IP network.
- **Subnet mask:** Valid in router mode only. Enter the mask of the IP network.

Step 3 Hold down CTRL-S keys to save the new configurations into your system RAM.

Note: For PPP or PPPOE protocol, if **Dynamic** function is selected in the IPCP field, your ISP IP server will auto-assign an IP address and subnet mask to the device. You can enter **MAIN/MON/ATM** menu to see what IP/Subnet you are assigned.

4.2.3 ATM VC Parameters

Step 1 Enter a VC leaf menu from the **MAIN/QC/VC** menu.

Step 2 Enter a parameter in each field.

- **VPI/VCI:** enter the value of VPI and VCI.

  VPI – The Virtual Path Identifier (VPI) is part of the cell header for the cells that are transferred over this connection.

  VCI – The Virtual Channel Identifier (VCI) is part of the cell header for the cells that are transferred over this connection. If you are configuring multiple VCs, enter the number of respective VC in this field. The VCI value should be between 32 and 65535.

- **AAL5 Encapsulation**

  VCMUX – VC based multiplexing

  LLC – LLC encapsulation

- **VC QOS**

  UBR – Unspecified Bit Rate. No limit is specified for information rate.

  CBR – Constant Bit Rate. A constant rate is specified for the flow of information.

  VBR – Variable Bit Rate. A certain rate is specified for the flow of information.

- **Peak Cell Rate (bps):** the Peak Cell Rate is the maximum amount of bit per second transmitted over this connection. This is determined by the minimum intercell spacing in seconds, which is the time interval from the first bit of one cell to the first bit of next cell. The PCR ranges from 30,000 to 960,000.

- **Sustainable Cell Rate (bps):** for VBR only. This is the rate at which cells are transmitted over this connection. The rate is counted in bit per second. Note that 30000 ≦ SCR ≦ PCR.

- **Burst Tolerance (msec) (refer to maximum Burst size):** for VBR only. This is a maximum number of cells that is sent at the peak rate. The number of cells is counted in milli-seconds. The BT ranges from 10 to 200.

Note: MBS (Maximum Burst Size) formula: $\left[1+\frac{BT}{\frac{1}{SCR}-\frac{1}{PCR}}\right]$ where [x] stands for the integer part of x. In the formula: BT is counted in seconds and SCR/ PCR in cell per second.

Step 3 Hold down Ctrl-S keys to save the parameters.

4.2.4 ISP

ISP should be configured when PPP/PPPOE is selected. The SDSL device can be connected to 8 ISPs respectively with different VPI/VCI values. Below shows how to configure the necessary parameters to connect to an ISP.

Step 1 Enter a leaf menu from the **MAIN/QC/ISP** menu.

Step 2 Enter a parameter in each field.

- ISP name: Account ISP name
- User name: Account user name for logging on to an ISP
- Password: Account password for logging on to an ISP

Step 3 Hold down Ctrl-S keys to save the parameters.

Step 4 Write the new configurations into the flash memory by selecting **WRITE** from the main menu.

Step 5 Reboot the system by selecting **REBOOT** from the main menu or reboot the system later.

Note: If any incorrect data is input, the system will respond with an error report.

4.3 SHDSL Characteristics Parameters

In the **MAIN/CONF/SHDSL** menu, the administrator can set up the system chipset's characteristics.

Field	Parameter	Description
Minimum Base Rate(1-36)	Nx64 Kbps (N=1-36)	You can set a fixed data rate when the following two conditions are matched. 1. Maximum subrate is set equal to minimum subrate 2. Maximum base rate is set equal to minimum base rate The data rate can be auto-adaptive according to the line performance with the following two conditions. The system will give an alarm message when you fail to follow. 1. Maximum subrate exceeds minimum subrate 2. Minimum base rate exceeds maximum base rate
Maximum Base Rate(1-36)	Nx64 Kbps (N=1-36)	
Maximum Sub Rate(0-1)	Ix8K (M=0 or 1)	
Minimum Sub Rate(0-1)	Ix8K (M=0 or 1)	
Power Back Off	Enable/Disable	It is recommended that user keep the default setting for this function. For explanation on power backoff, please refer to G.991.2 (G.shdsl)
Remote	Enable/Disable	Reserved only.

Note1: Total data rate= Nx64 Kbps + Ix8 Kbps.
Note2: The version doesn't support EOC (Embedded Operation Channel) function.

Chapter 5 Bridging

5.1 Overview

Chapter 5 and Chapter 6 specify how to configure the device in order to forward packets to LAN and ATM WAN interface. A router, such as the CT-520, forwards packets on the basis of network-level addresses. A bridge, such as the CT-320 forwards packets on the basis of physical level or Medium Access Control Address (MAC).

CT-520 supports both bridging and routing modes. It can be configured to route IP or bridge other protocols between workstations on Local Area Network (LAN) and up to 16 remote locations over an ATM Wide Area Network (WAN).

CT-320 supports the bridging mode only.

5.2 Static Bridging Configuration

This section describes the static bridging configurations. The user can add, delete static MAC entry, or view the bridging parameters.

5.2.1 Add A Static MAC Entry

Step 1 Enter the **MAIN/CONF/BRIDGING/STATIC/ADD** menu.

Step 2 In the menu, input the MAC address & Port Map

Note: Port Map

There are seventeen characters used to specify the operating mode of seventeen interfaces when the MAC address is processed in bridging mode. The first character represents LAN interface (10000000000000000) and the last character represents ATM16 interface (00000000000000001).

There are three operating modes, **filter, forward, and dynamic,** representing as 0, 1, 2, respectively. The dynamic mode means that the operating mode of the MAC address in the interface follows the learning result of the bridging function. For example, the port map of the MAC address is configured to be "10000000000000000". It means the MAC address will be forwarded to the LAN interface and filtered from all ATM interfaces. Similarly, 01000000000000000 means ATM interface 1.

Bit 1	Bit2	Bit 3……	Bit 16	Bit 17
LAN	ATM1	ATM2……	ATM15	ATM16

Step 3 Hold down Ctrl-S keys to save the new configurations.

5.2.2 Delete A Static MAC Address

Step 1 Enter the **MAIN/CONF/BRIDGING/STATIC /DELETE** menu.

Step 2 Enter the MAC address that you want to delete.

Step 3 Hold down Ctrl-S keys to delete the MAC address.

5.2.3 List Static Bridging Parameters

To display the static MAC entries, enter the **MAIN/CONF/BRIDGING/STATIC/LIST** menu.

5.3 Spanning Tree Protocol

The default setting of Spanning Tree Protocol (STP) function of the device is disabled. To enable it, please follow these steps.

Step 1 Enter the **MAIN/CONF/BRIDGING/STP/BRIDGE** menu.

- Spanning Tree: Enabled/Disabled (factory default: disabled)
- Priority (0-65535): **Priority** is used to define the bridging root

Step 2 Choose **Enabled** in the **Spanning Tree** field. After the spanning tree is enabled, it can operate normally without other adjustments.

Step 3 To further specify the bridge or port priority, keep on the following procedures.

Step 4 After choosing **Enabled** in **Spanning Tree** field, enter a value between 0~65535 in the **Priority** field.

Step 5 Go to the **MAIN/CONF/BRIDGING/STP/PORT** menu to configure the following fields.

- **Interface:** LAN /ATM1~16 (factory default: LAN)
- **Operation:** Enabled/ Disabled (factory default: Enabled)
- **Priority:** 128 (ranging from 0~255)

Step 6 Hold down Ctrl-S keys to save the parameters.

Step 7 Enter the **MAIN/WRITE** menu to write the new configurations into the flash memory.

Step 8 Enter the **MAIN/REBOOT** menu to reboot the system or reboot the system later.

