TOTAL ACCESS 600R
User Interface Guide (UIG)

64200600L1#T-31A
April 2002

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
(256) 963-8000

Notes provide additional useful information.

Caution signify information that could prevent service interruption.

WARNING *Warnings provide information that could prevent damage to the equipment or endangerment to human life.*

Safety Instructions

When using your telephone equipment, please follow these basic safety precautions to reduce the risk of fire, electrical shock, or personal injury:

1. Do not use this product near water, such as a bathtub, wash bowl, kitchen sink, laundry tub, in a wet basement, or near a swimming pool.
2. Avoid using a telephone (other than a cordless-type) during an electrical storm. There is a remote risk of shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.
4. Use only the power cord, power supply, and/or batteries indicated in the manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for special disposal instructions.

Save These Important Safety Instructions

FCC regulations require that the following information be provided in this manual to the customer:

1. This equipment complies with Part 68 of the FCC rules. On the side of the bottom of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN), if applicable, for this equipment. If required, this information must be given to the telephone company.
2. An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68-compliant. See installation instructions for details.
3. If your telephone equipment (Total Access 600R) causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.
4. Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be given advance notice to give you an opportunity to maintain uninterrupted service.
5. If you experience trouble with this equipment (Total Access 600R), please contact ADTRAN for repair/warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or until you are sure the equipment is not malfunctioning.
6. This unit contains no user-serviceable parts.
7. The FCC recommends that the AC outlet to which equipment requiring AC power is to be installed is provided with an AC surge arrester.
8. The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.
9. The following information may be required when applying to your local telephone company for leased line facilities.

Service Type	REN/SOC	FIC	USOC
1.544 Mbps - ESF and B8ZS	6.0N	04DU9-1SN	RJ-48C

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio frequencies. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Change or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada Compliance Information

Notice: The Industry Canada label applied to the product (identified by the Industry Canada logo or the "IC:" in front of the certification/registration number) signifies that the Industry Canada technical specifications were met.

Notice: The Ringer Equivalence Number (REN) for this terminal equipment is supplied in the documentation or on the product labeling/markings. The REN assigned to each terminal device indicates the maximum number of terminals that can be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices should not exceed five (5).

Canadian Emissions Requirements

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioelectriques applicables aux appareils numériques de Class A prescrites dans la norme sur le materiel brouilleur: "Appareils Numériques," NMB-003 edictee par le ministre des Communications.

Affidavit Requirements for Connection to Digital Services

- An affidavit is required to be given to the telephone company whenever digital terminal equipment without encoded analog content and billing protection is used to transmit digital signals containing encoded analog content which are intended for eventual conversion into voiceband analog signals and transmitted on the network.
- The affidavit shall affirm that either no encoded analog content or billing information is being transmitted or that the output of the device meets Part 68 encoded analog content or billing protection specifications.
- End user/customer will be responsible for filing an affidavit with the local exchange carrier when connecting unprotected customer premise equipment (CPE) to 1.544 Mbps or subrate digital services.
- Until such time as subrate digital terminal equipment is registered for voice applications, the affidavit requirement for subrate services is waived.

Affidavit for Connection of Customer Premises Equipment to 1.544 Mbps and/or Subrate Digital Services

For the work to be performed in the certified territory of _____(telco name)

State of _____

County of _____

I, _____ (name), _____(business address),

_____ (telephone number) being duly sworn, state:

I have responsibility for the operation and maintenance of the terminal equipment to be connected to 1.544 Mbps and/or _____ subrate digital services. The terminal equipment to be connected complies with Part 68 of the FCC rules except for the encoded analog content and billing protection specifications. With respect to encoded analog content and billing protection:

( ) I attest that all operations associated with the establishment, maintenance, and adjustment of the digital CPE with respect to analog content and encoded billing protection information continuously complies with Part 68 of the FCC Rules and Regulations.

( ) The digital CPE does not transmit digital signals containing encoded analog content or billing information which is intended to be decoded within the telecommunications network.

( ) The encoded analog content and billing protection is factory set and is not under the control of the customer.

I attest that the operator(s)/maintainer(s) of the digital CPE responsible for the establishment, maintenance, and adjustment of the encoded analog content and billing information has (have) been trained to perform these functions by successfully having completed one of the following (check appropriate blocks):

( ) A. A training course provided by the manufacturer/grantee of the equipment used to encode analog signals; or

( ) B. A training course provided by the customer or authorized representative, using training materials and instructions provided by the manufacturer/grantee of the equipment used to encode analog signals; or

( ) C. An independent training course (e.g., trade school or technical institution) recognized by the manufacturer/grantee of the equipment used to encode analog signals; or

( ) D. In lieu of the preceding training requirements, the operator(s)/maintainer(s) is (are) under the control of a supervisor trained in accordance with _____ (circle one) above.

I agree to provide _____ (telco's name) with proper documentation to demonstrate compliance with the information as provided in the preceding paragraph, if so requested.

_____Signature

_____Title

_____ Date

Transcribed and sworn to before me

This _____ day of _____, 20____

_____
Notary Public

My commission expires:

_____

Warranty and Customer Service

ADTRAN will repair and return this product within ten years from the date of shipment if it does not meet its published specifications or fails while in service. For detailed warranty, repair, and return information refer to the ADTRAN Equipment Warranty and Repair and Return Policy Procedure.

Return Material Authorization (RMA) is required prior to returning equipment to ADTRAN.

For service, RMA requests, or further information, contact one of the numbers listed at the end of this section.

LIMITED PRODUCT WARRANTY

ADTRAN warrants that for ten years from the date of shipment to Customer, all products manufactured by ADTRAN will be free from defects in materials and workmanship. ADTRAN also warrants that products will conform to the applicable specifications and drawings for such products, as contained in the Product Manual or in ADTRAN's internal specifications and drawings for such products (which may or may not be reflected in the Product Manual). This warranty only applies if Customer gives ADTRAN written notice of defects during the warranty period. Upon such notice, ADTRAN will, at its option, either repair or replace the defective item. If ADTRAN is unable, in a reasonable time, to repair or replace any equipment to a condition as warranted, Customer is entitled to a full refund of the purchase price upon return of the equipment to ADTRAN. This warranty applies only to the original purchaser and is not transferable without ADTRAN's express written permission. This warranty becomes null and void if Customer modifies or alters the equipment in any way, other than as specifically authorized by ADTRAN.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE FOREGOING CONSTITUTES THE SOLE AND EXCLUSIVE REMEDY OF THE CUSTOMER AND THE EXCLUSIVE LIABILITY OF ADTRAN AND IS IN LIEU OF ANY AND ALL OTHER WARRANTIES (EXPRESSED OR IMPLIED). ADTRAN SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING (WITHOUT LIMITATION), ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THIS EXCLUSION MAY NOT APPLY TO CUSTOMER.

In no event will ADTRAN or its suppliers be liable to Customer for any incidental, special, punitive, exemplary or consequential damages experienced by either Customer or a third party (including, but not limited to, loss of data or information, loss of profits, or loss of use). ADTRAN is not liable for damages for any cause whatsoever (whether based in contract, tort, or otherwise) in excess of the amount paid for the item. Some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to Customer.

Customer Service, Product Support Information, and Training

ADTRAN will repair and return this product if within ten years from the date of shipment the product does not meet its published specification or the product fails while in service.

A return material authorization (RMA) is required prior to returning equipment to ADTRAN. For service, RMA requests, training, or more information, use the contact information given below.

Repair and Return

If you determine that a repair is needed, please contact our Customer and Product Service (CAPS) department to have an RMA number issued. CAPS should also be contacted to obtain information regarding equipment currently in house or possible fees associated with repair.

CAPS Department (256) 963-8722

Identify the RMA number clearly on the package (below address), and return to the following address:

ADTRAN Customer and Product Service
901 Explorer Blvd (East Tower)
Huntsville, Alabama 35806

RMA # _____

Pre-Sales Inquiries and Applications Support

Your reseller should serve as the first point of contact for support. If additional pre-sales support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, latest product documentation, application briefs, case studies, and a link to submit a question to an Applications Engineer. All of this, and more, is available at:

http //support adtran com

When needed, further pre-sales assistance is available by calling our Applications Engineering Department.

Applications Engineering (800) 615-1176

Post-Sale Support

Your reseller should serve as the first point of contact for support. If additional support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, updated firmware releases, latest product documentation, service request ticket generation and trouble-shooting tools. All of this, and more, is available at:

http //support adtran com

When needed, further post-sales assistance is available by calling our Technical Support Center. Please have your unit serial number available when you call.

Technical Support	(888) 4ADTRAN

Installation and Maintenance Support

The ADTRAN Custom Extended Services (ACES) program offers multiple types and levels of installation and maintenance services which allow you to choose the kind of assistance you need. This support is available at:

http //www adtran com/aces

For questions, call the ACES Help Desk.

ACES Help Desk	(888) 874-ACES (2237)

Training

The Enterprise Network (EN) Technical Training Department offers training on our most popular products. These courses include overviews on product features and functions while covering applications of ADTRAN's product lines. ADTRAN provides a variety of training options, including customized training and courses taught at our facilities or at your site. For more information about training, please contact your Territory Manager or the Enterprise Training Coordinator.

Training Phone	(800) 615-1176, ext 7500
Training Fax	(256) 963-6700
Training Email	training@adtran com

TOTAL ACCESS 600R USER INTERFACE GUIDE

This User Interface Guide is designed for use by network administrators and others who will configure and provision the system. It contains information about navigating the VT 100 user interface, configuration information, and menu descriptions.

TABLE OF CONTENTS

Navigating the Terminal Menu **15**
Terminal Menu Window 15
Navigating using the Keyboard Keys 17

Terminal Menu and System Control **20**
Selecting the Appropriate Menu 20
Security Levels 20

Configuring the Total Access 600R **21**
System Info 21
System Info>System Name 21
System Info>System Location 21
System Info>System Contact 21
System Info>Unit Name 21
System Info>Part Number 22
System Info>Serial Number 22
System Info>Firmware Revision 22
System Info>Bootcode Revision 22
System Info>System Uptime 22
System Info>Date/Time 22
System Config 23
System Config>Operating Mode 23
System Config>T1 Timing Mode 23
System Config>Telnet Access 23
System Config>Telnet User List 23
System Config>Telnet IP Access List 24
System Config>SNMP Menu 25
System Config>Maint Port Menu 26
System Config>Network Time 27
System Utility 28
System Utility>Upgrade Firmware 29
System Utility>Config Transfer 29
System Utility>Ping 31
System Utility>Terminal Mode 31
Router Menus 32
Router>Config 32
Router>Status 54
Router>Logs 59
Modules Menus 61
Modules>Modules 61
Modules>DS0 Maps 64
Initial Setup 66
Setting up Routing Options 67

Initial Setup 72
Setting up Bridging Options 72

FIGURES

Figure 1. Top-Level Terminal Menu Window 15
Figure 2. Alternate Menu View 16
Figure 3. System Information Menu 21
Figure 4. System Config Menu 23
Figure 5. System Utility Menu 28
Figure 6. Router/Configuration Menu 32
Figure 7. Global Menu 32
Figure 8. Ethernet Menu 38
Figure 9. WAN Menu 40
Figure 10. Router/Status Menu 54
Figure 11. Router/Logs Menu 60
Figure 12. Modules Menu 61

1. NAVIGATING THE TERMINAL MENU

Terminal Menu Window

The Total Access 600R uses a multi-level menu structure that contains both menu items and data fields. All menu items and data fields display in the terminal menu window (see Figure 1), through which you have complete control of the Total Access 600R.

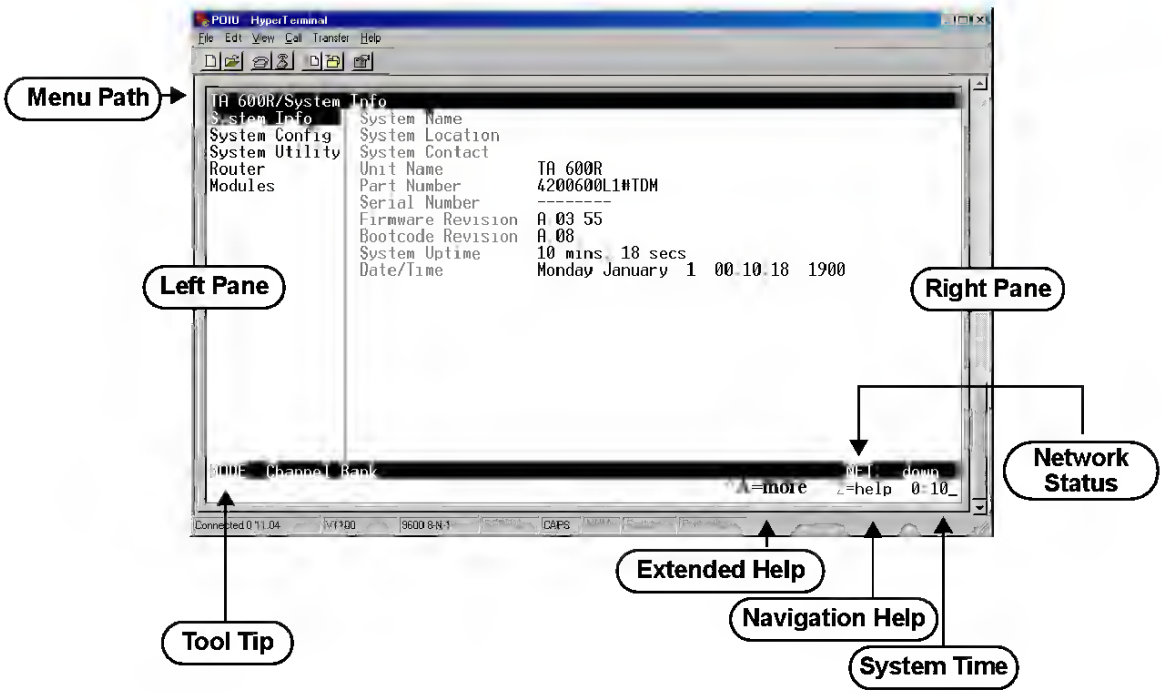

Figure 1. Top-Level Terminal Menu Window

Menu Path

The first line of the terminal menu window (the menu path) shows the session's current position (path) in the menu structure. For example, Figure 1 shows the top-level menu with the cursor on the **SYSTEM INFO** submenu, therefore, the menu path reads **TA 600R/SYSTEM INFO**.

Window Panes

When you first start a terminal menu session, the terminal menu window is divided into left and right panes. The left pane shows the list of available submenus, while the right pane shows the contents of the currently selected submenu.

You can view the terminal windows in two ways: with fields and submenus displaying horizontally across the right pane, or with fields and submenus displaying vertically down the right pane. Viewing submenus vertically rather than horizontally allows you to see information at a glance rather than scrolling horizontally across the window. To change the view, move your cursor to an index number and press **<Enter>**. Figure 2 shows this alternate view. Fields and submenu names may vary slightly in this view.