5.4 Forwarding Table

To reach the bridging table where you can find the network status, enter the MAIN/UTIL/BRIDGING/LIST menu.

Chapter 6 Routing

The IP routing function of CT-520 is disabled by factory default. To enableit, enter the **MAIN/CONF/SYSTEM** menu, and select **Router** in the Operation Mode field (also described in Section 4.1.3). Then, you can configure RIP, static route, and ping test functions that are explained in this chapter.

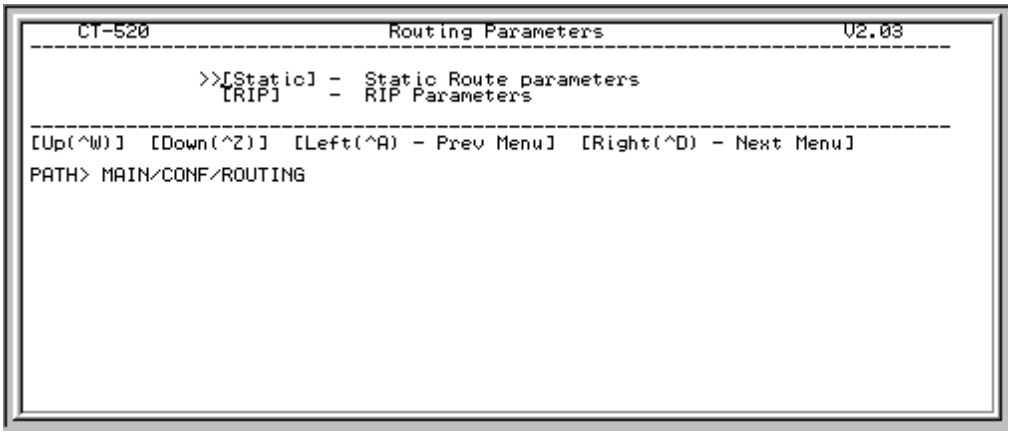


Figure 6–1 Configuring Routing Functions

6.1 RIP Configuration (CT-520 only)

Step 1 Enter the **MAIN/CONF/ROUTING/RIP/GENERIC** menu.

Step 2 There are two fields in the menu. Enter a parameter in each field.

- Mode: Disabled/Enabled
- Auto Summary: Select **Enabled** if you use RIP version 1.

Step 3 Hold down CTRL-S keys to save the change.

Now the RIP function is enabled. The default RIP parameter for each interface is RIPV1. In this default mode, the device can operate normally without other adjustments. If you want to configure advanced RIP functions, please continue the following procedures.

Step 4 Go to the **MAIN/CONF/ROUTING/RIP/INTERFACE/ATM** menu. There are ATM1 to ATM16 sixteen ATM interfaces.

Step 5 Enter one of these choices, e.g.,

MAIN/CONF/ROUTING/RIP/INTERFACE/ATM/ATM1.

Step 6 Enter a parameter in each field.

- Mode: Select **Enabled**
- Version: RIP version 2 or Version 1
- Authentication

  None: no authentication code is required.

  PlainText: an authentication code is required. You should also fill in the **Authentication Code** field to assign a password.
- Poison Reverse

  Disabled – Splitting Horizon

  Enabled – Poison Reverse enable.
- Authentication Code: Enter the password for authentication.

Step 7 Hold down CTRL-S keys to save the change.

6.2 Static Route Configuration

In this section, you will learn how to add the static route, delete the static route, and view the static route table of the CT-520. This function for the CT-320 is for remote access (e.g., web and Telnet access) only.

6.2.1 Add A Static Route

Step 1 Enter the MAIN/CONF/ROUTING/STATIC/ADD menu.

Step 2 Enter a parameter in each field.

- **Network/Host address:** Enter the network or host address of the destination
- **Subnet Mask:** Enter the mask of the IP network.
- **Gateway Address:** Enter the address of gateway.
- **Metric:** The maximum number of router(s) (1-15) through which the data packets must travel before reaching their destination.

Step 3 Hold down Ctrl-S keys to save the static route.

Note: the default route for network/host address and subnet mask are 0.0.0.0.

6.2.2 Delete A Static Route

Step 1 Enter the **MAIN/CONF/ROUTING/STATIC/DELETE** menu.

Step 2 Enter a parameter in each field.

- **Network/Host address:** Enter the destination with network or

host address

- **Subnet Mask:** Enter the subnet address of the IP network.
- **Gateway:** Enter the address of the gateway.

Step 3 Hold down CTRL-S keys to delete the static route.

6.2.3 List Static Routes

To view the static routes, enter the **MAIN/CONF/ROUTING/STATIC/LIST** menu.

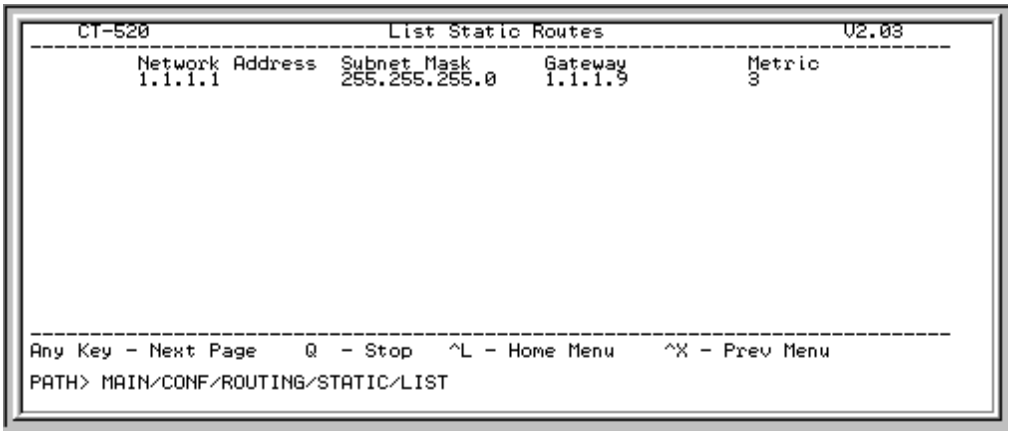


Figure 6–2 Static Routes

6.3 Routing Table

In order to validate the above RIP configuration for each interface, the device provides one utility function to access the routing table, where its directory is **MAIN/UTIL/ROUTING** menu.

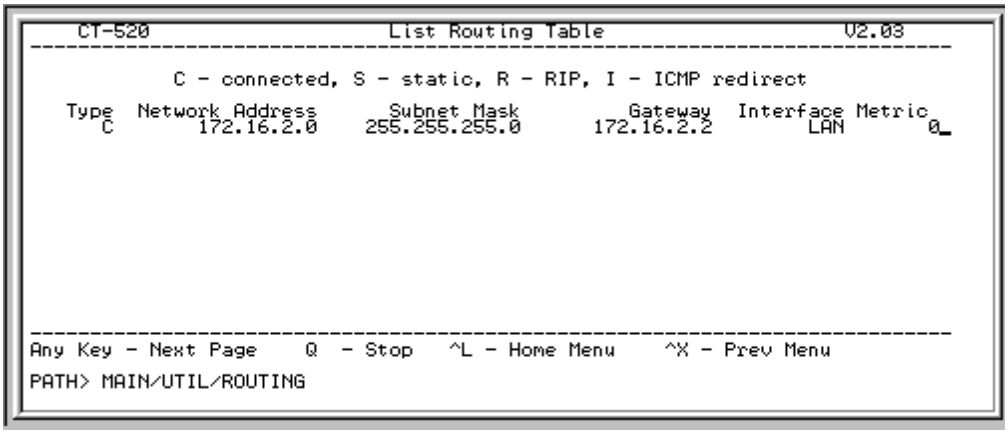


Figure 6–3 Routing Table

6.4 Ping Test Utility

Ping test is used to verify the status of the network connection after the above RIP or static route function is enabled. It sends a request message to the host and waits for a return message. This diagnostic function can verify if the remote host is reachable for Telnet or FTP purpose. It can also measure the roundtrip time to the remote host.

Step 1 Enter the **MAIN/UTIL/PING** menu.

Step 2 Enter a parameter in each field.

- **Network/Host address:** Enter network address or host address of the destination.
- **Data Size:** Enter the packet size for ping with a value between 32-1500.
- **Times:** Enter times of the ping test to be executed.

Step 3 Hold down CTRL-S keys to start the ping test.

Step 4 In a few minutes, the test result will be displayed.

- Ping Total: this indicates the time of test that is performed
- Ping Success: the number of the ping test that is successfully performed.
- Ping Fail: the number of the ping test that fails.
- Ping Average Time(ms): The average round-trip time of the test
- Ping Last Time(ms): the round-trip time of last ping test

Chapter 7 Network & Port Address Translation (CT-520 only)

7.1 Overview

Public IP addresses are registered and can be used within a public network, such as the Internet. Due to the limitation of IP version 4 address space and the growth of the Internet, the public addresses are becoming more scarce. One solution to this problem is by using private addresses in the small LANs and using Address Translation when accessing device on public network. CT-520 supports Port Address Translation (PAT) and Network Address Translation (NAT).

Note that private IP addresses that are not specified for NAT IP pool are factory pre-set to PAT IP pool with WAN global IP addresses.

7.2 Enable PAT/NAT

The following lists the required parameters for NAT/PAT function.

NAT	PAT
LAN network type: **Virtual**	LAN network type: **Virtual**
ATM network type: **Global**	ATM network type: **Global**
Private/Global pool translation: **NAT**	Private/Global pool translation: **PAT**

Table 7–1 NAT/PAT Parameters

Step 1 Enter the **MAIN/QC/LAN** menu.

Step 2 Enter a parameter in each field.

- **IP address:** Enter the reserved private network address for the LAN interface. The default IP address is 210.65.231.206.
- **Subnet Mask:** Enter the mask of the IP network. The default subnet mask is 255.255.255.0.
- **Network Type: S**elect the **Virtual** mode.

Step 3 Hold down CTRL-S keys.

Step 4 Enter the **MAIN/CONF/SYSTEM** menu.

Step 5 Select **Router** in the Operation Mode field.

Step 6 Hold down CTRL + S keys.

Step 7 Enter the **MAIN/CONF/NAT** menu to set the NAT/PAT parameters. Refer to Section 7.3 and 7.4 to configure these parameters.

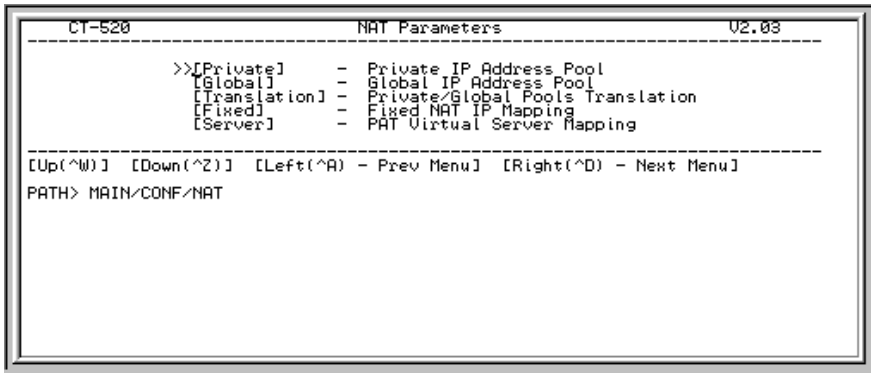


Figure 7–1 Configuring NAT/PAT functionality

Note: reserved private IP address range

- Class A: 10.0.0.0 ~ 10.255.255.255
- Class B: 172.16.0.0 ~ 172.31.255.255
- Class C: 192.168.0.0~192.168.255.255

7.3 PAT Virtual Server

If you want to set up Internet servers in the virtual LAN when PAT is enabled, you should register the servers with the device first, and then Internet users can access the service via ATM interface of SDSL device. This section will guide you to configure a virtual server.

7.3.1 Add Virtual Server Entry

Step 1 Enter the **MAIN/CONF/NAT/SERVER/ADD** menu.

Step 2 Enter a parameter in each field.

- **Protocol**: TCP or UDP (factory default: TCP)
- **Interface**: LAN, Any and ATM1 ~ ATM16. The factory default is ANY. Specify the interface via which the server provides service to. If **ANY** is selected, any of the interfaces can access the service.
- **Service Name:** it is used for operator to recognize the service that the virtual server provides. You can define the service name as web, e-mail, ftp and so on**.**
- **Service Port Number:** it is related to service port, i.e. well-known port of web server 80, ftp server 21, and smtp 25.
- **Private IP Address**: define a private IP address of the virtual server.
- **Private Port Number:** specify the actual port of the server in the virtual LAN. You can set it the same as service port number.

Step 3 Hold down Ctrl-S keys to save the new configurations.

7.3.2 Delete Virtual Server

To delete a virtual server entry, follow the steps.

Step 1 Enter the **MAIN/CONF/NAT/SERVER/DELETE** menu.

Step 2 Enter the following parameters of the virtual server.

- **Protocol**: TCP and UDP (factory default: TCP)
- **Interface**: LAN, and ATM1 ~ ATM16. If the virtual server is located at the same LAN interface of the SDSL device, then select **LAN**. If virtual server is located at the same SDSL interface, then select one of ATM1 ~ ATM16.
- **Service Port Number:** it is related to the service name. For example, web with port number 80.

Step 3 Hold down Ctrl-S keys to delete the virtual server.

7.3.3 List Virtual Server Entry

To display the virtual server entry, enter the **MAIN/CONF/NAT/SERVER/LIST** menu.

7.4 Configure NAT/PAT IP Pools

This section specifies how to configure the device to do one-to-one, virtual-to-global IP address translation.

Step 1 Assign the private IP addresses. Refer to Section 7.4.1.

Step 2 Assign the global IP addresses. Up to five sets of continuous global IP addresses are supported. The workstations in the private IP pools will be translated to one of the global IP address that is set in Section 7.4.2.

Step 3 Map the private IP pool to the global IP pool for NAT/PAT functionality. Refer to Section 7.4.3.

Step 4 Assign fixed IP address. Refer to Section 7.4.4.

Step 5 Write the configurations in the flash memory by entering MAIN/WRITE menu.

Step 6 Reboot the system by entering MAIN/REBOOT.

Note: Except those configured in the NAT virtual IP address pools, other hosts in the virtual LAN will perform the PAT functionality when the packets are transmitted through the SDSL device.

7.4.1 Private IP Address

Step 1 Enter the **MAIN/CONF/NAT/PRIVATE** menu.

Step 2 Enter the following parameters. Maximum five IP address pools can be configured.

- Pool Number: Pool 1 ~ Pool 5
- Start IP Address
- End IP Address

For example, in a LAN, there are two sets of IP addresses. The first ranges from 210.25.231.1 to 210.25.231.20 and the second from 210.25.231.100 to 210.25.231.200.

To configure the first set of IP addresses, assign it to Pool 1. Appoint 210.25.231.1 at the Start IP Address field and 210.25.231.20 at the End IP Address field. Then assign 210.25.231.100 to 210.25.231.200 to Pool 2 in the same way.