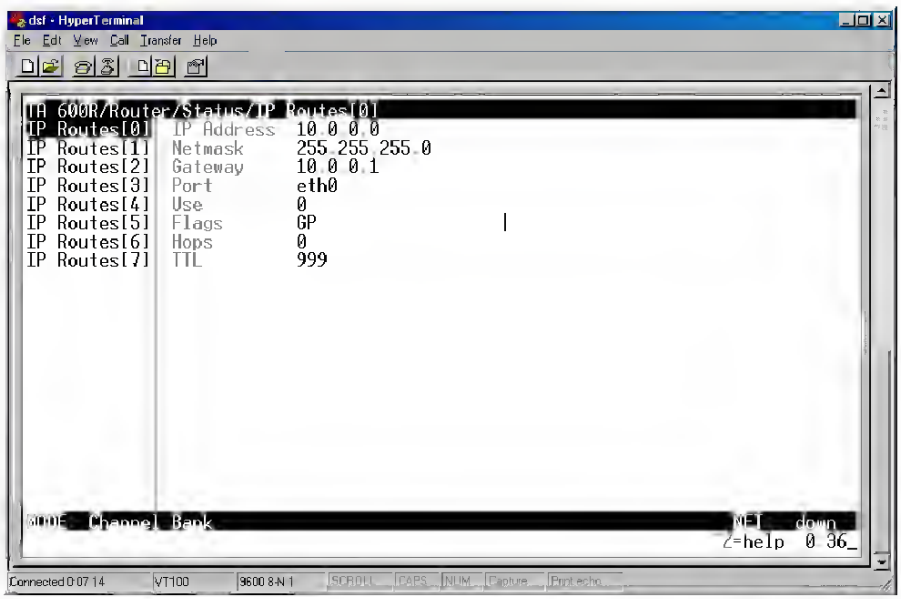

Figure 2. Alternate Menu View

Window Pane Navigation

Use the following chart to assist you in moving between and within the two window panes

To do this...	Press this key...
Move from left pane to right pane	Tab Enter Right arrow
Move from right pane to left pane	Tab Escape Left arrow Backspace
Move within each pane	Up arrow Down arrow Left arrow Right arrow

Right Window Pane Notation

The right window pane shows the contents of the currently selected menu These contents can include both submenu items and data fields Some submenus contain additional submenus and some data fields contain additional data fields The following chart explains the notation used to identify these additional items

This notation...	Means that...
[+]	More items are available when selected
<+>	An action is to be taken, such as activating a test
Highlighted menu item	You can enter data in this field
Underlined field	The field contains read-only information

Additional Terminal Menu Window Features

- Tool Tip - provides a brief description of the currently selected mode
- Network Status - displays network status information, Up or Down
- Extended Help - displays information about selected commands (CTRL+A)
- Navigation Help - lists characters used for navigating the terminal menu and session management (CTRL+Z)
- System Time - displays current time

Navigating using the Keyboard Keys

You can use various keystrokes to move through the terminal menu, to manage a terminal menu session, and to configure the system Press <CTRL+Z> to activate a pop-up screen listing the navigation keystrokes

Moving through the Menus

To do this...	Press this key...
Return to the home screen	H
Jump between two menu items Press <J> while the cursor is located on a menu item, and you jump back to the main screen. Go to another menu item, press <J>, and you jump back to the screen that was displayed the first time you pressed <J> Press <J> anytime you want to jump between these items.	J
Select items	Arrows
Edit a selected menu item	Enter
Cancel an edit	Escape
Close pop-up help screen	Escape
Move between the left and right panes	Tab Arrows
Move to the top of a screen	A
Move to the bottom of a screen	Z
Ascend one menu level	Backspace

Session Management Keystrokes

To do this...	Press this key...
Log out of a session	CTRL+L
Refresh the screen To save time, only the portion of the screen that has changed is refreshed. This option should only be necessary if the display picks up incorrect characters.	CTRL+R

Configuration Keystrokes

To do this...	Press this key...
Restore factory default settings This setting restores the factory defaults based on the location of the cursor. If the cursor is on a module line (in the **MODULES** menu), then only the selected module is updated to factory defaults	F
Copy selected items to the clipboard The amount of information you can copy depends on the cursor location when you press <C>. If the cursor is over an editable field, only that item is copied. If the cursor is over the index number of a list, then all of the items in the row of the list are copied. For example, if the cursor is over the **DS0** field in the **MAP 1** screen, all of the information associated with the DS0 is copied.	C
Paste the item stored in the clipboard, if the information is compatible You must confirm all pastes - except those to a single editable field	P
Increment the value of certain types of fields by one when you paste information into those fields.	>
Decrement the value of certain types of fields by one when you paste information into those fields.	<
Insert a new list item. For example, add a new item to the **TELNET USER LIST** connection list by pressing <I> while the cursor is over the index number.	I
Delete a list item. For example, delete an item from the **TELNET USER LIST** connection list by pressing <D> while the index number is active.	D

Getting Help

The bottom line of the terminal menu window contains context-sensitive help information. When the cursor is positioned over a set of configuration items, a help message displays (when available) providing a description of the item. When more detailed help is available for a particular item, ^A displays at the bottom of the window. At this point, if you press <CTRL+A>, a pop-up help screen displays with information about the item.

Press <CTRL+Z> to activate a help screen that displays the available keystrokes you can use to navigate the terminal menu.

Press <ESC> to cancel these pop up windows.

2. TERMINAL MENU AND SYSTEM CONTROL

Selecting the Appropriate Menu

The terminal menu is the access point to all other operations. Each terminal menu item has several functions and sub-menus that identify and provide access to specific operations and parameters. Use the chart below to help select the appropriate terminal menu.

To do this...	Go to this menu...
Review and monitor general system information for the Total Access 600R	**SYSTEM INFO**
Set up the operational configuration for the Total Access 600R	**SYSTEM CONFIG**
Upgrade firmware, do config transfers, ping, and access terminal mode	**SYSTEM UTILITY**
Define, configure, and monitor all Total Access 600R Router functions	**ROUTER**
Review and configure settings for the network interface and configure the DS0 maps	**MODULES**

Security Levels

To edit terminal menu items, you must have a password and the appropriate security level. Table 1 describes the security levels.

Table 1. Password Security Level

Security Level	Description
5	Read-only permission for all menu items - **minimum rights**
4	Read permission for all menu items and permission to use test commands
3	Access to all commands except passwords, flash download, authentication methods, interface configurations, and telnet security levels
2	Access to all commands except passwords, flash download, authentication methods, and telnet security levels
1	Access to all commands except passwords and telnet security levels
0	Permission to edit every menu item, including creating and editing passwords - **maximum rights**
Router Only	Read access to all menus and write access to only the router menu

3. CONFIGURING THE TOTAL ACCESS 600R

SYSTEM INFO

The **SYSTEM INFO** menu provides basic information about the unit as well as data fields for editing information. Figure 3 displays the submenus that are available when you select this menu item.

Figure 3. System Information Menu

SYSTEM INFO>SYSTEM NAME

Provides a user-configurable text string for the name of the Total Access 600R. This name can help you distinguish between different installations. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an underscore). This name will appear on the top line of all screens. The factory default is to have no entry in the system name field.

SYSTEM INFO>SYSTEM LOCATION

Provides a user-configurable text string for the location of the Total Access 600R. This field is to help you keep track of the actual physical location of the unit. You can enter up to 31 alphanumeric characters in this field, including spaces and special characters (such as an underscore). The factory default is to have no entry in the system location field.

SYSTEM INFO>SYSTEM CONTACT

Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or email address of a person responsible for the Total Access 600R system. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an underscore). The factory default is to have no entry in the system contact field.

SYSTEM INFO>UNIT NAME

Product-specific name.

SYSTEM INFO>PART NUMBER

ADTRAN part number for the Total Access 600R

SYSTEM INFO>SERIAL NUMBER

Serial number of the Total Access 600R

SYSTEM INFO>FIRMWARE REVISION

Displays the current firmware revision level of the Total Access 600R

SYSTEM INFO>BOOTCODE REVISION

Displays the bootcode revision

SYSTEM INFO>SYSTEM UPTIME

Displays the length of time since the last Total Access 600R system reboot

Each time you reset the system, this value resets to 0 days, 0 hours, 0 min and 0 secs.

SYSTEM INFO>DATE/TIME

Displays the current date and time, including seconds. This field can be edited. Enter the time in 24-hour format (such as 23 00 00 for 11 00 pm). Enter the date in mm-dd-yyyy format (for example, 10-30-1998).

SYSTEM CONFIG

Set up the Total Access 600R operational configuration from the **SYSTEM CONFIG** menu. Figure 4 shows the items included in this menu.

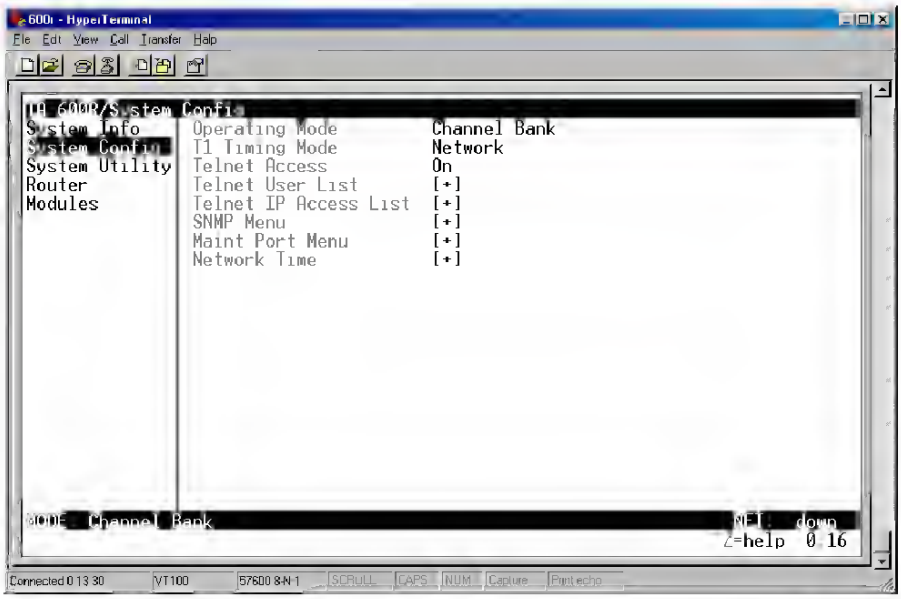

Figure 4. System Config Menu

SYSTEM CONFIG>OPERATING MODE

For the T1 TDM application, the mode will be displayed as Channel Bank.

SYSTEM CONFIG>T1 TIMING MODE

The **T1 TIMING MODE** choices are **NETWORK** and **INTERNAL.** Select **NETWORK** if the TELCO is providing clocking on the T1 line. Select **INTERNAL** if there is no timing on the T1 circuit and the 600R will have to provide the clock. Default is **NETWORK.**

SYSTEM CONFIG>TELNET ACCESS

Sets Telnet access to **ON** or **OFF**. The factory default value for this parameter is **ON**.

SYSTEM CONFIG>TELNET USER LIST

SYSTEM CONFIG>TELNET USER LIST>NAME

Up to four users can be configured for access to the 600R. Each user can be assigned a security level and time out.

The name is a text string of the user name for this session. You can enter up to 15 characters in this field. The factory default is no entry in the **NAME** field.

SYSTEM CONFIG>TELNET USER LIST>AUTHEN METHOD

The user can be authenticated by selecting

PASSWORD	The Password field is used to authenticate the user
RADIUS	The Radius client is used for authenticating the user

The factory default is **password**.

SYSTEM CONFIG>TELNET USER LIST>PASSWORD

When the authenticating method is password, this text string is used for the password. You can enter up to 15 characters in this field. The factory default is no entry in this field.

SYSTEM CONFIG>TELNET USER LIST>IDLE TIME (MINS)

This sets the amount of time in minutes you can be idle before you are automatically logged off. The factory default is **10 MINUTES.** The range is **1-255 MINUTES.**

SYSTEM CONFIG>TELNET USER LIST>LEVEL

This is the security level granted to the user. The table below gives a brief description of each level. The factory default is **0.**

Select level...	If you want the user to....
5	Have read-only permission for all menu items - **minimum rights**
4	Have read permission for all menu items and permission to use test commands
3	Have access to all commands except passwords, flash download, authentication methods, interface configurations, and telnet security levels
2	Have access to all commands except passwords, flash download, authentication methods, and telnet security levels
1	Have access to all commands except passwords and telnet security levels
0	Have permission to edit every menu item, including creating and editing passwords -- **maximum rights**
Router Only	Have read access to all menu items and write access to only the router menu

SYSTEM CONFIG>TELNET IP ACCESS LIST

SYSTEM CONFIG>TELNET IP ACCESS LIST>NETWORK ADDRESS AND MASK

This is a list of allowed telnet managers. Enter a network address and subnet mask from which telnet access to the Total Access 600R is allowed. When a remote unit requests telnet access to the Total Access 600R, if the access list is empty or the remote's IP address matches a list entry, remote access is granted. A subnet mask of 0 0 0 0 will allow any host telnet access, regardless of the network address. A network address of 0 0 0 0 with a corresponding netmask of 255.255.255.255 will disallow any host telnet access.

The factory default is 0 0 0 0 for both parameters, which will allow all users telnet IP access.

SYSTEM CONFIG>SNMP MENU

SYSTEM CONFIG>SNMP MENU>ACCESS

The Total Access 600R is an SNMP agent. The SNMP Menu parameters set up the manager, communities, and levels. When set to **OFF**, SNMP access is denied. When set to **ON**, the 600R will respond to SNMP managers based on the configuration. The factory default is **ON**.

SYSTEM CONFIG>SNMP MENU>COMMUNITIES

SYSTEM CONFIG>SNMP MENU>COMMUNITIES>NAME

This list is used to set up to 60 SNMP communities names that the 600R will allow. This is a text string for the community name. You can enter up to 31 characters in this field. The factory default is no entry in the name parameter.

SYSTEM CONFIG>SNMP MENU>COMMUNITIES>PRIVILEGE

The access for this manager can be assigned three levels. The factory default is **NONE**.

NONE	No access is allowed for this community or manager.
GET	Manager can only read items.
GET/SET	Manager can read and set items.

SYSTEM CONFIG>SNMP MENU>COMMUNITIES>MANAGER IP

This is the IP address of the SNMP manager. If set to 0.0.0.0, any SNMP manager can access the Total Access 600R for this community. The factory default is **0.0.0.0**.

SYSTEM CONFIG>SNMP MENU>TRAPS

SYSTEM CONFIG>SNMP MENU>TRAPS>MANAGER NAME

The 600R can generate SNMP traps. This list allows up to four managers to be listed to receive traps. **MANAGER NAME** is the text string describing the name of the entry. It is intended for easy reference and has no bearing on the SNMP trap function. You can enter up to 31 characters in this field. The factory default is no entry in the manager name field.

SYSTEM CONFIG>SNMP MENU>TRAPS>MANAGER IP

This is the IP address of the manager that is to receive the traps. The factory default is **0.0.0.0**.

SYSTEM CONFIG>SNMP MENU>FDL

SYSTEM CONFIG>SNMP MENU>FDL>MODE

This enables the FDL (only in ESF mode) to be used for management. Learning mode can also be enabled so the Total Access 600R can "learn" its IP configuration to be used for its FDL management. Once it learns this information from, for example a Total Access 4303, the configuration items populate. The factory default is **ON**.

SYSTEM CONFIG>SNMP MENU>FDL>LINK IP ADDRESS

This is the local IP address used for the FDL management. The FDL uses a separate IP network for communication, distinct from the customer data configured under the **ROUTER** menus. The factory default is **0.0.0.0**.

SYSTEM CONFIG>SNMP MENU>FDL>FAR END IP ADDRESS

This is the far-end IP address used for FDL management. The FDL is a separate IP network from the customer data that is configured under the **ROUTER** menus. The factory default is **0.0.0.0**.

SYSTEM CONFIG>SNMP MENU>FDL>IP NETMASK

This is the subnet mask defining the IP network used for FDL management. The factory default is **0.0.0.0**.

SYSTEM CONFIG>SNMP MENU>FDL>LEARN ADDRESS

When set to **ON**, the destination address on each received packet is assumed to be the FDL interface address. A 255.255.255.252 netmask is used, which determines the far-side address as well (since there can be only two addresses on a subnet with that netmask). When set to **OFF**, the user must input the IP address assigned to the FDL interface. Default is **ON**.

SYSTEM CONFIG>SNMP MENU>FDL>ACCEPT ALL SNMP

When set to **ON**, SNMP gets/sets received over the FDL link are always accepted regardless of the community table. When set to **OFF**, the community table is searched for valid manager IP addresses and the SNMP traffic is rejected if a match is not found. Default is **ON**.

SYSTEM CONFIG>MAINT PORT MENU

SYSTEM CONFIG>MAINT PORT MENU>PASSWORD PROTECT

The Total Access 600R's VT 100 **CRAFT** port can be accessed through a RJ-48 connector located on the rear of the unit. The setup for this port is under this menu.

When **PASSWORD PROTECT** is set to **NO**, the maintenance port is not password protected. When **YES** (def), the 600R will prompt for a password upon startup.

SYSTEM CONFIG>MAINT PORT MENU>PASSWORD

This is the text string that is used for comparison when password protecting the maintenance port. By default, no password is entered. You can enter up to 15 characters in this field.