Step 3 Hold down Ctrl-S keys.

7.4.2 Global IP Address

Step 1 Enter the **MAIN/CONF/NAT/GLOBAL** menu.

Step 2 Enter the following parameters. Maximum five IP address pools can be configured.

- Pool Number: Poo1 ~ Pool 5
- Start IP Address
- End IP Address

Step 3 Hold down Ctrl-S keys.

7.4.3 Private/Global IP Pool Mapping

You can specify a private IP pool to a global pool for PAT or NAT mapping.

Add Pool Translation

Step 1 Enter the **MAIN/CONF/NAT/TRANSLATION/ADD** menu.

Step 2 Enter a parameter in each field.

- Private IP Pool: press Tab key to select a private pool number
- Global IP Pool: press Tab key to select a global pool number
- Translation Type: press Tab key to select a type, NAT or PAT.

Step 3 Hold down Ctrl-S keys.

Delete A NAT/PAT Pool Translation

Step 1 Enter the **MAIN/CONF/NAT/TRANSLATION/DELETE** menu.

Step 2 Enter a parameter in each field.

- Private IP Pool: press Tab key to select a private pool number
- Global IP Pool: press Tab key to select a global pool number
- Translation Type: press Tab key to select a type, NAT or PAT.

Step 3 Hold down Ctrl-S keys to delete it.

List NAT/PAT Pool Translation

To display the NAT Pool Translation, enter the **MAIN/CONF/NAT/TRANSLATION/LIST** menu. You can find the mapping of NAT pool.

7.4.4 Fixed IP Address Mapping

Fixed IP address function is used for mapping between selected Global IP address and private IP address. Each private IP address is mapped to a global IP address via which the data is received and transmitted.

Step 1 Enter the **MAIN/CONF/NAT/FIXED** menu. In this menu, you can add, delete or view the fixed private and globa1 address.

Step 2 Hold down Ctrl-S keys to delete the IP address.

Chapter 8 DNS Proxy (CT-520 only)

8.1 Overview

A Domain Name Server (DNS) provides an IP address to a host computer for an applied Domain Name. The device supports DNS proxy feature that receives and attempts to find an entry in its local tables and when one is not found, forward the request to remote server.

8.2 Configure DNS Proxy

The default setting for DNS Proxy is disabled. To enable it, please go through the following procedures.

Step 1 Enter the **MAIN/CONF/DNS** menu.

Step 2 Enter a parameter in each field.

- **DNS proxy:** Enabled/ disabled (factory default: disabled)
- **Primary Server IP address:** Enter the primary server IP address. This is the top priority.
- **Secondary Server IP address:** Enter the secondary server IP address that will be used immediately when primary server IP address fails or is not available.

Step 3 Hold down Ctrl-S keys.

Chapter 9 DHCP (CT-520 only)

9.1 Overview

Dynamic Host Configuration Protocol (DHCP) is designed to provide a centralized approach to configure the IP address and parameters.

When a workstation is configured for automatic IP address assignments, it broadcasts a request on to the LAN. The device plays a role as DHCP Server and responds with:

- An IP address and subnet mask for the workstation.
- The Domain name, which is the same as that in MAIN/CONF/SYSTEM.
- The IP addresses of the default router, two DNS servers.

9.2 Configure DHCP

Step 1 Enter the **MAIN/CONF/DHCP/GENERIC** menu.

Step 2 Enter a parameter in the following fields.

- **DHCP Server:** Enabled/Disabled (factory default: Disabled)
- **DHCP start IP:** Enter the DHCP server start IP address
- **DHCP End IP:** Enter the DHCP server end IP address
- **Default Gateway:** this is one entry on the LAN that packets are received or transmitted
- **Subnet mask:** Enter the mask of the IP network
- **Domain Name Server (1):** Enter the IP address of the primary domain name server. This is the top priority.
- **Domain Name Server (2):** Enter the IP address of the secondary domain name server that will be used when primary server IP address fails or is not available.

Step 3 Hold down Ctrl-S keys to save the new configuration.

Chapter 10 SNMP

The device supports SNMP (Simple Network Management Protocol) management. MIBs of MIB II and SDSL Forum TR006 are implemented. The default settings for read-only/ read-write communities are **public** and **private**. This section will tell you how to change the default community and add the trap destinations. Up to five trap destinations are available in the system.

Step 1 Enter the **MAIN/CONF/SNMP** menu. Go through Section 10.1 ~10.2 to configure community and trap functions.

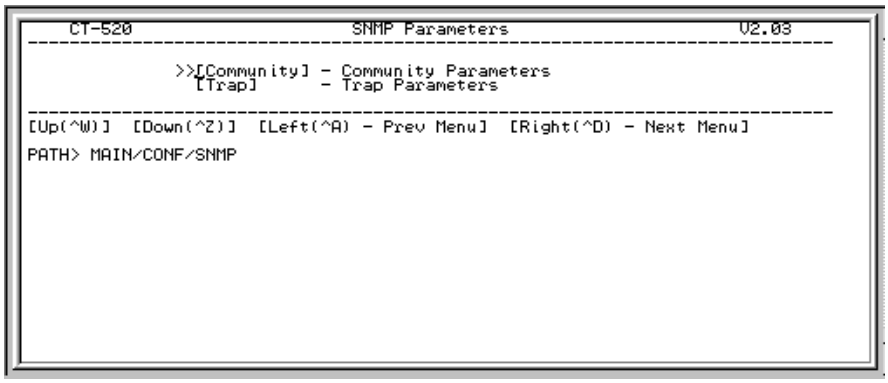


Figure 10-1 SNMP Parameters

Step 2 Go through Section 10.1 to set the community parameters or Section 10.2 to set the trap parameters.

10.1 Community

Step 1 Enter the **MAIN/CONF/SNMP/COMMUNITY** menu.

Step 2 Enter a parameter in each field.

- Read-Only Community- enter the password for read-only access
- Read-Write Community- enter the password for read-write access

Step 3 Hold down Ctrl-S keys to save the new configuration.

10.2 Trap

10.2.1 Add A Trap Destination Entry

Step 1 Enter the **MAIN/CONF/SNMP/TRAP/ADD** menu.

Step 2 Enter a parameter in each field.

- Version: Version 1/Verion2
- Destination IP- the destination IP address
- Community: enter a parameter for the community

Step 3 Hold down Ctrl-S keys to save the new configuration.

10.2.2 Delete A Trap Destination Entry

Step1 Enter **MAIN/CONF/SNMP/TRAP** menu.

Step 2 Enter a parameter in each field to delete a trap destination entry.

- Version: Version 1/Verion2
- Destination IP- enter the destination IP
- Community: enter a parameter for the community.

Step 3 Hold down Ctrl-S keys to delete the trap destination entry.

10.2.3 List Trap Destination Entries

To display trap destination entries, enter the **MAIN/CONF/SNMP/TRAP/LIST** menu.

Chapter 11 Maintenance

11.1 Load Factory Default Values

Step 1 Enter the **MAIN/DEFAULT** menu.

Step 2 The screen displays the following message.

"This will set system parameters to factory default !(Y/N)."

Step 3 Type **"Y"** key. The system will proceed to restore the default configurations.

Step 4 After the default values are restored, the following message displays.

"Set system parameters to factory default! Press any key to return to previous menu ..."

Step 5 Press **ESC** to return to previous menu.

Step 6 Enter the **MAIN/WRITE** menu to write the configurations to the flash memory.

Step 7 Enter the **MAIN/REBOOT** menu to reboot the system.

11.2 Write System Configurations

When you hold down Ctrl-S keys, you only save the parameters into RAM. RAM stores the configurations temporarily, and these parameters are lost after the system is quit or reboot. To save them permanently, you should write the configurations into flash memory and reboot the system.

Step 1 Enter the **MAIN/WRITE** menu.

Step 2 The screen will display "This will write configurations to flash (Y/N)." Type **"Y"**.

Step 3 After the system completes, the following message displays, ***"Write configuration to flash complete! Press any key to return to previous menu ..."***

Press any key to return to the main menu.

Step 4 Reboot the system.

11.3 Reboot System

After the parameters are written in the flash memory, you should reboot the system to make the new parameters effective. Reboot is the same as power off and power on.

Step 1 Start from the main menu and select **REBOOT.**

Step 2 Enter the **MAIN/REBOOT** menu. It will prompt a message ***"This will reboot the system? (Y/N)."***

Step 3 Type **"Y"** to reboot the system, or **"N"** if not.

11.4 Software Upgrade

The device utilizes TFTP protocol to upgrade the device firmware. If there is a new firmware, follow the steps to upgrade the device.

Step 1 Enter the **MAIN/UTIL/TFTP** menu.

Step 2 Enter a parameter in the following fields.

- TFTP Server IP Address:
- File Name: The file name used for the configuration parameters.
- TFTP option: Choose ***Download***
- Application Type: Choose ***Firmware***

Step 3 Hold down Ctrl-S keys to download the software from the TFTP server.

Step 4 When download completes, the system will prompt ***"Transfer Completed! Upgrade now?(Y/N)."*** Press **Y** key to start upgrading the software with the new file.

Step 5 When the new firmware is upgraded, the screen will display the message, ***"Upgrade completed! Press any key to continue."***

Therefore, press any key as instructed.

Step 6 You have successfully upgraded the device firmware now.

11.5 Configuration Backup and Restoration

The device utilizes TFTP protocol to back up and restore the current configuration parameters. The administrator may save the configuration parameters as a file and retrieve it later. To do the functionality, you can set up a TFTP server, which can be LAN-connected or WAN-connected to the device. After that, keep on the following steps.

11.5.1 Configuration Backup

The configuration backup function is used to save the current system parameters as a file. To do this, follow the steps.

Step 1 Enter the **MAIN/UTIL/TFTP** menu.

Step 2 Enter a parameter in the following fields.

- TFTP Server IP Address:
- File Name: The file name used for the configuration parameters.
- TFTP option: Choose ***Upload***
- Application Type: Choose ***Configuration***

Step 3 Hold down CTRL-S keys to start uploading the file to the TFTP server.

Step 4 When the upload completes, the system will prompt, ***"Configuration Upload Completed! Press any key to continue."***

Step 5 Press any key to exit the menu. You have succesfully upload the configuration now.

11.5.2 Configuration Restoration

To retrieve the configuration parameters, follow the steps.

Step 1 Start from the **MAIN/UTIL/TFTP** menu.

Step 2 Enter a parameter in the following fields.

- TFTP Server IP Address:
- File Name: The file name of the configuration parameters.
- TFTP option: Choose ***Download***
- Application Type: Choose ***Configuration.***

Step 3 Hold down CTRL-S keys to start downloading the file.

Step 4 When the restoration completes, the system will prompt ***"Configuration Restoration Completed! Press any key to continue."***

Step 5 Press any key to exit the menu. You have succesfully restore the configuration now.

11.6 Performance Monitoring

Enter MAIN/MON/ATM menu. You can monitor the following status.

- SHDSL Status Monitor
- ATM Interface Monitor
- SHDSL Performance Statistics
- Interface Performances Statistics

11.6.1 SHDSL Status Monitor

You can find the SHDSL status from **MAIN/MON/STATUS** menu. The following information is provided.

- Terminal Type : CO or CPE
- Operate State

  There are five operate modes that represent different states of the session: idle, handshake, PMMS (Power Measurement Modulation Session), training, and data. The PMMS mode does not exit when fixed data rate is set. A correct process to establish the session will go through idle, handshake, PMMS, training, and data. Data state means the session is established.
- Bit Rate(Actual) : the current data rate (Nx64 Kbps + Ix8 Kbps , refer to 4.3 SHDSL Characteristics)
- Indicator :the error that is detected at the moment.

11.6.2 ATM Interface Monitor

You can find the ATM interface status from the **MAIN/MON/ATM** menu. In the menu, the status of ATM1~ATM16 are listed.

- Interface (ATM1 to ATM16)
- IP/Mask address
- VPI/VCI
- Encapsulation
- PCR or SCR
- Protocol
- Status: disable, up (the interface is ready for transmission) or down (the interface is not ready for transmission)

11.6.3 SHDSL Performance Statistics

You can monitor the SDSL line performance from the **MAIN/MON/SHDSLPERF** menu. In the menu, the statistics of the SDSL line performance are recorded. You can reset the items marked **since reset** by holding down Ctrl-T keys.

- Line Attenuation (dB) - Current attenuation
- Noise margin (dB) - Current noise margin
- CRC (since reset) - the cumulative statistics of seconds since last reset when there is CRC error in the proceeding superframe.
- ES (since reset) - the cumulative stastistics of Errored Seconds since last reset.
- SES (since reset) - the cumulative stastistics of Severely Errored Seconds since last reset.
- LOSWS (since reset) - the cumulative stastistics of Loss of Sync Word Second since last reset.
- UAS (since reset)- the cumulative stastistics of Unavailable Seconds since last reset.
- CRC (Current 15 min/Current 1 day) - the cumulative statistics of CRC error seconds for the current 15 minutes or 1 day.
- ES (Current 15 min/Current 1 day) - the cumulative stastistics of Errored Seconds for the current 15 minutes or 1 day.
- SES (Current 15 min/Current 1 day) - the cumulative stastistics of Severely Errored Seconds for the current 15 minutes or 1 day.
- LOSWS (Current 15 min/Current 1 day) - the cumulative stastistics of Loss of Sync Word Failure when there is Loss of Signal for the current 15 minutes or 1 day.
- UAS (Current 15 min/Current 1 day)- the cumulative stastistics of Unavailable Seconds for the current 15 minutes or 1 day.

For more details of the above errors, please refer to G.992.2 (G.shdsl).

11.6.4 Interface Performance Statistics

You can monitor the interface performance statistics of LAN & ATM1~ATM16 from the **MAIN/MON/INTRPREF** menu. You can reset the items marked **since reset** by holding down Ctrl-T keys.

- Interface- LAN or ATM interface
- Transmitted packets (since reset): the transmitted packets since last reset
- Received packets (since reset): the received packets since last reset
- Received errors (since reset): the received errors since last reset

a. The following explains the possible received errors that may occur in WAN interface.

HEC error: A received HEC error happens to at least one cell of the frame.

ABORT error: A frame abort is detected.

Receive Length error (LN): The number of octets received in the frame does not match the length specified in the length field of the AAL5 CPCS-PDU.

CRC error (CR): A frame with CRC error is received.

b. The following explains the conditions of received errors that may occur in LAN interfaces.

Receive Frame Length Violation (LG): a frame length exceeds the maximum defined is received.

Receive noneoctect-aligned frame (NO): a frame containing a number of bits not visible by eight is received.

Short Frame (SH): a frame less than the minimum defined is received.

CRC error (CR): a frame with CRC error is received

Overrun: When Overrun occurs, the received byte will be written over the previous byte. The previous byte and frame status are lost.

Collision (CL): a frame is closed because a collision occurs during frame receipt.