NOTE *The security level for the maintenance port is always set to 0. This gives full access to all menus.*

NOTE *Passwords are case-sensitive.*

Instructions for Changing Passwords	
Step	**Action**
1	Select the **PASSWORD** field—a new **PASSWORD** field displays
2	Type the new password in the **ENTER** field
3	Type the new password again in the **CONFIRM** field
NOTE	*The password can contain up to 15 alphanumeric characters. You can also use spaces and special characters in the password.*

SYSTEM CONFIG>MAINT PORT MENU>BAUD RATE

This is the asynchronous rate that the maintenance port will run. The possible values are **300**, **1200**, **2400**, **4800**, **9600**, **19200**, **38400**, and **57600**. The default value is **9600**.

SYSTEM CONFIG>MAINT PORT MENU>DATA BITS

This is the asynchronous bit rate that the maintenance port will run. The possible values are **7** or **8** (def) bits.

SYSTEM CONFIG>MAINT PORT MENU>PARITY

This is the asynchronous parity that the maintenance port will run. The possible values are **NONE** (def), **ODD**, or **EVEN**.

SYSTEM CONFIG>MAINT PORT MENU>STOP BITS

This is the number of stop bits used for the maintenance port. The possible values are **1** (def), **1.5** or **2**.

SYSTEM CONFIG>NETWORK TIME

SYSTEM CONFIG>NETWORK TIME>SERVER TYPE

The Total Access 600R unit time can be entered manually from the **SYSTEM INFO** menu, or the unit can receive time from an NTP/SNTP server. The **NETWORK TIME** menu includes all parameters relating to how the unit communicates with the time server.

The server type defines the port on which the Total Access 600R will listen to receive timing information from the time server. The choices are **NT TIME** and **SNTP.** When set to **NT TIME,** the Total Access 600R will receive time from an NT server running SNTP software on its TIME port. When set to **SNTP,** the 600R will receive time directly from an SNTP server. The factory default is **SNTP.**

SYSTEM CONFIG>NETWORK TIME>ACTIVE

This network timing feature can be turned on and off. It determines whether the unit will request and receive time from a time server. The choices are **YES** and **NO**. The factory default is **NO.**

SYSTEM CONFIG>NETWORK TIME>TIME ZONE

There are several time zones available for which the time may be displayed. All time zones are based off of Greenwich Mean Time (GMT). The choices are **GMT -10 (HAWAII), GMT -9 (ALASKA), GMT -8 (PACIFIC), GMT -7 (MOUNTAIN), GMT -6 (CENTRAL), GMT -5 (EASTERN),** and **GMT**. The factory default is **GMT-6 (CENTRAL).**

SYSTEM CONFIG>NETWORK TIME>ADJUST FOR DAYLIGHT SAVING

Since some areas of the world use Daylight Savings Time, the Total Access 600R is designed to adjust the time on the first Sunday in April and the last Sunday in October accordingly if this option is turned on. The choices are **YES** and **NO**. The factory default is **YES**.

SYSTEM CONFIG>NETWORK TIME>HOST ADDRESS

This is the IP address of the time server that the Total Access 600R will request and receive time from. The factory default is no entry in the host address field

SYSTEM CONFIG>NETWORK TIME>REFRESH

This is the interval of time between each request the Total Access 600R sends out to the time server. A smaller refresh time guarantees that the unit receives the correct time from the server and corrects possible errors more quickly. This may be more taxing on the machine. A range of refresh times is available for the user to decide which is best for their unit. The choices are **5 MINS**, **10 MINS**, **15 MINS**, **20 MINS**, **25 MINS**, **30 MINS**, **35 MINS**, **40 MINS**, **45 MINS**, **50 MINS**, **55 MINS**, and **60 MINS**. The factory default is **60 MINS**.

SYSTEM CONFIG>NETWORK TIME>STATUS

This displays the current status of the time negotiation process. If an error is displayed, check all connections and configurations to try to resolve the problem

SYSTEM UTILITY

Use the **SYSTEM UTILITY** menu to view and set the system parameters shown in Figure 5

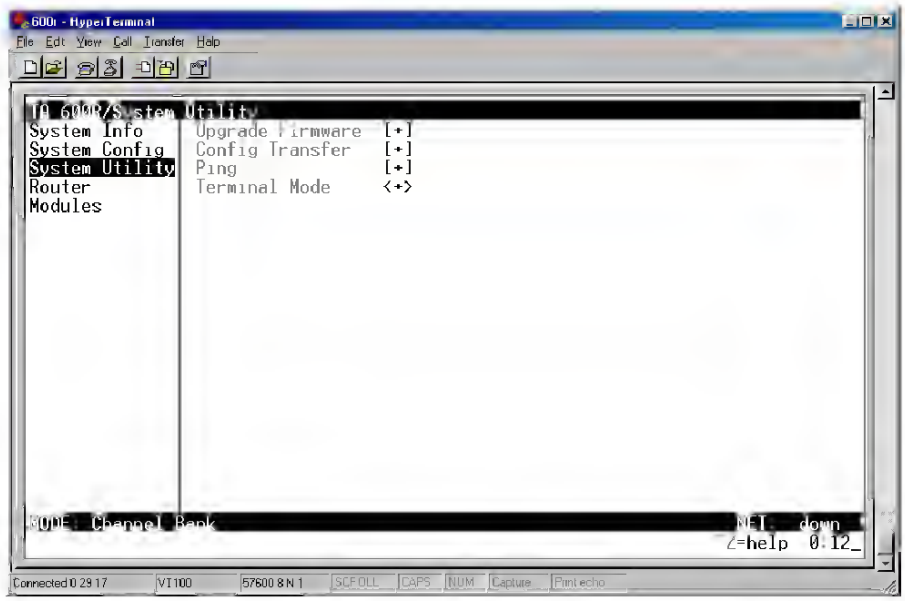

Figure 5. System Utility Menu

SYSTEM UTILITY>UPGRADE FIRMWARE

SYSTEM UTILITY>UPGRADE FIRMWARE>TRANSFER METHOD

Updates firmware when Total Access 600R enhancements are released. Two transfer methods are available for use in updating the Total Access 600R.

The two methods for upgrading are **XMODEM** and **TFTP. TFTP** requires a TFTP server running on the network. The Total Access 600R starts a TFTP client function which gets the upgrade code from the TFTP server. Selecting **XMODEM** will load the upgrade code through the **CRAFT** port using any PC terminal emulator with xmodem capability. The factory default is **TFTP.**

SYSTEM UTILITY>UPGRADE FIRMWARE>TFTP SERVER ADDRESS

This is required when the transfer method is TFTP. It is the IP address or domain name (if DNS is configured) of the TFTP server. The factory default is no entry in the **TFTP SERVER ADDRESS** field.

SYSTEM UTILITY>UPGRADE FIRMWARE>TFTP SERVER FILENAME

This is required when the transfer method is TFTP. It is the case-sensitive file name which contains the upgrade code. The factory default is no entry in the **TFTP SERVER FILENAME** field.

SYSTEM UTILITY>UPGRADE FIRMWARE>TRANSFER STATUS

This appears when TFTP is used. It displays the status of the transfer as it happens. Any error or success message will be displayed here.

SYSTEM UTILITY>UPGRADE FIRMWARE>START TRANSFER

This activator is used when the configurable items in this menu are complete.

Before using **START TRANSFER**, *the Total Access 600R should have a valid IP address, subnet mask, and default gateway (if required).*

SYSTEM UTILITY>UPGRADE FIRMWARE>ABORT TRANSFER

Use this activator to cancel any TFTP transfer in progress.

SYSTEM UTILITY>CONFIG TRANSFER

SYSTEM UTILITY>CONFIG TRANSFER>TRANSFER METHOD

Sends a file containing the Total Access 600R configuration to a PC connected to the **CRAFT** port using XMODEM protocol or to a file on a TFTP server using the TFTP protocol.

CONFIG TRANSFER also lets you save the Total Access 600R configuration as a backup file, so you can use the same configuration with multiple Total Access 600R units. In addition, **CONFIG TRANSFER** can retrieve a configuration file from a TFTP server.

To support these transfers, ADTRAN delivers a TFTP program with the Total Access 600R called *TFTP Server*. You can configure any PC running Microsoft Windows with this software, and store a configuration file.

Before using the TFTP method for **CONFIG TRANSFER**, *the Total Access 600R should have a valid IP address, subnet mask, and default gateway (if required).*

Only one configuration transfer session (upload or download) can be active at a time.

Displays the method used to transfer the configuration file to or from a server. **XMODEM** and **TFTP** are supported.

SYSTEM UTILITY>CONFIG TRANSFER>TRANSFER TYPE

Only **BINARY** transfers are currently supported from this menu.

SYSTEM UTILITY>CONFIG TRANSFER>TFTP SERVER IP ADDRESS

Specifies the IP address of the TFTP server. Get this number from your system administrator. If using the ADTRAN Utilities TFTP server, this number appears in the TFTP server status window. The factory default value is **0.0.0.0.**

SYSTEM UTILITY>CONFIG TRANSFER>TFTP SERVER FILENAME

Defines the name of the configuration file that you transfer to or retrieve from the TFTP server. The default name is **ta600.cfg**, but you can edit this name.

SYSTEM UTILITY>CONFIG TRANSFER>CURRENT TRANSFER STATUS

Indicates the current status of the update.

SYSTEM UTILITY>CONFIG TRANSFER>PREVIOUS TRANSFER STATUS

Indicates the status of the previous update.

SYSTEM UTILITY>CONFIG TRANSFER>LOAD AND USE CONFIG

Retrieves the configuration file specified in the **TFTP SERVER FILENAME** field from the server. To start this command, enter **Y** to begin or enter **N** to cancel.

If you execute this command, the Total Access 600R retrieves the configuration file, reboots, then restarts using the new configuration.

SYSTEM UTILITY>CONFIG TRANSFER>SAVE CONFIG REMOTELY

Saves the configuration file specified in **TFTP SERVER FILENAME** to the server identified in **TFTP SERVER IP ADDRESS**. To start this command, enter **Y** to begin or enter **N** to cancel.

Before using this command, you must have identified a valid TFTP server in **TFTP SERVER IP ADDRESS**.

SYSTEM UTILITY>PING

SYSTEM UTILITY>PING>START/STOP

Activator to start and cancel a ping test

> NOTE *Only one ping session can be active at a time.*

SYSTEM UTILITY>PING>HOST ADDRESS

IP address or domain name (if DNS is configured) of device to receive the ping. The factory default is no entry in the host address field.

SYSTEM UTILITY>PING>SOURCE ADDRESS

Selects whether the ping packet should use the interface address or the NAPT (if that interface uses NAT) as the source address of the ping packet. This is the address that is used for ICMP requests. Interface means it will use the IP address associated with the WAN for outgoing packets and the Ethernet IP address for ICMP requests made on the LAN. NAPT address will replace the WAN IP address with the NAPT address for outgoing ICMP requests. Default is **INTERFACE**.

SYSTEM UTILITY>PING>SIZE (40-1500)

Total size of the ping to send. Range is 40 to 1500 bytes. The default is **64.**

SYSTEM UTILITY>PING># OF PACKETS

Total packets to send every 2 seconds. Setting this to **0** allows the client to ping continuously. The default is **1.**

SYSTEM UTILITY>PING># TRANSMITS

Total packets sent (read only).

SYSTEM UTILITY>PING># RECEIVES

Total packets received (read only).

SYSTEM UTILITY>PING>% LOSS

Percentage loss based on ping returned from host (read only).

SYSTEM UTILITY>TERMINAL MODE

The terminal mode gives the user a command-line prompt. From this prompt, you can

- Perform a reset with the command "reset"
- Perform a factory restore with the command "factory_reset"
- Configure the unit. The Total Access 600R has the ability to download a text file which contains the configuration of the entire unit. This configuration may then be altered in a text editor, and then uploaded to that same or any other Total Access 600R.
- Debug and troubleshooting. This function would be carried out with the assistance of ADTRAN Technical Support.

ROUTER MENUS

Use the **ROUTER/CONFIGURATION** menu (Figure 6) to access the **GLOBAL**, **ETHERNET**, and **WAN** menus.

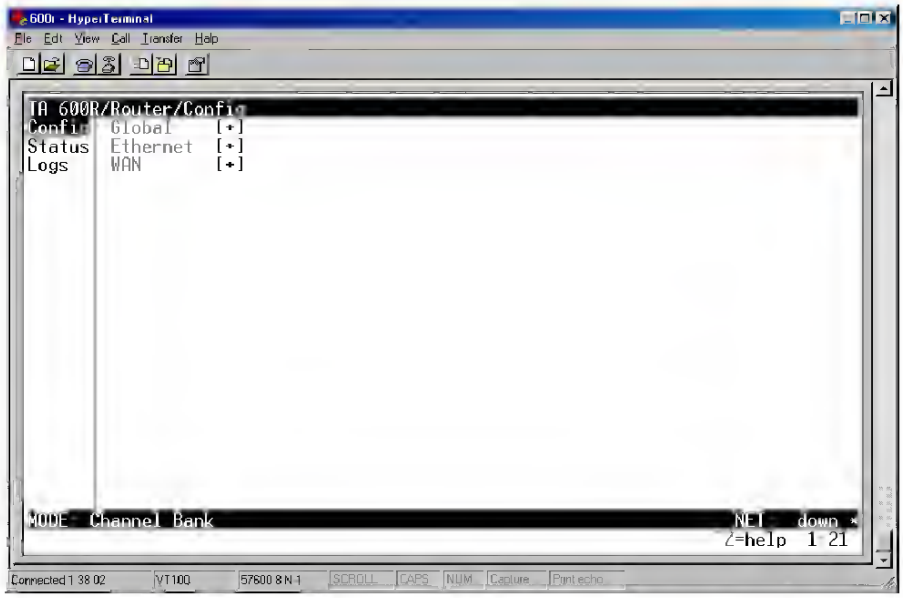

Figure 6. Router/Configuration Menu

ROUTER>CONFIG

ROUTER>CONFIG>GLOBAL

Use the **GLOBAL** menu (Figure 7) to set up general router functions.

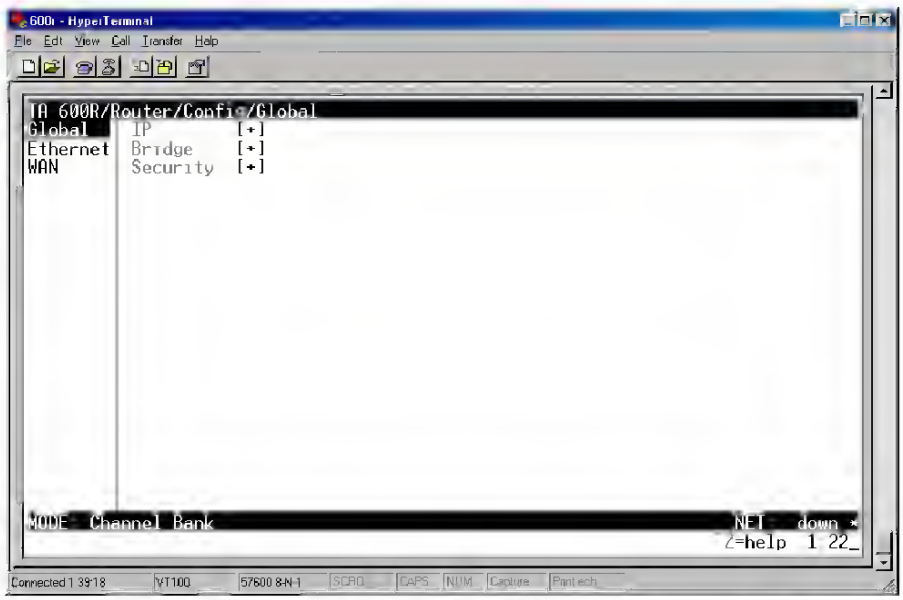

Figure 7. Global Menu

ROUTER>CONFIG>GLOBAL>IP

This parameter is used for general IP configuration

Mode

This item controls the **GLOBAL** option for IP routing. The choices are **ON** and **OFF**. The default is **ON**

Static Routes

Use this menu to enter static routes to other networks

ACTIVE	Adds this static route entry to the IP routing table when set to **YES** and removes it (if it was previously added) if set to **NO**. Default is **YES**.
IP ADDRESS	The IP address of the host or network address of the device being routed to. Default is **0.0.0.0**
SUBNET MASK	Determines the bits in the previous IP address that are used. *If this is to be a host route, it must be set to all ones* (255.255.255.255). Default is **0.0.0.0**
GATEWAY	The IP address of the router to receive the forwarded IP packet. Default is **0.0.0.0**
HOPS	The number of router hops required to get to the network or host. Maximum distance is 16 hops. Default is **1**
PRIVATE	When set to **NO**, the 600R will advertise this static route using RIP. Setting to **YES** means that the route is kept private. Default is **NO**

DHCP Server

Use this menu to set up the DHCP server.

DHCP MODE	When set to **ON**, the 600R acts as a DHCP server and will dynamically assign IP, network mask, default gateway, and DNS addresses to any device which transmits a broadcast DHCP request. The addresses assigned are based on the 600R's own IP address and will be within the same network. Default is **OFF**
DHCP RENEWAL TIME (HOURS)	The number of hours that the DHCP server should allow the device before it is required to send a new DHCP request. The range is **0-255**. The default is **15** hours, and **0** represents an infinite lease.

DNS

Enter the 600R's domain name and the DNS servers in this menu.

DOMAIN NAME	Text string used to represent the domain name used by the Total Access 600R.
SERVER 1	First server to which domain name requests are sent. Default is **0.0.0.0**
SERVER 2	Server used as a backup, in case the primary address does not respond to the request. Default is **0.0.0.0**

UDP Relay

This menu configures the 600R to act as a UDP relay agent for applications requiring a response from UDP hosts that are not on the same network segment as their clients

MODE	When this option is set to **ON**, the 600R will act as a relay agent. Default is **OFF**.
UDP RELAY LIST	Up to four relay destination servers can be specified in this list.
RELAY ADDRESS	This is the IP address of the server that will receive the relay packet. Default is **0.0.0.0**.
UDP PORT TYPE	The choices are **STANDARD** (def) and **SPECIFIED**. The following standard UDP protocols are relayed when set: DHCP, TFTP, DNS, NTP (Network Time Protocol, port 123), NBNS (NetBios Name Server, port 137), NBDG (NetBIOS Datagram, port 138), and BootP. When **SPECIFIED** is set, the UDP port (1 to 65535) can be specified in the UDP Port columns (up to three per server).
UDP PORT 1, 2, 3	Used for specifying UDP ports to be relayed. These fields only apply when **UDP PORT TYPE** is set to **SPECIFIED**. Default is **0**.

ROUTER>CONFIG>GLOBAL>BRIDGE

The **BRIDGE** menu is used to set up the bridge parameters for the 600R. The bridging function runs at the Media Access Control (MAC) level which allows any protocol packets that run over Ethernet to be forwarded. Bridging can run concurrently with IP. However, when IP routing is active, IP packets (which include ARP packets) are not bridged.

Mode

This is used to enable the bridge function. Default is **OFF**.

Address Table

The 600R automatically maintains a table of MAC addresses detected and associates those addresses with the LAN or WAN port from which they were received.

AGING (0-65535)	The maximum time an idle MAC address remains in the table before being removed. The value is in minutes. Range is **0 - 65535**. Default is **5**.
FORWARD POLICY	When this parameter is set to **UNKNOWN** (def), any bridge packet with a destination MAC address that is not in the bridge table is forwarded to all other ports (LAN and WAN). When set to **KNOWN**, the packet with the unknown destination MAC address is dropped and is not forwarded.

ROUTER>CONFIG>GLOBAL>SECURITY

Authentication

The method used for authenticating the PPP peer is selected here. The possible values are listed below.

NONE (default)	No attempt is made to authenticate the PPP peer.
RADIUS	The 600R will act as a RADIUS client and authenticate the PPP peer using the RADIUS server. The Radius server parameters must be set up properly for this to work.
PPP	The PPP profile is used to authenticate the PPP peer.

Radius Server

The parameters for the RADIUS server are configured in this menu. The RADIUS server can be used for authenticating a PPP peer (if defined under **SECURITY/AUTHENTICATION**) and for Telnet server sessions.

PRIMARY SERVER	This is the IP address of the first RADIUS server that the Total Access 600R should attempt to communicate with when authenticating a PPP peer. Default is **0.0.0.0**.
SECONDARY SERVER	This is the IP address of the back-up RADIUS server that the 600R should attempt to communicate with when the primary server does not respond. Default is **0.0.0.0**.
UDP PORT	This is the UDP port that the 600R should use when communicating with the RADIUS server. The default is **1645**, which is the commonly used port.
SECRET	The RADIUS server and 600R share this text string. It is used by the RADIUS sever to authenticate the 600R, the RADIUS client. The factory default is not to use a secret.
RETRY COUNT (1-10)	This is the number of times the 600R should send a request packet to the RADIUS server without a response before giving up. If the number of attempts to communicate with the primary server is equal to the retry count, the secondary server (if defined) is tried. If the secondary server does not respond within the retry count, the PPP peer (or Telnet session) is not authenticated and is dropped. The default is **5**.

PPP

The PPP peer can be authenticated using three standard methods: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Protocol) and EAP (Extensible Authentication Protocol). The strength of the authentication is determined in the order EAP, CHAP, followed by PAP, where EAP is the strongest and PAP is the weakest. PAP is a clear-text protocol, which means it is sent over the PPP link in a readable format. Care must be taken not to allow highly sensitive passwords to become compromised using this method. CHAP and EAP use a one-way hashing algorithm which makes it virtually impossible to determine the password. EAP has other capabilities which allow more flexibility than CHAP. The following selections are possible:

PAP, CHAP, OR EAP	The 600R will ask for EAP during the first PPP LCP negotiation and allow the PPP peer to negotiate down to CHAP or PAP.
CHAP OR EAP (DEF)	The 600R will ask for EAP during the first PPP LCP negotiation and allow the PPP peer to negotiate down to CHAP but not PAP.
EAP	The 600R will only allow EAP to be negotiated. If the PPP peer is not capable of doing EAP, then the connection will not succeed.

Filter Defines

The 600R can filter packets based on certain parameters within the packet. The method used by the 600R allows the highest flexibility for defining filters and assigning them to a PVC or PPP link. The filters are set up in two steps: (1) defining the filter types, and (2) applying them to a list under the PVC or PPP configuration. This menu is used to define the individual filter defines based on packet type.

NOTE *The* **FILTER DEFINES** *option applies to both Frame Relay and PPP applications.*

MAC FILTER DEFINES

The MAC filter is applied to bridge packets only. Bridge packets which are forwarded by the bridge functionality of the Total Access 600R are defined here. Up to 32 MAC defines can be specified.

NAME	Identifies the filter entry. Default is no entry in name field.
SRC ADDR	48-bit MAC source address used for comparison (hexadecimal format). Default is **00:00:00:00:00:00**
SRC MASK	Bits in the MAC source address which are compared (hexadecimal format). Default is **00:00:00:00:00:00**
DEST ADDR	48-bit MAC destination address used for comparison (hexadecimal format). Default is **00:00:00:00:00:00**
DEST MASK	Bits in the MAC destination address used for comparison (hexadecimal format). Default is **00:00:00:00:00:00**
TYPE	16-bit type field used for comparison (hexadecimal format). Default is **00:00**
TYPE MASK	Bits in the type field used for comparison (hexadecimal format). Default is **00:00**

PATTERN FILTER DEFINES

The pattern filter is applied to bridge packets only. That is any packet which is forwarded by the bridge functionality of the Total Access 600R. Up to 32 pattern defines can be specified.

NAME	Identifies the filter entry. Default is no entry in name field.
OFFSET	Offset from beginning of packet of where to start the pattern comparison. Default is **0**
PATTERN	64 bits used for comparison (hexadecimal format). Default is **00:00:00:00:00:00:00:00.**
MASK	Bits in the pattern to be compared (hexadecimal format). Default is **00:00:00:00:00:00:00:00.**

IP Filter Defines

The IP filter defines apply to any IP packet, whether it is routed or bridged. Up to 32 IP defines can be specified.

Name — Identifies the filter entry. Default is no entry in name field.

Src Addr — IP address compared to the source address (dotted decimal format). Default is **0.0.0.0.**

Src Mask — Bits which are used in the source comparison (dotted decimal format). Default is **0.0.0.0.**

Dest Address — IP address compared to the destination address (dotted decimal format). Default is **0.0.0.0.**

Dest Mask — Bits which are used in the destination comparison (dotted decimal format). Default is **0.0.0.0.**

Src Port — IP source port number used for comparison. Range: 0 to 65535 (decimal format). Default is **0.**

Src Port Comp — Type of comparison that is performed. Default is none.

= means ports equal to

not = means port not equal to

> means port greater than

< means port less than

None - means the source port is not compared

Dest Port — IP destination port number used for comparison. Range: 0 to 65535 (decimal format). Default is **0.**

Dest Port Comp — Type of comparison that is performed. Default is none.

= means ports equal to

not = means port not equal to

> means port greater than

< means port less than

None - means the destination port is not compared

Proto Port — Protocol used for comparison. Range: 0 to 255 (decimal format). Default is **0.**

Proto Port Comp — Type of comparison that is performed. Default is **none**

= means protocols equal to

not = means protocols not equal to

> means protocols greater than

< means protocols less than

None means the protocol is not compared

TCP ESTAB	**Yes** - only when TCP established
	No - only when TCP not established
	Ignore - ignore TCP flags (default)

ROUTER>CONFIG>ETHERNET

Use the **ETHERNET** menu (Figure 8) to configure the Ethernet port on the 600R

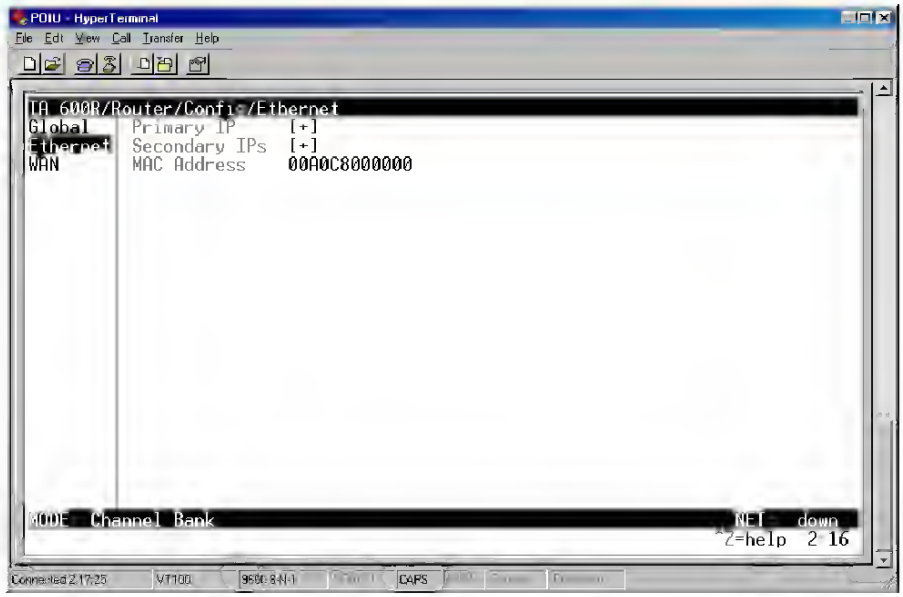

Figure 8. Ethernet Menu

ROUTER>CONFIG>ETHERNET>PRIMARY IP

This is used to setup the IP address for the LAN on the 600R

IP Address

The IP address assigned to the 600R's Ethernet port is set here. This address must be unique within the network. Default is **10.0.0.1.**

Subnet Mask

This is the IP network mask that is to be applied to the 600R's Ethernet port. Default is **255.255.255.0.**

Default Gateway

The default gateway is used by the 600R to send IP packets whose destination address is not found in the route table. Default is **0.0.0.0.**

RIP

Use this menu to enable RIP on the LAN interface

MODE	Enables or disables RIP. Default is **OFF.**
PROTOCOL	Specifies the RIP protocol. Choices are **V1** (RIP version 1) or **V2** (RIP version 2). Default is **V1.**
METHOD	Specifies the way the RIP protocol sends out its advertisements. Choices are given below.
NONE	All routes in the router table are advertised with no modification of the metrics.
SPLIT HORIZON	Only routes not learned from this circuit are advertised.
POISON REVERSE (DEF)	All routes are advertised, but the routes learned from this port are "poisoned" with an infinite metric.
DIRECTION	Allows the direction at which RIP advertisements are sent and listened to be specified.
TX AND RX (DEF)	RIP advertisements are periodically transmitted and are listened to on this port.
TX ONLY	RIP advertisements are periodically transmitted but are not listened to on this port.
RX ONLY	RIP advertisements are listened to on this port, but are not transmitted on this port.
V2 SECRET	Enter the secret used by RIP version 2 here.

Proxy ARP

This feature allows the network portion of a group of addresses to be shared among several physical network segments. The ARP protocol provides a way for devices to create a mapping between physical addresses and logical IP addresses. Proxy ARP makes use of this mapping feature by instructing a router to answer ARP requests as a "proxy" for the IP addresses behind one of its ports. The device which sent the ARP request will then correctly assume that it can reach the requested IP address by sending packets to the physical address that was returned. This technique effectively hides the fact that a network has been (further) subnetted. If this option is set to **YES**, when an ARP request is received on the Ethernet port the address is looked up in the IP routing table. If the forwarding port is not on the Ethernet port and the route is not the default route, the Total Access 600R will answer the request with its own hardware address. Default is **YES.**

ROUTER>CONFIG>ETHERNET>SECONDARY IPS

This allows the Total Access 600R to specify additional IP addresses and networks on its Ethernet. The maximum number of entries is 10.

IP Address

This is the second IP address the 600R will respond to on the Ethernet. Default is **0.0.0.0**

Subnet Mask

This is the mask for the network. Default is **255.255.255.0**

ROUTER>CONFIG>ETHERNET>MAC ADDRESS

This is a read-only field which displays the unique MAC address programmed at ADTRAN.

ROUTER>CONFIG>WAN

Use the **WAN** menu (Figure 9) to configure WAN settings on the 600R.

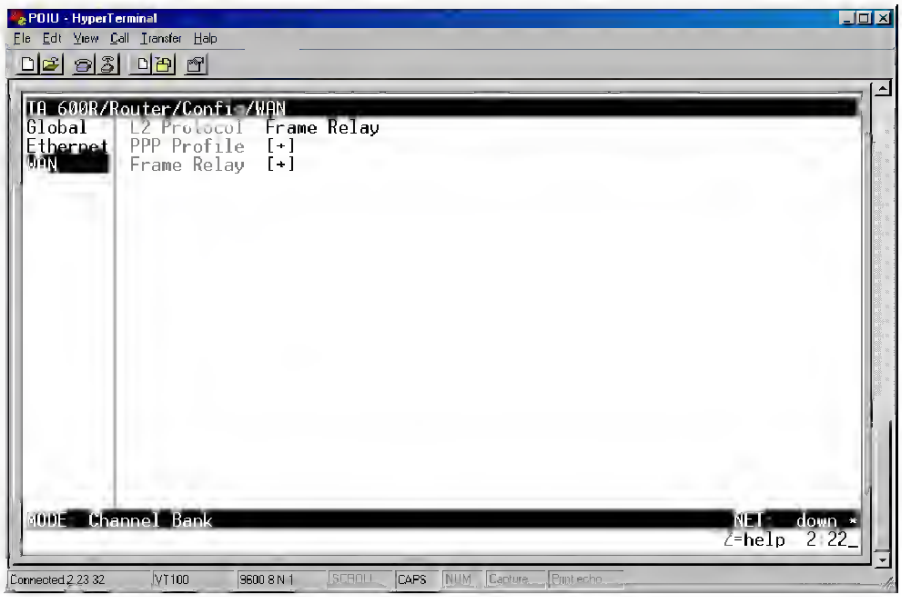

Figure 9. WAN Menu

ROUTER>CONFIG>WAN>L2 PROTOCOL

Displays the current L2 protocol. Choices are **PPP**, **FRAME RELAY**, and **AUTO DETECT**. Default is **FRAME RELAY**.

ROUTER>CONFIG>WAN>PPP PROFILE

The Total Access 600R uses the WAN/PPP profile to specify the profile used when connected using PPP.