- Received rate (bps): the receive rate of the interface
- Transmit/Receive rate (bps): the transmit/receive rate of the interface
- Status of the interface - disable, up (the interface is ready for transmission) or down (the interface is not ready for transmission)

Chapter 12 Web Configuration

This chapter introduces how to manage the device via web browser. The web management is enabled by factory default. To disable it, enter the console or Telnet and go to **MAIN/CONF/HTTPD**. It is suggested to read the web page with display of 1024x768 or 800 x600 resolution.

12.1 Logging on to Web

Step 1 Start your Internet browser.

Step 2 Enter the IP address of the device in the web address field. For example, the IP address is 210.65.231.205. Enter http://210.65.231.205.

The default LAN IP address is 210.65.231.65.

Step 3 You will be requested to enter user name and password. Type the password that is set in console (refer to Section 3.1.1). Or if the password is not changed, type the default passwords. The default ADMINISTRATOR password is **root**, and USER password is **user**.

Step 4 After successfully logging in, you will reach a major configuration page.

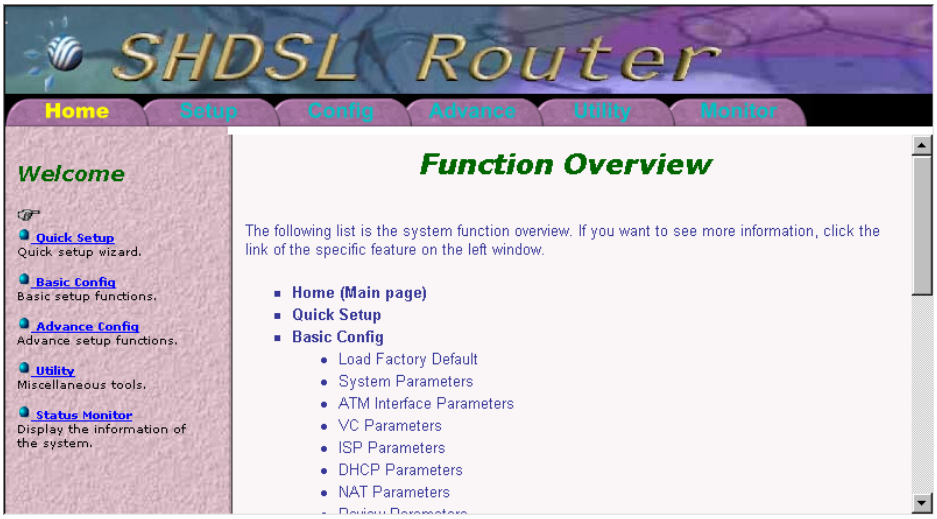


Figure 12-1 Web Main Menu

On the above page, there are three basic areas. The first is the main menu on the top. It includes these items, **Home, Setup, Config, Advance,**

Utility, and **Monitor.** The second is the sub-menu located on the left side that displays after the operator selects an item from the main menu. The third in the middle of the page is the area that will display the parameters or explanations of the sub-menu.

12.2 Operation

The web page follows a tree-structured design. Being familiar with the console/Telnet control would be helpful to get used to the web operation.

The web configuration uses a step-by-step method that familiarizes the operator to configure the SDSL device. On-screen explanations of each function or parameters are provided to help the user know what is being doing and what can be processed next.

During the operation, there are some buttons used to achieve the configurations.

	Button	**Function**
1	Next	To go to the following step or next page
2	Back	To return to the previous page
3	Reset	If the parameters are changed, click this button to restore the original parameters
4	Cancel	To stop and quit the current page without changing any setting
5	Finish	To accept the setting or when a status table is finished reading, click this button to exit the page
6	OK	To confirm the setting when a parameter is inserted or changed.
7	Modify	To modify the parameters.
8	Add	To add an item in a list, like MAC entry or a static rout entry by clicking the Add button after inserting the required parameters. Click Finish when the “ADD” action is completed.

12.2.1 Quick Setup

The device can function normally after the quick setup. **Setup** link is a quick configuration for the operator to easily customize the device for application.

Step 1 Click the **Setup** button. A quick setup wizard displays and teaches the administrator how to configure the device at this stage.

Figure 12-2 Quick Setup

Step 2 Follow the five steps described in the quick setup wizard. Press the **Next** button when a step is completed to go on the next step until all steps are completed.

Step 3 In the last step (Step 5), the page will display all the adjusted settings that the administrator can review.

Step 4 Click the **Finish** button to confirm the settings.

Step 5 The system will prompt the administrator to save (write) the configurations into the system flash memory and then restart the system to make the new parameters functional. Click the Save button and then the Restart button as instructed.

12.2.2 Basic Configuration

At this stage, you can perform the following configurations.

- Load Factory Default
- System Parameters
- ATM Interface Parameters
- VC Parameters
- ISP Parameters
- DHCP Parameters
- NAT Parameters
- Review Parameters
- Save and Restart

Step 1 Click the **Config** button. There is a basic configuration description displaying on the page that teaches the operator how to configure at this stage.

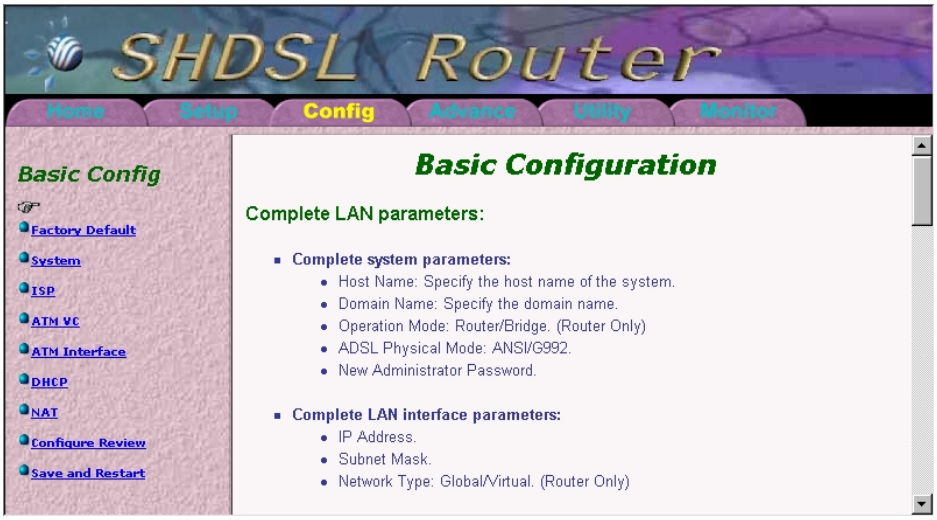


Figure 12-3 Basic Configuration

Step 2 The administrator can set the configurations to factory default settings or configure the other functions by following the online explanations.

Step 3 After the parameters are set up, the page will display all the adjusted settings for the administrator to review.

Step 4 Click the **Finish** button to confirm the settings.

Step 5 The system will ask the administrator to save (write) the configurations into the system flash memory and then restart the system to make the new parameters effective. Click the **Save** button and then the Restart button as instructed.

12.2.3 Advance Configuration

On the **Advance** page, you can do the following configurations.

- Static Route Parameters
- RIP Parameters (Router Only)
- Transparent Bridging Parameters
- SNMP Parameters
- TFTP Parameters
- Basic system parameters
- Save and Restart

Step 1 Click the **Advance** button. The **Advance Configuration** page will describe how to configure the SDSL device at this stage.