Authentication

The authentication menu contains the required parameters for the authentication of the PPP peer and for being authenticated by the PPP peer. Authentication is applied between the Total Access 600R and the PPP peer as follows.

TX METHOD

This parameter specifies how the Total Access 600R is to be authenticated by the PPP peer. There are four possible selections. Default is **PAP, CHAP**, or **EAP**.

NONE	The connection will not allow the PPP peer to authenticate it.
PAP, CHAP, OR EAP	The Total Access 600R will ask for EAP during the first PPP LCP negotiation and allow the PPP peer to negotiate down to CHAP or PAP.
CHAP OR EAP	The Total Access 600R will ask for EAP during the first PPP LCP negotiation and allow the PPP peer to negotiate down to CHAP but not PAP.
EAP	The Total Access 600R will only allow EAP to be negotiated. If the PPP peer is not capable of doing EAP, then the connection will not succeed.

TX USERNAME
This is the username that is used when being authenticated by the PPP peer. You can enter up to 31 characters in this field. Default is no entry in the TX username field.

TX PASSWORD
This is the password or secret that is used when being authenticated by the PPP peer. You can enter up to 15 characters in this field. Default is no password.

RX USERNAME
This is the username used to authenticate the PPP peer. You can enter up to 31 characters in this field. Default is no entry in the RX username field.

RX PASSWORD
This is the password or secret that is used to authenticate the PPP peer. You can enter up to 15 characters in this field. Default is no password.

IP

The IP menu contains the parameters for exchanging IP data with the PPP peer.

MODE
Setting to **ON** (def) will permit this connection profile to negotiate PPP IPCP with the PPP peer for routing of IP packets. Choices are **OFF** and **ON**.

NAT
The Total Access 600R can perform Network Address Translation. This feature is most widely used when connecting to the Internet. The Ethernet network can consist of private network numbers. When this profile is connected, all IP addresses on the Ethernet side are translated into the one real IP address negotiated with the PPP peer (ISP). Multiple stations on the Ethernet side can access the Internet simultaneously.

PORT TRANSLATION	By enabling port translation, IP packets are modified as they pass through this interface. During transmission, private addresses are translated into a single public (NAPT) IP address. Incoming packets are translated from the public to private address based on the protocol port numbers. Once enabled, you must set up NAT for use. Default is **DISABLED**. When disabled, the unit will route across the connection normally.
PUBLIC IP ADDRESS MODE	This option is only available when **NAT PORT TRANSLATION** is enabled. The port translation requires at least a single real IP address for translating. This value can use the IP assigned to the interface (or assigned via layer 2 protocol like PPP), obtained using DHCP client, or statically specified on this menu. If the address cannot be learned, then it must be specified in order for the translation to work. Choices are **INTERFACE, SPECIFIED,** and **DHCP CLIENT.** Default is **INTERFACE.**
PUBLIC IP ADDRESS	This is the specified address used for NAT. This option is only available when **NAT PORT TRANSLATION** is enabled and the **PUBLIC IP ADDRESS MODE** is set to **SPECIFIED**. Default is 0.0.0.0.
TRANSLATION TABLE	This option is only available when **NAT PORT TRANSLATION** is enabled. Add translation entries to "fine tune" special protocols or specify private addresses.

PUBLIC ADDRESS MODE	This option is only available when **NAT PORT TRANSLATION** is enabled. The public IP address used for this translation entry can be the NAPT IP address assigned to the link or can be specified. You specify an address to direct packets with certain protocols to different servers. Choices are **NAPT ADDR** and **SPECIFIED.** Default is **NAPT ADDR.**
PUBLIC ADDRESS	This option is only available when **NAT PORT TRANSLATION** is enabled and the **PUBLIC ADDRESS MODE** is set to **SPECIFIED**. Default is **0.0.0.0.**
PROTOCOL MODE	This option is only available when **NAT PORT TRANSLATION** is enabled. The upper layer protocol that is to be monitored for translation. For TCP and UDP, a port number must also be specified. Choices are **TCP; UDP; ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED;** and **NONE.** Default is **NONE.**
PROTOCOL	This option is only available when **NAT PORT TRANSLATION** is enabled and **PROTOCOL MODE** is set to **SPECIFIED.** Default is **0** (decimal)
PROTOCOL TYPE	This option is only available when **NAT PORT TRANSLATION** is enabled and **PROTOCOL MODE** is set to **SPECIFIED.** This is a read-only field
PUBLIC PORT MODE	This option is only available when **NAT PORT TRANSLATION** is enabled and **PROTOCOL MODE** is set to either **TCP** or **UDP** The public destination port associated with this entry can be specified to add more control over certain types of traffic. Choices are **SPECIFIED** and **ANY PORT.** The default, **ANY PORT**, covers all port types.
PUBLIC PORT	This option is only available when **NAT PORT TRANSLATION** is enabled and **PUBLIC PORT MODE** is set to **SPECIFIED.** However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED;** or **NONE.** Default is **0** (decimal)
PUBLIC PORT TYPE	This option is only available when **NAT PORT TRANSLATION** is enabled and **PUBLIC PORT MODE** is set to **SPECIFIED.** However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED;** or **NONE.** This is a read-only field

PRIVATE ADDRESS MODE	This option is only available when **NAT PORT TRANSLATION** is enabled. The private IP address can be specified to steer certain protocols and ports to specific servers in the private network. Likewise, internal hosts can be steered to certain servers on the public network. A new request from the public network matching this entry's public parameters will be dropped if this mode is set to **ANY INTERNAL**. Choices are **SPECIFIED** and **ANY INTERNAL.** Default is **ANY INTERNAL.**
PRIVATE ADDRESS	This option is only available when **NAT PORT TRANSLATION** is enabled and **PRIVATE ADDRESS MODE** is set to **SPECIFIED.** Default is **0.0.0.0.**
PRIVATE PORT MODE	This option is only available when **NAT PORT TRANSLATION** is enabled. However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED** or **NONE.** The private destination port associated with this entry can be specified to add more control over certain types of traffic. Leave as **ANY PORT** to cover all port types. Choices are **ANY PORT** and **SPECIFIED.** Default is **ANY PORT**
PRIVATE PORT	This option is only available when **NAT PORT TRANSLATION** is enabled and the **PRIVATE PORT MODE** is set to **SPECIFIED**. However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED** or **NONE.** Default is **0** (decimal)
TRANSLATE BODY	This option is only available when **NAT PORT TRANSLATION** is enabled. When set to **YES**, the application payload in the packet is scanned for occurrences of the private/public IP address in binary or ASCII form. Set this to **NO** (default) for applications where this will cause problems

NAT VIEW — Shows the protocols that are actively being translated

PRIV ADDR	This option is only available when **NAT PORT TRANSLATION** is enabled. This shows the private address of the host that the entry is used for
PUB ADDR	This option is only available when **NAT PORT TRANSLATION** is enabled. This shows the public address this entry is using for its NAPT
SERV ADDR	This option is only available when **NAT PORT TRANSLATION** is enabled. This is the destination of the packet
PROTO	This option is only available when **NAT PORT TRANSLATION** is enabled. This shows the protocol used (**TCP, UDP, ICMP**, etc.)
PRIV PORT	This option is only available when **NAT PORT TRANSLATION** is enabled. This is the private port used for the entry
SPOOF PORT	This option is only available when **NAT PORT TRANSLATION** is enabled. If the same private port is already used in the table, it will spoof a different port for the entry

SERVER PORT	This option is only available when **NAT PORT TRANSLATION** is enabled. This is the port used on the public side.
TIME	This option is only available when **NAT PORT TRANSLATION** is enabled. This is the time since the entry was last used.
IN CNT	This option is only available when **NAT PORT TRANSLATION** is enabled. This is the number of packets that came in.
OUT CNT	This option is only available when **NAT PORT TRANSLATION** is enabled. This is the number of packets sent out.
NAPT ADDRESS	This option is only available when **NAT PORT TRANSLATION** is enabled. Represents the public address that is being used as the NAPT address. Read-only.
ENTRY COUNT	This option is only available when **NAT PORT TRANSLATION** is enabled. The number of entries in the NAT table. Maximum is 1500.
ENTRY OVERFLOW COUNT	This option is only available when **NAT PORT TRANSLATION** is enabled. A count of the dropped entries due to entry count being 1500 or greater, i.e., the NAT table is full.

ROUTE

The IP parameters are configured in this menu. For unnumbered interfaces, the Total Access 600R will automatically discover the PPP peer's networks using PPP IPCP and/or RIP.

FAR-END IP/NET	The PPP peer's IP address or network can be set here, if known. Leaving this at 0.0.0.0 means that the Total Access 600R will determine the PPP peer's IP and network (if unnumbered) using the PPP IPCP. Default is **0.0.0.0.**
NETMASK	This network mask is applied to the **IP/NET** address for determining the PPP peer's network. If left as 0.0.0.0, a standard network mask is used. Default is **0.0.0.0.**
STATIC ROUTE	Selecting **YES** will add a static route to the remote peer to the route table. Default is **YES.**
PRIVATE	Selecting **YES** will prevent this route from being advertised. Default is **NO.**
HOPS (1-16)	This value is the metric or number of hops that RIP will use in advertising the static route. The range is 1 to 16, where 1 is the default. The value 16 is considered an infinite distance in RIP and is, in effect, poisoning the route.
FORCE IP	When set to **YES**, the 600R will force the PPP peer to use the IP address in the **IP/Net** for this profile as its WAN IP address. Normally this is set in the **No** position. Default is **No.**
LOCAL IP	This is the IP address that is assigned to the PPP link when using numbered links. By default, no address is assigned and the PPP link is unnumbered. Default is **0.0.0.0.**

RIP

Use this menu to enable RIP on the WAN interface.

MODE	Enables or disables RIP. Default is **OFF.**
PROTOCOL	Specifies the RIP protocol. Choices are **V1** (RIP version 1) or **V2** (RIP version 2). The default is **V1**.
METHOD	Specifies the way the RIP protocol sends out its advertisements. Choices are given below.
NONE	All routes in the router table are advertised with no modification of the metrics.
SPLIT HORIZON (DEF)	Only routes not learned from this circuit are advertised.
POISON REVERSE	All routes are advertised, but the routes learned from this port are "poisoned" with an infinite metric.
DIRECTION	Allows the direction at which RIP advertisements are sent and listened to be specified.
TX AND RX (DEF)	RIP advertisements are periodically transmitted and are listened to on this port.
TX ONLY	RIP advertisements are periodically transmitted but are not listened to on this port.
RX ONLY	RIP advertisements are not transmitted on this port, but are listened.
TRIGGERED	When set to **YES**, only IP RIP updates are sent when the routing table has changed and learned routes are not "aged." When set to **NO** (def), updates are sent periodically.
RETAIN	When this Connection List entry is disconnected and this parameter is set to **YES**, all routes learned from this WAN connection are retained and their routing interface is set to idle. This permits dial-on-demand to occur using this profile for any IP network that might have been advertised by the particular PPP peer. The idle routes can be flushed or "zombies" from the routing table if a manual hangup is performed when this WAN connection is not active. When this Connection List entry is disconnected and this parameter is set to **NO** (def), routes learned from this session are "zombies" and are not retained.

Bridge

The Bridge menu contains the parameters needed for exchanging bridged packets with the PPP peer.

MODE

When set to **ON**, the Total Access 600R will attempt to negotiate PPP BCP with the PPP peer. Bridging can be used even in route mode only if the PPP peer cannot support certain PPP protocols for that particular routing protocol. Default is **OFF**.

PPP

The Total Access 600R supports the IETF standards for the Point-to-Point Protocol. The PPP state machine running in the 600R can be fine-tuned to support many applications that can be employed. The configurable items under this menu can be changed from their default values for special cases.

VJ COMPRESSION
When this item is set to **ON**, the Total Access 600R will perform TCP/IP header compression known as Van Jacobson Compression to the PPP peer. Default is **OFF.**

MAX CONFIG
This value is the number of unanswered configuration requests that should be transmitted before giving up on a connection. Choices are **5, 10, 15,** and **20**. Default is **20.**

MAX TIMER (SEC)
This value is the number of seconds to wait between unanswered configuration requests. Choices are **1, 2, 3, 5,** and **10**. Default is **3.**

MAX FAILURE
Due to the nature of PPP, configuration options may not be agreed upon between two PPP peers. This value is the number of configuration-NAKS that should occur before an option is configuration-rejected. This allows a connection to succeed that might otherwise fail. Choices are **5, 10, 15,** and **20**. Default is **5.**

Filters

The 600R can block packets in and out of a WAN port by use of the filters. They are set up in two steps: 1) define the types of packets that would be of interest in the **CONFIGURATION/SECURITY/FILTER DEFINES** menu, and 2) set up the filter type and combination of defines that will cause a packet block.

WAN-TO-LAN (IN)
The packets which come into the Total Access 600R can be filtered in three ways:

DISABLE (DEF)	Turns off packet input filtering. No incoming packets are blocked.
BLOCK ALL	All incoming packets from the WAN are blocked except as defined in the **FILTERS/IN EXCEPTIONS** list.
FORWARD ALL	All incoming packets from the WAN are not blocked except as defined in the **FILTERS/IN EXCEPTIONS** list.

IN EXCEPTIONS
This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

ACTIVE	Turns this entry active when set to **YES**. Default is **NO.**
TYPE	Selects the filter define list to reference (default is **MAC**):
MAC	from the **CONFIGURATION/SECURITY/FILTER DEFINES/MAC FILTER DEFINES** list.
PATTERN	from the **CONFIGURATION/SECURITY/FILTER DEFINES/PATTERN FILTER DEFINES** list.
IP	from the **CONFIGURATION/SECURITY/FILTER DEFINES/IP FILTER DEFINES** list.
FILTER LIST NAME	Selects between filters defined in the list. Default is no entry in filter list name.
NEXT OPER	The next operation to use to combine with the next filter in the list (default is **END**):
END	the last filter to combination
AND	logically AND this filter with the next filter in the list
OR	logically OR this filter with the next filter in the list

LAN-TO-WAN (OUT)

The packets which come out toward the WAN from the 600R can be filtered in three ways

DISABLE (DEF)	Turns off packet output filtering No outgoing packets are blocked
BLOCK ALL	All outgoing packets to the WAN are blocked except as defined in the **FILTERS/OUT EXCEPTIONS** list
FORWARD ALL	All outgoing packets to the WAN are not blocked except as defined in the **FILTERS/OUT EXCEPTIONS** list

OUT EXCEPTIONS

This is a list of up to 32 filter entries The setup is exactly the same as the **FILTER/IN EXCEPTIONS** list

ROUTER>CONFIG>WAN>FRAME RELAY

Frame Relay is a connection-oriented service requiring circuits to be configured by your carrier to establish a physical link between two or more locations Multiple virtual circuits (which appear as virtual point-to-point links) can be run through the same physical connection

There are two types of virtual circuits supported in Frame Relay Permanent Virtual Circuits (PVC) and Switched Virtual Circuit (SVC) PVCs are like dedicated point-to-point private lines Since the physical connection is always there in the form of a leased line, call setup and tear down is done by a carrier via a network management system SVCs require setup and tear down and are generally not available from Frame Relay carriers Virtually all Frame Relay communications are implemented using PVCs The Total Access 600R supports PVCs only

A number called the Data Link Connection Identifier (DLCI) identifies each virtual circuit within a shared physical channel

Maintenance Protocol

The Frame Relay maintenance protocol is used on the WAN port The maintenance protocol is used to send link status and virtual circuit information between Frame Relay switches and other devices (such as routers) that communicate with them Possible choices are listed below

ANNEX D (DEF)	This is an ANSI standard and is the most commonly used standard in the US
ANNEX A	This is the CCITT European standard
LMI	This was developed by a vendor consortium and is also known as the "consortium" management interface specification It is still used by some carriers in the U S
STATIC	This should be selected when there is no Frame Relay switch in the circuit The DLCIs are assigned in the DLCI Mapping and must be the same for the device it will communicate with

Polling Frequency (5-30)

This parameter is the interval that the Total Access 600R polls the Frame Relay switch using the maintenance protocol selected above The Total Access 600R is required to poll the Frame Relay switch periodically to determine whether the link is active The value is in seconds and ranges from 5 to 30 seconds with a default of 10 seconds

DLCI Mapping

This menu allows each DLCI to be mapped to a particular Frame Relay maintenance protocol. Each protocol parameter can be individually configured for each DLCI. By factory default, the DLCI map is empty.

When empty and a maintenance protocol other than static is used, the Total Access 600R will poll the switch to determine which DLCIs are active. These active DLCIs will attempt to determine the IP addresses on the other end of the virtual circuit using Inverse ARP (IARP). If there is a response, the network learned will be added to the router tables and the virtual circuit will be treated as an unnumbered interface. Bridge connections are made using bridge group 1.

When more than one DLCI mapping is listed, the 600R will try to match the DLCIs learned from the Frame Relay switch with the DLCI values in the map. If there is a match, the protocols specified in the map are used. However, if an active DLCI is not in the list, it looks for an entry that has 0 in the DLCI field. This entry is considered the default entry to use when no match occurs. If this default entry is not present, the Total Access 600R falls back to using IARP (as discussed in the previous paragraph) to determine the protocols to use with that particular virtual circuit. If a static maintenance protocol is used, at least one DLCI mapping must be specified.

*To insert a new profile, press the **I** key when over the* **Num** *column. A new inserted profile will always be set up with the default parameters. To copy parameters from an old profile to this newly inserted profile, use the copy (**C**) and paste (**P**) keys. Entire configuration trees can be copied with this method.*

*To delete an unused profile, use the **D** key when the cursor is over the number in the* **Num** *column. Once deleted, the profile is gone permanently as soon as the DLCI Mapping is saved. Items may be deleted when* **DEL** *appears below the status bar.*

ACTIVE

When this parameter is set to **Yes** (def), the mapping is used to determine the protocols used. If set to **No**, the Total Access 600R will ignore the virtual circuit with this DLCI.

DLCI

This is the DLCI associated with this virtual circuit. This value can range from 16 to 1007. Default is **0**.

IP MAP

This menu represents the IP protocol mapping that is to take place for this DLCI.

ACTIVE — When this is set to **Yes** (def), the Total Access 600R will attempt to route IP packets for this DLCI. A setting of **No** means that no IP traffic will be routed.

IARP	When this is set to **Yes**, the Total Access 600R will send Inverse ARP packets to determine the IP address on the other end of the virtual circuit. If the IARP is responded to, a route is placed in the IP route table. A setting of **No** (default) means that the route address is to be assigned statically using the **IP MAP/FAR-END IP ADDRESS** parameter. The Total Access 600R will always respond to Inverse ARP requests.
FAR-END IP ADDRESS	This is the IP address of the device on the other end of the virtual circuit. When this DLCI becomes active, the Total Access 600R will add a route in the IP routing table. Default is **0.0.0.0.**
IP NETMASK	The IP network mask to apply to the **FAR-END IP ADDRESS** and **LINK IP ADDRESS** is specified here. Default is **0.0.0.0.**
LOCAL IP ADDRESS	The virtual circuit may require an IP address to be specified at this DLCI interface. This is called a numbered interface. This address is used by the Total Access 600R to respond to Inverse ARP requests. If this IP address is left as 0.0.0.0, the link is treated as unnumbered and the 600R responds to the Inverse ARP with its Ethernet IP address. Default is **0.0.0.0.**

NAT

The Total Access 600R can perform Network Address Translation. This feature is most widely used when connecting to the Internet. The Ethernet network can consist of private network numbers. When this profile is connected, all IP addresses on the Ethernet side are translated into the one real IP address. Multiple stations on the Ethernet side can access the Internet simultaneously.

PORT TRANSLATION	By enabling port translation, IP packets are modified as they pass through this interface. During transmission, private addresses are translated into a single public (NAPT) IP address. Incoming packets are translated from the public to private address based on the protocol port numbers. Once enabled, you must set up NAT for use. Default is **DISABLED.** When disabled, the unit will route across the connection normally.
PUBLIC IP ADDRESS MODE	This option is only available when **NAT PORT TRANSLATION** is enabled. The port translation requires at least a single real IP address for translating. This value can use the IP assigned to the interface (or assigned via layer 2 protocol like PPP), obtained using DHCP client, or statically specified on this menu. If the address cannot be learned, then it must be specified in order for the translation to work. Choices are **INTERFACE, SPECIFIED,** and **DHCP CLIENT.** Default is **INTERFACE.**
PUBLIC IP ADDRESS	This is the specified address used for the NAT. This option is only available when **NAT PORT TRANSLATION** is enabled and the **PUBLIC IP ADDRESS MODE** is set to **SPECIFIED**. Default is **0.0.0.0**

TRANSLATION TABLE This option is only available when **NAT PORT TRANSLATION** is enabled. Add translation entries to "fine tune" special protocols or specify private addresses.

- **PUBLIC ADDRESS MODE** This option is only available when **NAT PORT TRANSLATION** is enabled. The public IP address used for this translation entry can be the NAPT IP address assigned to the link or can be specified. You specify an address to direct packets with certain protocols to different servers. Choices are **NAPT ADDR** and **SPECIFIED.** Default is **NAPT ADDR.**
- **PUBLIC ADDRESS** This option is only available when **NAT PORT TRANSLATION** is enabled and the **PUBLIC ADDRESS MODE** is set to **SPECIFIED**. Default is **0.0.0.0.**
- **PROTOCOL MODE** This option is only available when **NAT PORT TRANSLATION** is enabled. The upper layer protocol that is to be monitored for translation. For TCP and UDP, a port number must also be specified. Choices are **TCP; UDP; ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED;** and **NONE.** Default is **NONE.**
- **PROTOCOL** This option is only available when **NAT PORT TRANSLATION** is enabled and **PROTOCOL MODE** is set to **SPECIFIED.** Default is **0** (decimal).
- **PROTOCOL TYPE** This option is only available when **NAT PORT TRANSLATION** is enabled and **PROTOCOL MODE** is set to **SPECIFIED.** Read-only.
- **PUBLIC PORT MODE** This option is only available when **NAT PORT TRANSLATION** is enabled and **PROTOCOL MODE** is set to either **TCP** or **UDP.**

  The public destination port associated with this entry can be specified to add more control over certain types of traffic. Choices are **SPECIFIED** and **ANY PORT.** The default, **ANY PORT**, covers all port types.
- **PUBLIC PORT** This option is only available when **NAT PORT TRANSLATION** is enabled and **PUBLIC PORT MODE** is set to **SPECIFIED.** However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED;** or **NONE.** Default is **0** (decimal).
- **PUBLIC PORT TYPE** This option is only available when **NAT PORT TRANSLATION** is enabled and **PUBLIC PORT MODE** is set to **SPECIFIED.** However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED;** or **NONE.** Read-only.

PRIVATE ADDRESS MODE	This option is only available when **NAT PORT TRANSLATION** is enabled. The private IP address can be specified to steer certain protocols and ports to specific servers in the private network. Likewise, internal hosts can be steered to certain servers on the public network. A new request from the public network matching this entry's public parameters will be dropped if this mode is set to **ANY INTERNAL**. Choices are **SPECIFIED** and **ANY INTERNAL.** Default is **ANY INTERNAL.**
PRIVATE ADDRESS	This option is only available when **NAT PORT TRANSLATION** is enabled and **PRIVATE ADDRESS MODE** is set to **SPECIFIED.** Default is **0.0.0.0.**
PRIVATE PORT MODE	This option is only available when **NAT PORT TRANSLATION** is enabled. However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED;** or **NONE.** The private destination port associated with this entry can be specified to add more control over certain types of traffic. Leave as **ANY PORT** to cover all port types. Choices are **ANY PORT** and **SPECIFIED.** Default is **ANY PORT**.
PRIVATE PORT	This option is only available when **NAT PORT TRANSLATION** is enabled and **PRIVATE PORT MODE** is set to **SPECIFIED**. However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP, OR ICMP); ALL; SPECIFIED;** or **NONE.** Default is **0** (decimal).
TRANSLATE BODY	This option is only available when **NAT PORT TRANSLATION** is enabled. When set to **YES**, the application payload in the packet is scanned for occurrences of the private/public IP address in binary or ASCII form. Set this to **NO** (default) for applications where this will cause problems.

NAT VIEW — Shows the protocols that are actively being translated

PRIV ADDR	This option is only available when **NAT PORT TRANSLATION** is enabled. This shows the private address of the host that the entry is used for.
PUB ADDR	This option is only available when **NAT PORT TRANSLATION** is enabled. This shows the public address this entry is using for its NAPT.
SERV ADDR	This option is only available when **NAT PORT TRANSLATION** is enabled. This is the destination of the packet.
PROTO	This option is only available when **NAT PORT TRANSLATION** is enabled. This shows the protocol used (**TCP, UDP, ICMP**, etc.)
PRIV PORT	This option is only available when **NAT PORT TRANSLATION** is enabled. This is the private port used for the entry.
SPOOF PORT	This option is only available when **NAT PORT TRANSLATION** is enabled. If the same private port is already used in the table, it will spoof a different port for the entry.

SERVER PORT	This option is only available when NAT PORT TRANSLATION is enabled. This is the port used on the public side.
TIME	This option is only available when NAT PORT TRANSLATION is enabled. This is the time since the entry was last used.
IN CNT	This option is only available when NAT PORT TRANSLATION is enabled. This is the number of packets that came in.
OUT CNT	This option is only available when NAT PORT TRANSLATION is enabled. This is the number of packets sent out.
NAPT ADDRESS	This option is only available when NAT PORT TRANSLATION is enabled. Represents the public address that is being used as the NAPT address. Read-only.
ENTRY COUNT	This option is only available when NAT PORT TRANSLATION is enabled. The number of entries in the NAT table. Maximum is 1500.
ENTRY OVERFLOW COUNT	This option is only available when NAT PORT TRANSLATION is enabled. A count of the dropped entries due to entry count being 1500 or greater, i.e., the NAT table is full.

RIP		
VERSION		The RIP protocol can be specified per DLCI. The possible selections are **Off** (default) (meaning no RIP packets are listened to or sent), **V1** (RIP version 1) or **V2** (which is RIP version 2).
METHOD		This specifies the way the RIP protocol sends out its advertisements.
	NONE (DEF)	All routes in the router table are advertised out this virtual circuit with no modification of the metrics.
	SPLIT HORIZON	Only routes not learned from this particular virtual circuit are advertised.
	POISON REVERSE	All routes are advertised, but the routes learned from this port are "poisoned" with an infinite metric.
DIRECTION		This parameter specifies the direction at which RIP advertisements are sent and listened.
	TX AND RX (DEF)	RIP advertisements are periodically transmitted and are listened to on this virtual circuit.
	TX ONLY	RIP advertisements are periodically transmitted but are not listened to on this virtual circuit.
	RX ONLY	RIP is not transmitted on this virtual circuit but they are listened to.

Bridge Map

This menu is used to permit bridging of packets over this DLCI. Each DLCI or virtual circuit must be assigned a bridge group. The bridge group treats all virtual circuits as one circuit. Bridge packets destined to be transmitted out a particular bridge group are copied and transmitted individually out each DLCI in the bridge group. However, incoming bridge packets received from one DLCI are not retrans-

mitted out the other DLCIs in the same bridge group. Any device in the bridge group must transmit to each DLCI. This requires a fully meshed circuit, meaning each device has a virtual circuit to each other.

ACTIVE
When this is set to **Yes**, the 600R will bridge packets to and from this DLCI. Bridge packets are any packets that are not IP packets except when the router is turned off, in which case that particular router's protocol packets are bridged. A setting of **No** (def) means that no bridging will occur.

BRIDGE GROUP
The bridge group that this DLCI is part of is specified here as **Group 1** (def) or **Group 2**. These groups correspond to the spanning tree protocols Bridge Group 1 and Bridge Group 2.

Filter

The 600R can block packets in and out of a PVC port by use of the filters. They are set up in two steps: 1) define the types of packets that would be of interest in the **CONFIGURATION/SECURITY/FILTER DEFINES** menu, and 2) set up the filter type and combination of defines that will cause a packet block.

IN FROM PVC
The packets which come into the Total Access 600R via this PVC can be filtered in three ways:

DISABLE (DEF)	Turns off packet input filtering. No incoming packets from this PVC are blocked.
BLOCK ALL	All incoming packets from this PVC are blocked except as defined in the **FILTERS/IN EXCEPTIONS** list.
FORWARD ALL	All incoming packets from this PVC are not blocked except as defined in the **FILTERS/IN EXCEPTIONS** list.

IN EXCEPTIONS
This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

ACTIVE	Turns this entry active when set to **Yes**. Default is **No.**
TYPE	Selects the filter define list to reference
MAC (DEF)	from the **CONFIGURATION/SECURITY/FILTER DEFINES/MAC FILTER DEFINES** list
PATTERN	from the **CONFIGURATION/SECURITY/FILTER DEFINES/PATTERN FILTER DEFINES** list
IP	from the **CONFIGURATION/SECURITY/FILTER DEFINES/IP FILTER DEFINES** list
FILTER LIST NAME	Selects between filters defined in the list
NEXT OPER	The next operation to use to combine with the next filter in the list
END (DEF)	the last filter to combination
AND	logically AND this filter with the next filter in the list
OR	logically OR this filter with the next filter in the list

OUT TO PVC

The packets which transmit out this PVC from the Total Access 600R can be filtered in three ways

DISABLE (DEF)	Turns off packet output filtering. No outgoing packets to this PVC are blocked
BLOCK ALL	All outgoing packets to this PVC are blocked except as defined in the **FILTERS/OUT EXCEPTIONS** list
FORWARD ALL	All outgoing packets to this PVC are not blocked except as defined in the **FILTERS/OUT EXCEPTIONS** list

OUT EXCEPTIONS

This is a list of up to 32 filter entries. The setup is exactly the same as the **FILTER/IN EXCEPTIONS** list.

Maintenance DLCI

The Total Access 600R can be configured from the WAN without having to preset a DLCI mapping or IP address. This value is the DLCI number used to open an IP session by the Total Access 600R. Any IP packet arriving from the PVC is assumed to be for the Total Access 600R's IP stack. The destination address in the packet is assigned as the PVC's local IP address. The source address is used to add a host route in the routing table. The default is 901, but any legal DLCI number can be used.

BECN Timeout (msec)

This value is expressed in milliseconds and represents the amount of time the Total Access 600R will stop transmitting over a PVC which received a packet with the BECN bit set. The default is 1.5 seconds.

ROUTER>STATUS

Use the **ROUTER/STATUS** menu to view and set the parameters shown in Figure 10. The **ROUTER/STATUS** screens give the user useful information for debugging the current routes in the 600R.