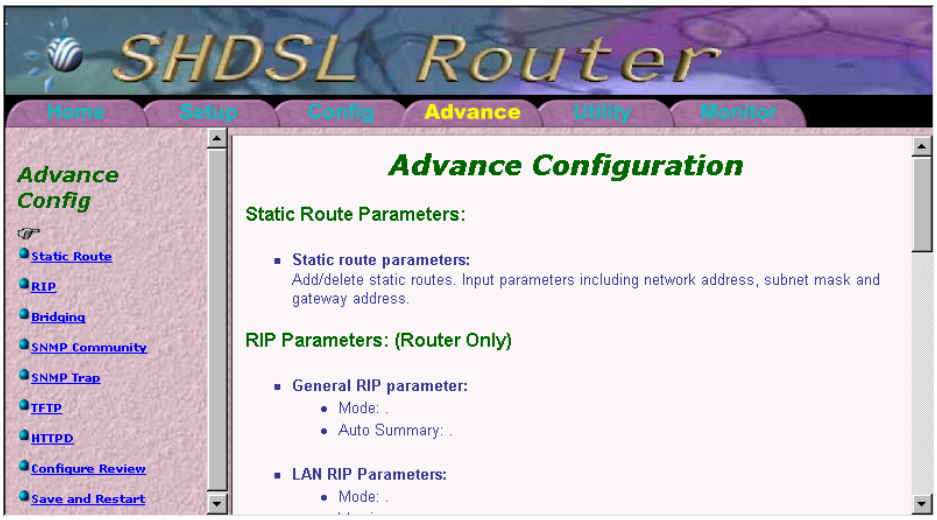


Figure 12-4 Advance Configuration

Step 2 Following the online explanations to complete the setting.

Step 3 After the parameters are set up, the page will display all the adjusted settings for the administrator to review the settings.

Step 4 Click **Finish** button to confirm the settings.

Step 5 The system will prompt the administrator to save (write) the configurations into the system flash memory and then restart the system to make the new parameters effective. Click the Save button and then Restart button as instructed.

12.2.4 Utility

On the **Utility** page, you can perform the following utilities.

- **Ping Test**
  Use this function to test specific network connection.
- **Routing Table Utility**
  Use this function to see the routes of the system.
- **Forwarding Table Utility**
  Use this function to see the forwarding table of the system.
- **TFTP Application**
- **Save and Restart**

  Perform this function to save adjusted configuration to the flash memory and make it effective after restart.

12.2.5 Monitor

On the **Monitor** page, you can perform the following functions.

- System information

  System Name.

  Firmware Version.

  Hardware Information.

  System Time.
- **SHDSL Status Monitor**
- **ATM Interface Monitor**
- **SHDSL Performance Statistics**

  Line Attenuation and Noise Margin

  CRC/ES/SES/LOSWS/UAS
- **Interface Performance Statistics**

  Transmitted and Received Packets

  Transmitted and Received Rates

12.2.6 Incorrect Setting

When an incorrect parameter is input, the system will inform that the parameter is not right and will request a correction.

12.3 Upgrading Homepage

The homepage image file is pre-downloaded in the system by factory default. If there is a new version to upgrade, the administrator must do it in the console or Telnet mode. Follow the steps to upgrade it.

Step 1 Enter the **MAIN/UTIL/TFTP** menu.

Step 2 Enter a parameter in the following fields.

- TFTP Server IP Address:
- File Name: The file name used for the configuration parameters.
- TFTP option: Choose ***Download***
- Application Type: Choose ***Homepage***

Step 3 Hold down Ctrl-S to start downloading the file from the TFTP server.

Step 4 When the download is completed, the screen will prompt **"Transfer Completed! Upgrade now?(Y/N)."** Press **Y** key to upgrade the homepage with the new file.

Step 5 After the new firmware version is upgraded, the screen displays **"Upgrade completed! Press any key to continue."**

Therefore, press any key as instructed.

Step 6 You have successfully upgraded the homepage.

Appendix

Index of Console/Telnet

LEVEL1	LEVEL2	LEVEL3	LEVEL4	LEVEL5	LEVEL6	Default Value
QC	LAN		NETWORK TYPE			GLOBAL
			IP ADDRESS			210.65.231.206
			SUBNET MASK			255.255.255.0
	ATM	ATM1~ATM16	INTERFACE			ENABLED
			PROTOCOL			ETHERNET
			IPCP			STATIC
			ISP			ISP1
			NETWORK TYPE			GLOBAL
			ATM VC			VC1
			IP ADDRESS			210.65.231.206
			SUBNET MASK			255.255.255.0
	VC	VC1~VC16	VPI/VCI			0/33
			AAL5 ENCAPSULATION			LLC
			VC QOS			CBR
			PEAK CELL RATE			65000
			SUSTAINABLE CELL RATE			0
			BURST TOLERANCE			0
	ISP	ISP1~8	ISP NAME			
			USER NAME			
			PASSWORD			
CONF	DEFAULT					
	SYSTEM		HOST NAME			SDSLR
			OPERATION MODE			BRIDGE
			CONSOLE PASSWORD CHECK			DISABLED
			TERMINAL TYPE			CO
			NEW ADMINISTRATOR PASSWORD			
			RETYPE PASSWORD			

			NEW USER PASSWORD			
			RETYPE PASSWORD			
	INTERFACE	LAN	NETWORK TYPE			GLOBAL
			IP ADDRESS			215.65.231.206
			SUBNET MASK			255.255.255.0
		ATM	ATM1~ATM16	INTERFACE		
				PROTOCOL		ETHERNET
				IPCP		STATIC
				ISP		ISP?
				NETWORK TYPE		GLOBAL
				ATM VC		VC?
				IP ADDRESS		
				SUBNET MASK		
	ISP	ISP1~8		ISP NAME		
				USER NAME		
				PASSWORD		
	NAT	PRIVATE		POOL NUMBER		POOL 1
				START IP ADDRESS		
				END IP ADDRESS		
		GLOBAL		POOL NUMBER		POOL 1
				START IP ADDRESS		
				END IP ADDRESS		
		TRANSLATION	ADD	PRIVATE IP POOL		POOL 1
				GLOBAL IP POOL		POOL1
				TRANSLATION TYPE		NAT
			DELETE	PRIVATE IP POOL		POOL 1
				GLOBAL IP POOL		POOL1
				TRANSLATION TYPE		NAT
			LIST	PRIVATE IP POOL		
				GLOBAL IP POOL		
		FIXED	ADD	PRIVATE IP ADDRESS		
				GLOBAL IP ADDRESS		
			DELETE	PRIVATE IP		

				ADDRESS		
				GLOBAL IP ADDRESS		
			LIST	PRIVATE IP ADDRESS		
				GLOBAL IP ADDRESS		
		SERVER	ADD	PROTOCOL		TCP
				INTERFACE		ANY
				SERVICE NAME		
				SERVICE PORT NUMBER		
				PRIVATE IP ADDRESS		
				PRIVATE PORT NUMBER		
			DELETE	PROTOCOL		TCP
				INTERFACE		ANY
				SERVICE PORT NUMBER		
			LIST	PROTOCOL		
				PRIVATE IP		
				PRIVATE PORT		
				SERVICE PORT		
				INTERFACE		
	DHCP	GENERIC	DHCP SERVER			DISABLED
			DHCP START IP			
			DHCP END IP			
			DEFAULT GATEWAY			
			SUBNET MASK			
			DOMAIN NAME SERVER(1)			
			DOMAIN NAME SERVER(2)			
		FIXED	ADD	MAC ADDRESS		
				IP ADDRESS		
			DELETE	MAC ADDRESS		
			LIST	IP ADDRESS		
				MAC ADDRESS		
	DNS			DNS PROXY		DISABLED
				PRIMARY SERVER IP ADDRESS		
				SECONDARY SERVER IP ADDRESS		
	SNMP	COMMUNITY		READ-ONLY COMMUNITY		PUBLIC
				READ-WRITE		PRIVATE