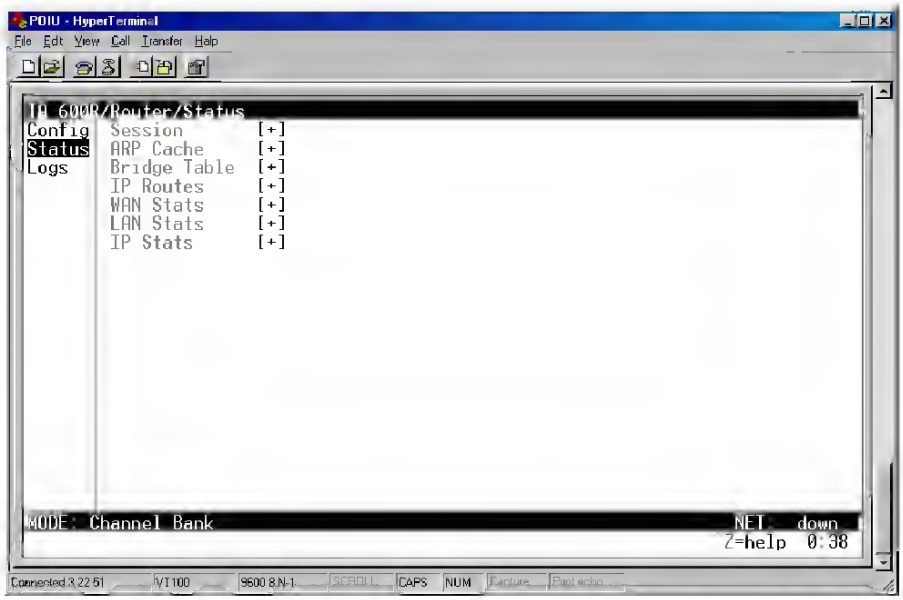

Figure 10. Router/Status Menu

ROUTER>STATUS>SESSION

This menu contains the current status of all sessions and spanning tree ports

ROUTER>STATUS>SESSION>PPP SESSION

This menu reflects the results of PPP negotiations, user name, time connected, and data rates for the session

LCP	Link Control Protocol. Reflects LCP layer active
BCP	Shows UP if PPP Bridge Control Protocol has negotiated successfully
IPCP	Shows UP if PPP IP Control Protocol has negotiated successfully
UP TIME	Displays how long the PPP session has been connected
TX PKTS	Number of packets transmitted
RX PKTS	Number of packets received
TX BYTES	Number of bytes transmitted
RX BYTES	Number of bytes received

ROUTER>STATUS>SESSION>FRAME RELAY

Port

Shows Frame Relay statistics for the WAN port

PORT INDEX	Integer used for identifying DLCIs on an interface. A single DLCI will always be port index 0. Subsequent DLCIs will have incrementing port index values
SIGNAL STATE	Displays "up" when the Total Access 600R is communicating with the Frame Relay switch, otherwise displays "down"
TX FRAMES	Total packets transmitted out
RX FRAMES	Total packets received from port
TX BYTES	Total bytes transmitted out port
RX BYTES	Total bytes received from port
SIGNAL TX FRAMES	Number of Frame Relay signaling packets transmitted out port
SIGNAL RX FRAMES	Number of Frame Relay signaling packets received from port
DROP UNKNOWN DLCI	Number of frames received that were not associated with any known PVC
DROP INVALID DLCI	Number of frames received that had illegal DLCIs

PVC's

The status of all virtual circuits is displayed here

DLCI	The DLCI that is associated with this virtual circuit
STATE	The state of the virtual circuit Inactive - means the circuit exists but has been deactivated by the Frame Relay switch Exists - means the circuit exists at this point and should be activated soon Active - means the circuit is fully active Off - means the circuit has been turned off by the DLCI mapping active selection
TX FRAMES	Number of Frame Relay packets that have been transmitted via this DLCI
RX FRAMES	Number of Frame Relay packets that have been received via this DLCI
TX BYTES	Number of Frame Relay bytes that have been transmitted via this DLCI
RX BYTES	Number of Frame Relay bytes that have been received via this DLCI
IP SUBIFC	The IP router port assigned for this DLCI Possible ports are fr0, fr1, . . . , fr9 None means that this DLCI is not used for routing IP
BRIDGE GROUP	The bridge group that this DLCI belongs to (Group 1 or Group 2) None means that this DLCI is not used for bridging
TX THROUGHPUT	Current transmit rate of this DLCI
RX THROUGHPUT	Current receive rate of this DLCI
DE COUNT	Number of packets received on this DLCI with the DE bit set
CR COUNT	Number of packets received on this DLCI with the CR bit set
BECN COUNT	Number of packets received on this DLCI with the **BECN** bit set
FECN COUNT	Number of packets received on this DLCI with the **FECN** bit set
UNKNOWN FRAME RX	Status indicating the number of frames that have been received that the Total Access 600R does not know where to route The router does not know where to send these frames

ROUTER>STATUS>ARP CACHE

This lists the contents of the Total Access 600R's ARP table All resolved cache entries time out after 20 minutes Unresolved entries time out in 3 minutes The ARP cache can be cleared by pressing "f" while on the menu or by pressing "d" on the individual number for that entry

ROUTER>STATUS>ARP CACHE>IP ADDRESS

IP address used for resolving MAC address

ROUTER>STATUS>ARP CACHE>MAC ADDRESS

Ethernet address resolved (0=no resolution)

ROUTER>STATUS>ARP CACHE>TIME

Minutes since entry was first entered

ROUTER>STATUS>BRIDGE TABLE

This lists the contents of the Total Access 600R's bridge table.

ROUTER>STATUS>BRIDGE TABLE>MAC ADDRESS

Ethernet address for device learned

ROUTER>STATUS>BRIDGE TABLE>PORT

This shows whether the packet is forwarded across the link (LAN or WAN). This populates after receiving a packet from a device, either from the Ethernet or the WAN connection.

ROUTER>STATUS>BRIDGE TABLE>TTL

Seconds until address is removed from table

ROUTER>STATUS>IP ROUTES

This lists the contents of the Total Access 600R's IP router table.

ROUTER>STATUS>IP ROUTES>IP ADDRESS

Network or host destination address

ROUTER>STATUS>IP ROUTES>NETMASK

Network mask applied to the destination address

ROUTER>STATUS>IP ROUTES>GATEWAY

Host or router to receive this packet

ROUTER>STATUS>IP ROUTES>PORT

Port gateway is located on

LOCAL	Sent directly to the Total Access 600R router
ETH0	Total Access 600R's ethernet port
WAN0	Total Access 600R's first PPP bundle
FR 0 . . . FR 9	Total Access 600R is connected up to 10 DLCIs

ROUTER>STATUS>IP ROUTES>USE

Number of times the Total Access 600R has referenced the route

ROUTER>STATUS>IP ROUTES>FLAGS

Important tags associated with this route entry

- **H** route is a host route
- **G** route is a gateway route
- **D** route learned dynamically from RIP
- **I** route learned from an ICMP redirect
- **P** route is private and is not advertised with RIP
- **T** route is to a triggered port (updates only when table changes)

ROUTER>STATUS>IP ROUTES>HOPS

Number of routers that must go through to get to destination. Ranges from 0-15 or 16 for infinite (can't get there from here)

ROUTER>STATUS>IP ROUTES>TTL

Seconds until address is removed from table. Value of 999 means route is static

ROUTER>STATUS>WAN STATS

This shows traffic over the WAN interface and contains generic WAN statistics on the HDLC hardware port.

TX BYTES	total number of raw bytes sent out HDLC
RX BYTES	total number of raw bytes received in HDLC
RX CRCS	total number of CRC errors detected on HDLC
CLEAR COUNTS	when activated, clears all WAN stat counts

ROUTER>STATUS>LAN STATS

This shows traffic over the LAN interface and contains statistics for the Ethernet port.

TX PACKETS	packets transmitted out the Ethernet port
RX PACKETS	packets received from the Ethernet port
TX ERRORS	total transmit errors encountered on Ethernet port
SINGLE COLLISIONS	total single collisions before successful transmission
MULTIPLE COLLISIONS	total multiple collisions before successful transmission
EXCESSIVE COLLISIONS	total collisions that resulted in packet being dropped
DEFERRED TRANSMISSIONS	total packets deferred due to collisions
CARRIER SENSE ERRORS	total carrier sense errors encountered (no link integrity)
RX ERRORS	Total packets received in error and dropped
CRCS	total packets detected with CRC errors
GIANTS	total packets received that were greater than 1518 bytes
RUNTS	total packets received that were less than 64 bytes
RX COLLISIONS	total collisions that occurred during reception
CLEAR COUNTS	When activated, clears all LAN Stat counts

ROUTER>STATUS>IP STATS

This menu contains IP statistics that can be useful when diagnosing problems. All are taken from the SNMP MIB-2 variables

TCP FAILED ATTEMPTS
TCP PASSIVE CONNECTIONS
TCP CURRENT CONNECTIONS
TCP SEGMENTS SENT
TCP SEGMENTS RECEIVED
TOTAL TCP RESETS
ACTIVE TCP CONNECTIONS
TOTAL TCP RETRANSMITS
UDP DATAGRAMS SENT
NO APPLICATION AT DEST PORT
UDP DATAGRAMS RECEIVED
UDP BAD PACKETS
ICMP REDIRECTED MESSAGES
ICMP PACKET ERRORS
ICMP TIMEOUTS RECEIVED
ICMP MESSAGES SENT
ICMP MESSAGES RECEIVED
ICMP SPECIFIC ERRORS
IP DATAGRAMS REASSEMBLED
IP DATAGRAMS SENT
IP DATAGRAMS RECEIVED
TOTAL FORWARDED DATAGRAMS
IP REASSEMBLY TIMEOUT
DISCARDED ROUTING ENTRIES
TOTAL IP FRAGMENTS
FAILED FRAGMENTS
IP REASSEMBLY FAILURES
DISASSEMBLED FRAGMENTS
ERROR FREE DISCARDS
ROUTELESS DISCARDS
DEFAULT TTL
BAD IP ADDRESS
SUCCESSFUL FRAGMENTS
BAD HEADER PACKETS
SENT DATAGRAMS TO UPPER LAYERS
DATAGRAMS DISCARDED
BAD PROTOCOL DISCARDS
CLEAR COUNTS

ROUTER>LOGS

The Logs menu (Figure 11 on page 60) contains logs displaying important information about the running condition of the Total Access 600R. The logs can be set to capture diagnostics of error conditions only by way of a log level. The levels are divided up as follows.

level 0 - Fatal event (causes reset)

level 1 - Critical event

level 2 - Error event

level 3 - Warning event

level 4 - Notify event

level 5 - Informational event

level 6 - Debugging event

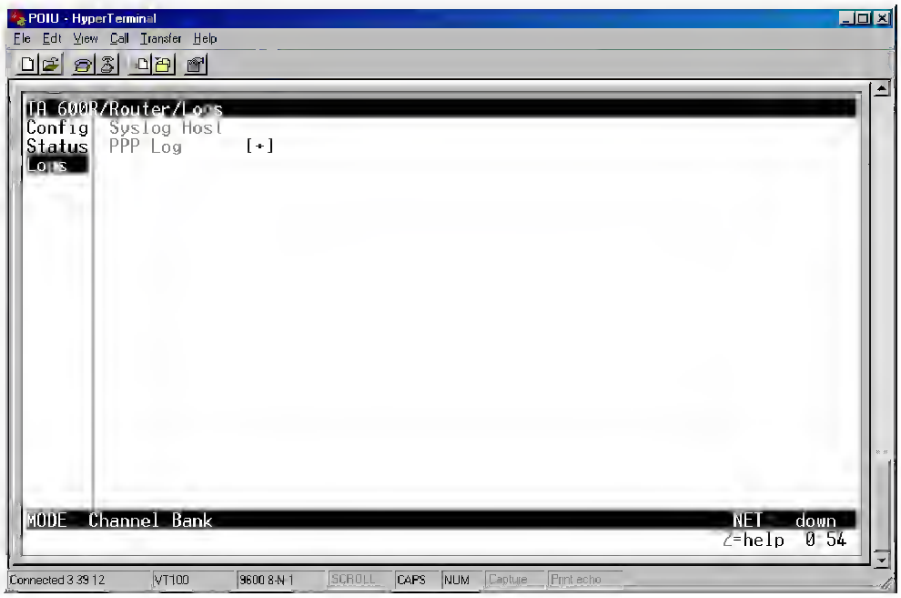

Figure 11. Router/Logs Menu

ROUTER>LOGS>SYSLOG HOST

Set this to the IP address or domain name (if DNS configured) of the syslog host device. All log events are sent to this device.

ROUTER>LOGS>PPP LOG

Information pertaining to the PPP negotiation and authentication is logged in the PPP log.

The PPP log contains the following elements.

Active

When set to **YES** (def), PPP events below or equal the log level are logged into the log.

Wrap

When set to **YES** (def), new PPP events will overwrite old PPP events when the log is full. All logging will stop when the log is full and set to **NO**.

Level

In order to log events, they must be at or below this level. Range is 0 to 6. The default is 3.

View

This menu displays the log list. The fields are as follows:

DATE/TIME	Date and time event occurred.
LEVEL	Level associated with this event (0-6)
MESSAGE	Text message for this event. If message is too long to fit on the line, another event appears below it continuing the message.

Clear
This clears the log when activated

MODULES MENUS

MODULES>MODULES

The **MODULES/MODULES** menu provides options that allow you to configure and control the network interface Figure 12 shows the **MODULES/MODULES** menu

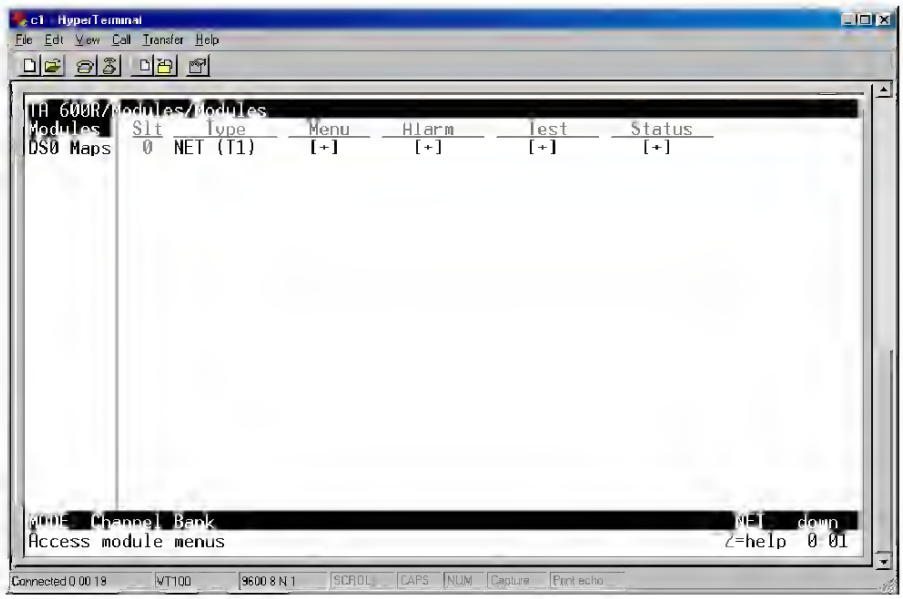

Figure 12. Modules Menu

To view the menus for the network interface via the terminal menu, use the arrow keys to scroll to the appropriate menu, then press Enter

The table contains **TYPE, MENU**, **ALARM**, **TEST**, and **STATUS** indicators/menus This document describes these menus for the Net (T1) interface

MODULES>MODULES>SLT

Identifies the slot number Slot 0 refers to the Total Access 600R This is a read-only field

MODULES>MODULES>TYPE

TYPE is displayed as **NET (T1)** indicating the network interface This is a read-only field

MODULES>MODULES>MENU

PRT identifies the port number One is the port number of the network T1 interface

MODULES>MODULES>MENU>DESC

Displays the name of the T1 interface being configured NET (network)

MODULES>MODULES>MENU>FORMAT

This sets the frame format for the T1 interface. The setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF, SF, SLC96 ALARM-16,** and **SLC96 ALARM-13. EXTENDED SUPERFRAME (ESF)** provides a nondisruptive means of full-time monitoring on the facility datelined (FDL). Default is **ESF.**

> NOTE *SF is equivalent to the D4 frame format.*

MODULES>MODULES>MENU>LINE CODE

This sets the line code for the T1 interface. The setting must match the line code of the circuit to which the interface is connected. Choices are **B8ZS** (bipolar with 8-zero substitution) and **AMI** (alternate mark inversion). Default is **B8ZS.**

MODULES>MODULES>MENU>EQUALIZATION

Select the line build out for the T1 interface. The setting of this field depends on whether the circuit is provisioned for DS1 by the telephone company. The choices are **0 dB, -7.5 dB, -15 dB, -22 dB.** Default is **0 dB.**

MODULES>MODULES>MENU>CSU LPBK

Choices are **ENABLE, DISABLE,** and **DISABLE ALL.** Default is **ENABLE.** This allows us to either respond or not respond to CSU loop up commands

MODULES>MODULES>ALARM

Indicates whether there is an alarm condition on a T1 interface. An asterisk in a field indicates that an alarm is active. Press **ENTER** to access the **ALARM** menu.

PRT	Displays the port number
LOSS OF SIGNAL (LOS)	No signal detected on port interface
RED ALARM (RED)	Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF)
YELLOW ALARM (YELLOW)	Remote alarm indicator (RAI) being received on port
BLUE ALARM (BLUE)	Receiving unframed all ones from the port alarm indicator signal (AIS)

MODULES>MODULES>TEST

These options are used to initiate local and remote loopback tests and display the test status.

MODULES>MODULES>TEST>LOC LB

Loopback of the local unit. Choices are **NONE**, **LINE**, and **PAYLOAD**. **LINE LOOPBACK** loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD LOOPBACK** is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

MODULES>MODULES>TEST>REM LB

Loopback of remote unit. Choices are **NONE**, **LINE**, and **PAYLOAD**. **LINE LOOPBACK** loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **PAYLOAD LOOPBACK** is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

MODULES>MODULES>TEST>TEST STATUS

Indicates whether a test is in progress.

MODULES>MODULES>STATUS

Displays T1 performance data.

MODULES>MODULES>STATUS>TIME FRAME

Choices are **CURRENT**, **15 MIN**, and **24 HR**. Default is **CURRENT**. The performance fields -- either **CURRENT**, **15 MIN**, or **24 HR** -- provide status on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 for the T1 port. When **CURRENT** is chosen, the performance data for the current 15 minute window is shown.

MODULES>MODULES>STATUS>CLEAR

Clears information for the T1 port. Press **Enter** when the cursor is over this field to clear the data.

MODULES>MODULES>STATUS>ES

Errored Seconds. An ES is a second with one or more error events *or* one or more Out Of Frame events *or* one or more Controlled Slips.

MODULES>MODULES>STATUS>SES

Severely Errored Seconds. An SES is a second with 320 or more error events *or* one or more Out Of Frame events.

MODULES>MODULES>STATUS>SEF

Severely Errored Frames.

MODULES>MODULES>STATUS>FS

Frame Sync Errors.

MODULES>MODULES>STATUS>LCV
Line Code Violations

MODULES>MODULES>STATUS>SLP
Slip Error Events

MODULES>MODULES>STATUS>UAS
Unavailable seconds

MODULES>DS0 MAPS

The **MODULES/DS0 MAPS** menu allows you to map network T1 time slots to the internal router. You can edit one of two maps stored in nonvolatile memory and make one of the maps the currently active map.

MODULES>DS0 MAPS>ACTIVE MAP

Activates one of the two dedicated maps (**MAP 1** or **MAP 2**). Default is **MAP 1.**

MODULES>DS0 MAPS>APPLY TEMPLATE TO MAP 1

Choices are **CURRENT MAP 1, CURRENT MAP 2,** and **CLEAR MAP**. Default is **CURRENT MAP 1. CLEAR MAP** clears the entire map.

MODULES>DS0 MAPS>MAP 1

Uses the currently defined map 1. The map 1 allows the user to assign slots and ports to individual DS0s 1-24.

MODULES>DS0 MAPS>MAP 1>DS0
Displays the network T1 time slot to be assigned.

MODULES>DS0 MAPS>MAP 1>SLOT
The first option is **OPEN**, which unassigns the slot if selected. Use **RCU:TA 600** to map network timeslots to the router. Pick the appropriate slot and press <Enter>. Default is **OPEN.**

MODULES>DS0 MAPS>MAP 1>PORT
The selection list shows only the remaining ports available to be assigned. It may be necessary to unassign a port in order to reassign it elsewhere. For the **RCU:TA 600**, the port choices are **UNASSIGNED, ROUTER 56K,** and **ROUTER 64K**. Default is **N/A.**

MODULES>DS0 MAPS>MAP 1>RBS
Robbed Bit Signaling is **N/A.**

MODULES>DS0 MAPS>APPLY TEMPLATE TO MAP 2

Choices are **CURRENT MAP 1, CURRENT MAP 2,** and **CLEAR MAP**. Default is **CURRENT MAP 2. CLEAR MAP** clears the entire map.

MODULES>DS0 MAPS>MAP 2

Define map 2. The map 2 allows the user to assign slots and ports to individual DS0s 1-24.

MODULES>DS0 MAPS>MAP 2>DS0

Displays the network T1 time slot to be assigned

MODULES>DS0 MAPS>MAP 2>SLOT

The first option is **OPEN**, which unassigns the slot if selected. Use **RCU:TA 600** to map network timeslots to the router. Pick the appropriate slot and press <Enter>. Default is **OPEN**.

MODULES>DS0 MAPS>MAP 2>PORT

The selection list shows only the remaining ports available to be assigned. It may be necessary to unassign a port in order to reassign it elsewhere. For the **RCU:TA 600**, the port choices are **UNASSIGNED**, **ROUTER 56K**, and **ROUTER 64K**. Default is **N/A**.

MODULES>DS0 MAPS>MAP 2>RBS

Robbed Bit Signaling is **N/A**

Appendix A. Configuring the Total Access 600R for Routing

Initial Setup

Before the Total Access 600R can be configured for routing, DS0s must be mapped. (See *DS0 Mapping* below.)

DS0 Mapping

DS0 Mapping Instructions	
Step	**Action**
1	From the Main menu, select **CHANNEL BANK** and then select **DS0 MAPS**.
2	Verify that the **ACTIVE MAP** is set to either **MAP 1** or **MAP 2**. This is the map that is actively running on the Total Access 600R. The unit has the ability to store two maps. • To edit the current map, press **Enter** on **MAP 1** [+] to view the map. (If Map 1 is the Active Map) • To edit the standby map, press **Enter** on **MAP 2** [+] to view the map. (If Map 1 is the Active Map)
NOTE	*The T1 line entering the Total Access 600R is broken up into 24 DS0s or channels. At least one DS0 needs to be mapped to the router in order to use the unit for routing purposes.*
3	Scroll down to the DS0 that will be mapped. (Any DS0 can be mapped to the router.)
4	Set the **SLOT** number of the DS0 that you are mapping to **RCU:TA600**.
5	Set the **PORT** of the DS0 that you are mapping to **ROUTER 64K** or **ROUTER 56K**, depending on the line speed.
6	Map all the DS0s as desired, and exit this menu by pressing the left arrow button. Your changes will automatically save when exiting the map.
7	Make sure the **ACTIVE MAP** is set to the correct map (the map you want running) before exiting the **MODULES/DS0 MAPS** menu.

Setting up Routing Options

The Total Access 600R can support IP routing and bridging These procedures are described on the pages that follow

IP Routing

There are three steps required for the Total Access 600R to be used for IP Routing (1) Global IP Setup, (2) Ethernet IP Setup, and (3) WAN IP Setup All of these procedures are described in the pages that follow

Global IP Setup

For basic IP routing, use all of the default values from the **GLOBAL** configuration menu

Global IP Setup Instructions	
Step	**Action**
1	From the Main Menu, select **ROUTER**, select **CONFIG**, and then select **GLOBAL**
2	Press **Enter** on the **IP [+]** option
3	Set the **MODE** to **ON**
4	Press **Enter** on the **STATIC ROUTES [+]** to place static routes in the routing table
5	Press **Enter** on **DHCP SERVER** [+] if the Total Access 600R needs to serve IP addresses to Ethernet devices
6	Set the **DHCP MODE** to **ON** It is **OFF** by default
7	To place DNS information in the Total Access 600R, press **Enter** on **DNS** [+] Enter Server IP addresses in the server fields

Ethernet IP Setup

Ethernet IP Setup Instructions	
Step	**Action**
1	From the Main Menu, select **ROUTER**, select **CONFIG**, and then select **ETHERNET**.
2	Press **Enter** on the **PRIMARY IP [+]** option to enter primary ethernet configuration.
3	Set the **IP ADDRESS** of the Ethernet port.
4	Set the **SUBNET MASK** of the Ethernet port.
5	Set the **DEFAULT GATEWAY** of the Ethernet port if needed.
6	**RIP** on the Ethernet is disabled by default. If **RIP** needs to be enabled, press **Enter** on **RIP [+]**.
7	Press the left arrow key to return to the main Ethernet menu.
8	If the Total Access 600R needs additional secondary IP addresses, press **Enter** on **SECONDARY IPS [+]**. The Total Access 600R supports up to 10 additional LAN segments. Enter each additional secondary IP address and subnet mask. Press "I" to insert additional entries.

WAN IP Setup

For WAN IP setup, choose either PPP IP Setup or Frame Relay IP Setup. Both of these procedures are described on the pages that follow.

WAN IP Setup - PPP IP Setup Instructions	
Step	**Action**
1	From the Main Menu, select **ROUTER**, select **CONFIG**, and then select **WAN**
2	Set the **L2 PROTOCOL** to **PPP**.
3	Press **Enter** on the **PPP PROFILE [+]** option
4	Press **Enter** on the **AUTHENTICATION [+]** option if you wish to change options related to how the link is established. Default is **TX METHOD = PAP, CHAP, OR EAP.**
5	Press the left arrow key to return to the **WAN/PPP PROFILE** menu, and then press **Enter** on the **IP [+]** option. Verify that **MODE** is **ON**
6	Arrow down to **ROUTE [+]** to enter WAN IP information.
7	Enter WAN information • Far-End IP Address — The far-end WAN IP address from the Total Access 600R • Subnet Mask — The subnet mask for this WAN link • Local IP — The local WAN IP address for the Total Access 600R The other config items can be left at the defaults
8	Use the <Esc> key to return to the top level Total Access 600R menu. Confirm any necessary changes.
9	For NAT configuration, please see **IP Routing with NAT**

WAN IP Setup - Frame Relay IP Setup Instructions (required if the Total Access 600R is to be used for Frame Relay IP Routing on the WAN interface)	
Step	**Action**
1	From the Main Menu, select **ROUTER**, select **CONFIG**, and then select **WAN**.
2	Set the **L2 PROTOCOL** to **FRAME RELAY**.
3	Press **Enter** on the **FRAME RELAY [+]** option.
4	Set the **MAINTENANCE PROTOCOL** to **ANNEX D, ANNEX A, LMI, OR STATIC**.
NOTE	*The* **MAINTENANCE PROTOCOL** *should be set based on the Frame Relay switch.*

WAN IP Setup-Frame Relay IP Setup - Map DLCIs	
Step	**Action**
1	From the Main Menu, select **ROUTER**, select **CONFIG**, and press **Enter** on the **FRAME RELAY [+]** option.
2	Press **Enter** on **DLCI MAPPING [+]**. Right arrow one time to create an entry.
3	Set **ACTIVE** to **YES**.
4	Set **DLCI** to the DLCI number.
5	Press **Enter** on the **IP MAP [+]**.
6	Set **ACTIVE** to **YES**.
7	Set **IARP** to **NO**.
8	Configure WAN IP information • Far-End IP Address — The far-end WAN IP address from the Total Access 600R • Subnet Mask — The subnet mask for this WAN link • Local IP — The local WAN IP address for the Total Access 600R The other config items can be left at the defaults.
9	For NAT configuration, please see **IP Routing with NAT**.
10	Press <Esc> to return to main menu. Confirm all changes by pressing "y" when prompted.

WAN IP Setup - IP Routing with NAT	
Step	**Action**
1	Depending on whether you are doing PPP or Frame Relay, the NAT menu is found under **ROUTER/CONFIG/WAN/PPP PROFILE/IP/NAT** or **ROUTER/CONFIG/WAN/FRAME RELAY/DLCI MAPPING/IP MAP/NAT**. The NAT menu can be easily accessed by pressing <Ctrl><N>. The <Ctrl> <N> command will take you to the **FRAME RELAY NAT** menu if the **L2 PROTOCOL** is set to **FRAME RELAY**. The <Ctrl> <N> command will take you to the **PPP NAT** menu if the **L2 PROTOCOL** is set to **PPP**.
2	From the **NAT** menu, set **NETWORK ADDRESS TRANSLATION** to **ENABLED**. (This will enable translation and populate the corresponding NAT menu options.)
3	Set **PUBLIC IP ADDRESS MODE** to either **INTERFACE** or **SPECIFIED**. • **INTERFACE** is the default and will use the WAN IP address for the NAPT address. • **SPECIFIED** allows you to enter another public address for private addresses to be translated into. For basic NAT, this is all of the configuration that needs to be done. For specific port translations or 1:1 mapping, you can enter **TRANSLATION TABLE** [+].
4	From the **TRANSLATION TABLE** menu, create a new entry by using the right arrow to enter the table.
5	Create specific NAT translations based on your application. **PUBLIC ADDRESS MODE** — **NAPT ADDR** (Address) or **SPECIFIED**. Choice of using the NAPT address or specifying a different public address to be used for this translation. **PROTOCOL** — Protocol for this translation. **PUBLIC PORT MODE** — **SPECIFIED** or **ANY PORT**. Choosing **SPECIFIED** brings up the **PUBLIC PORT** and **PUBLIC PORT TYPE** (read-only) settings. **PUBLIC PORT** — Numeric Public Port number to be translated (i.e., 23, 80). **PUBLIC PORT TYPE** — Read-only port type chosen by the user setting of the **PUBLIC PORT** option. **PRIVATE ADDRESS MODE** — **SPECIFIED** or **ANY INTERNAL**. Choosing **SPECIFIED** brings up the **PRIVATE ADDRESS** option. **PRIVATE PORT MODE** — **SPECIFIED** or **ANY PORT**. Choosing **SPECIFIED** brings up the **PRIVATE PORT** option. **PRIVATE PORT** — Numeric Private Port number to be translated to (i.e. 23, 80). **TRANSLATE BODY** — **YES** or **NO**. If set to **YES**, this will translate the body of the data packet and replace the private address with the NAPT address. Default is **NO**, which is used for most applications.

Appendix B. Configuring the Total Access 600R for Bridging

Initial Setup

Before the Total Access 600R can be configured for bridging, DS0s must be mapped. (See *DS0 Mapping* on page 66).

Setting up Bridging Options

If the Total Access 600R will be used for bridging, continue with the steps below.

Bridging

There are two steps required for the Total Access 600R to be used for Bridging: (1) Global Bridging Setup and (2) WAN Bridging Setup. Both of these procedures are described on the pages that follow.

Global Bridging Setup

Global Bridging Setup Instructions	
Step	**Action**
1	From the Main Menu, select **ROUTER**, select **CONFIG**, and then select **GLOBAL**.
2	Press **Enter** on the **BRIDGE [+]** option.
3	Set the **MODE** to **ON**. Return to the main **GLOBAL** menu.
4	Press **Enter** on the **IP [+]** option.
5	Set the **MODE** to **OFF**.
6	Return to the main menu. Confirm all configuration changes with "y" for yes.

WAN Bridging Setup

Choose one of the following options: PPP Bridge Setup or Frame Relay Bridge Setup. Both of these procedures are described on the pages that follow.

WAN Bridging - PPP Bridge Setup Instructions	
Step	**Action**
1	From the Main Menu, select **ROUTER**, select **CONFIG**, and then select **WAN**.
2	Set the **L2 PROTOCOL** to **PPP**.
3	Press **Enter** on the **PPP PROFILE [+]** option.
4	Press **Enter** on the **BRIDGE [+]** option.
5	Set the **MODE** to **ON**.
6	Return to the main **PPP PROFILE [+]** menu.

WAN Bridging - PPP Bridge Setup Instructions (Continued)	
7	Press **Enter** on the **IP [+]** option.
8	Set the **MODE** to **OFF**.
9	Press <Esc> to return to the main menu. Confirm all configuration changes with "y" for yes.

WAN Bridging - Frame Relay Bridge Setup Instructions	
Step	**Action**
1	From the Main Menu, select **ROUTER**, select **CONFIG**, and then select **WAN**.
2	Set the **L2 PROTOCOL** to **FRAME RELAY**.
3	Press **Enter** on the **FRAME RELAY [+]** option.
4	Set the **MAINTENANCE PROTOCOL** to **ANNEX D, ANNEX A, LMI, OR STATIC**.
NOTE	*The* **MAINTENANCE PROTOCOL** *should be set based on the Frame Relay switch.*

WAN Bridging - Frame Relay Bridge Setup - Map DLCIs	
Step	**Action**
1	From the Main Menu, select **ROUTER**, select **CONFIG**, select **WAN**, and press **Enter** on the **FRAME RELAY [+]** option.
2	Press **Enter** on **DLCI MAPPING [+]**.
3	Press **Enter** on the **BRIDGE MAP [+]** of each DLCI you wish to set up for bridging.
4	Set **ACTIVE** to **YES**.
5	Set the **BRIDGE GROUP**.
6	Return to the DLCI list.
7	Press **Enter** on the **IP MAP [+]** option.
8	Set **ACTIVE** to **NO**.
9	Return to the main menu. Confirm all configuration changes with "y" for yes.