				COMMUNITY		
		TRAP	ADD	VERSION		VERSION 1
				DESTINATION IP		
				COMMUNITY		
			DELETE	VERSION		VERSION 1
				DESTINATION IP		
				COMMUNITY		
			LIST	VERSION		
				DESTINATION IP		
				COMMUNITY		
	TFTP			SERVER IP ADDRESS		
				FILE NAME		
	VC	VC1~VC16		VPI/VCI		0/33
				AAL5 ENCAPSULATIO N		LLC
				VC QOS		UBR
				PEAK CELL RATE (BPS)		864000
				SUSTAINABLE CELL RATE (BPS)		0
				BURST TOLERANCE (MSEC)		0
	ROUTING	STATIC	ADD	NETWORK/HOS T ADDRESS		
				SUBNET MASK		
				GATEWAY ADDRESS		
				METRIC		
			DELETE	NETWORK/HOS T ADDRESS		
				SUBNET MASK		
				GATEWAY ADDRESS		
			LIST	NETWORK/HOS T ADDRESS		
				SUBNET MASK		
				GATEWAY ADDRESS		
				METRIC		
		RIP	GENERIC		MODE	DISABLED
					AUTO SUMMARY	ENABLED
			INTERFACE	LAN	MODE	DISABLED
					VERSION	2
					AUTHENTICATION	NONE

					POISON REVERSE	DISABLED
					AUTHENTICATION CODE	
				ATM (ATM1~ATM16)	MODE	ENABLED
					VERSION	2
					AUTHENTICATION	NONE
					POISON REVERSE	ENABLED
					AUTHENTICATION CODE	
	BRIDGING	STATIC		ADD	MAC ADDRESS	
					PORT MAP	
				DELETE	MAC ADDRESS	
				LIST	MAC ADDRESS	
					OPERATION	
		STP	BRIDGE		SPANNING TREE	DISABLED
					PRIORITY	32768
			PORT		INTERFACE	LAN
					OPERATION	ENABLED
					PRIORITY	128
	HTTPD				WEB SERVER	ENABLED
	SDSL				MINIMUM BASE RATE(1-36)	1
					MAXIMUM BASE RATE(1-36)	36
					MINIMUM SUB RATE(0-1)	0
					MAXIMUM SUB RATE(0-1)	1
					POWER BACK OFF	ENABLED
					REMOTE	DISABLED
MON	STATUS				TERMINAL TYPE	CO
					OPERATE STATE	
					BIT RATE (ACTUAL)	
					INDICATOR	
	ATM				INTERFACE	
					IP/MASK	
					VPI/VCI	
					ENCASULATION	
					PCR OR SCR	
					PROTOCOL	
					STATUS	
	SDSLPERF				LINE ATTENUATION	
					NOISE MARGIN	
					CRC	
					ES (SINCE RESET, CUURENT 15 MIN/ 1DAY)	
					SES (SINCE RESET, CUURENT 15 MIN/	

					1DAY)	
					LOSWS (SINCE RESET, CUURENT 15 MIN/ 1DAY)	
					UAS (SINCE RESET, CUURENT 15 MIN/ 1DAY)	
	INTRPREF				INTERFACE	
					TXPKTS	
					RXPKTS	
					EXERRORS	
					TX RATE (BPS)	
					RXRATE(BPS)	
					STATUS	
UTIL	TFTP	TFTP SERVER IP ADDRESS				
		FILE NAME				
		TFTP OPTION				DOWNLOAD
		APPLICATION TYPE				FIRMWARE
	PING	HOST IP ADDRESS				
		DATA SIZE				32
		TIMES				4
	ROUTING	TYPE				
		NETWORK ADDRESS				
		SUBNET MASK				
		GATEWAY				
		INTERFACE				
		METRIC				
	BRIDGING	S-STATUC				
		D-DYNAMIC				
		0-FILTER				
		1-FORWARD				
		2- DYNAMIC				
SYS		SYSTEM NAME				
		MODEL				
		FIRMWARE VERSION				
		CPU				
		SYSTEM CLOCK				
		RAM				
		FLASH				
		SDSL CHIPSET				
		ELAPSED TIME				
WRITE						

REBOOT						
QUIT						

Specifications

- **WAN interface (one SDSL port)**

Item	Specifications
SDSL standard	ITU-T G.991.2 (G.shdsl)
Line rate	80K to 2320 Kbps
Data rate	N*64 Kbps, N=1~36

- **ATM attributes**

Item	Specifications
PPP over AAL5	RFC2346 (CT-520 only)
Multi-protocol over AAL5	RFC-1483 Bridge
	RFC-1483 Route (CT-520 only)
VCs	16
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI 3.1 PVC
OAM F4/F5	Yes

- **Management**

Item	Specifications
Console port	RS232/DB9
SNMP	Yes
Telnet	Yes
Web-based management	Yes
Configuration backup and restoration	Yes
LED indicators	Power, Alert, LAN status, SDSL status

- **Local interface (One Ethernet port)**

Item	Specifications
Standard	IEEE 802.3 10Base-T
Transparent bridging and learning	Yes

■ **Routing functions (CT-520 only)**

Item	Specifications
IP static route	Yes
RIP and RIPv2	Yes

■ **Network functions (CT-520 only)**

Item	Specifications
ARP	Yes
DNS, NAT/PAT, DHCP/BOOTP	Yes
PAP, CHAP	Yes

■ **Power supply**

Item	Specifications
External power adapter	110VAC or 220VAC

■ **Environmental conditions**

Item	Specifications
Operating temperature	0 to 40 degrees Celsius
Relative humidity	5% to 90% (non-condensing)

■ **Dimension**

Item	Specifications
Height x Width x Depth	40mm x 200mm x 140 mm

Trouble Shooting

<table>
<tr><td>1</td><td colspan="2">Parameters are lost after restart</td></tr>
<tr><td></td><td colspan="2">Before you terminate the access or reboot the device, you should save the configurations into the flash memory by entering the MAIN/WRITE menu and then reboot the system by entering the MAIN/REBOOT menu. If this procedure is not done, the parameters you change will be lost.</td></tr>
<tr><td>2</td><td colspan="2">Console/Telnet/Web Passwords</td></tr>
<tr><td></td><td colspan="2">According to default setting, the console password check function is disabled; it is not necessary to enter passwords during console access. But to access Telnet or Web, you will be requested to enter a password. You can try the default passwords to log in, but it is only valid when it is not changed to a new one.
■ Read-write access: ADMINISTRATOR
Login: root
Password: root
■ Read only: USER
Login: user
Password: user</td></tr>
<tr><td>3</td><td colspan="2">Access denied</td></tr>
<tr><td></td><td colspan="2">There are several conditions that will disable you to enter Console, Telnet or Web.</td></tr>
<tr><td></td><td>Message</td><td>Solution</td></tr>
<tr><td></td><td>Incorrect user</td><td>The password you enter is wrong. Check your user name and password again.</td></tr>
<tr><td></td><td>Administrator is configuring! Reject to enter console mode configuration!</td><td>Somebody with administrator's password is configuring the device via Telnet or Web. Only one administrator can access the device at any one time. You can't enter until the person logs out, or you can try user's password.</td></tr>
<tr><td></td><td>Exceed maximum three telnet logins. Login reject!</td><td>Simultaneously up to two users and one administrator can use Telnet to access the device. If there are already three operators using Telnet, you can try Web or wait till one of the users log out.</td></tr>
<tr><td></td><td>Exceed maximum two telnet logins with user account. Login reject!</td><td>There are already two users with user password accessing the device via Telnet. You can try administrator's password to log in, or login in via Web.</td></tr>
<tr><td></td><td>Administrator is configuring, you can try user login...</td><td>Somebody is configuring the device with administrator's password. You can use user's password to log in.</td></tr>
</table>