OPERATIONS MANUAL

2800 Series
Remote Access Server (RAS)

PATTON Electronics Co.

Part #07M2800-D
Doc. #10701UD
Revised 7/27/98

SALES OFFICE
(301) 975-1000
TECHNICAL SUPPORT
(301) 975-1007
http://www.patton.com

ISO 9001 CERTIFIED

An ISO-9001
Certified Company

OPERATIONS MANUAL

2800 Series
Remote Access Server (RAS)

Patton Electronics Company

Patton Electronics Company, Inc.
7622 Rickenbacker Drive
Gaithersburg, MD. 20879
tel: (301) 975-1000
fax: (301) 869-9293
support: (301) 975-1007
web: http://www.patton.com
email: support@patton.com

Copyright © 1998 Patton Electronics Company. All rights reserved.

The information in this document is subject to change without notice. Patton Electronics assumes no liability for errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

Table of Contents

About This Guide

Table of Contents

Audience

This Operations Manual is intended to be used by qualified systems administrators and network engineers to successfully configure the Patton Electronics Model 2800 Programmable Access Router. Knowledge of basic networking and routing concepts is assumed.

Preview of this Operations Manual

Chapter 1, "Introduction" generally describes the 2800, including product features, terminology descriptions, product applications, connections, LED descriptions and product specifications.

Chapter 2, "Getting Started" describes how the 2800 works, how to set and save initial operating parameters, and T1/E1/ISDN Provisioning parameters.

Chapter 3, "Configuring the PSTN Line Interface" describes how to set up the 2800's PSTN Line Interface.

Chapter 4, "Configuring Authentication" describes how to set up the 2800's Local or RADIUS™ Authentication parameters

Appendix A, "Using The Internal HTML Management Pages" provides a description of the 2800's internal HTTP/HTML management pages.

Documentation Conventions

Table A-1. Documentation Conventions

Convention	Meaning
Bold Helvetica Text	Describes configuration commands or parameters that you may enter or change to configure the 2800.
NOTE:	Denotes important additional information.
WARNING!	Means that a failure to take appropriate safety measures could result in physical injury.
CAUTION:	Means that users should proceed with caution or should contact appropriate technicians. A failure to do so could result in damage or injury.
Application Tips!	Denote helpful hints that could aid in 2800 operation or troubleshooting.
(snmpObject)	Denote SNMP or Patton Enterprise MIB Variables

Compliance Information

FCC Compliance

The 2800 has been tested and found to comply with the specifications found in Part 68 of the FCC rules and regulations. A label on the equipment bears the FCC registration number. You may be requested to provide this information to your telephone company.

The telephone company may decide to temporarily discontinue your service if they believe that the 2800 may cause harm to the telephone network. Whenever possible the telephone company will attempt to notify you in advance. You have a right, if you so choose, to file a complaint with the FCC.

In accordance with FCC rules and regulation CFR 47 68.218(b)(6), the user must notify the telephone company prior to disconnection.

The Universal Service Order Code (USOC) is RJ48C.
The Facility Interface Codes (FIC) are 04DU9-BN, 04DU9-DN, 04DU9-1KN, and 04DU9-1SN.
The Service Order Code (SOC) is 6.0Y.

Industry Canada Notice

The Canadian Department of Communications label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective , operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above condition may not prevent degradation of service in some situations.

Repairs to some certified equipment should be made by an authorized maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment , or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the ground connections of the power utility, telephone lines and internal metallic water pipe system, are connected together. This protection may be particularly important in rural areas.

> **CAUTION:** Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate

Additional References

Please use the following references to obtain additional information that may be helpful in operating 2800 Series products:

RFCs

..You may use a World Wide Web browser to find online copies of the following Request for Comments (RFC).

RFC 1643, *Definitions of Managed Objects for the Ethernet-like Interface Types*
RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types*
RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*
RFC 1315, *Management Information Base for Frame Relay DTEs*
RFC 1389, *RIP Version 2 MIB Extension*
RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types*
RFC 1643, *Definitions of Managed Objects for the Ethernet-like Interface Types*

Contacting Technical Support

Patton Electronics' technical staff is also available to answer any questions that might arise concerning the installation or use of your 2800. Technical Service hours: **8AM to 5PM EST, Monday through Friday.**

All warranty and non-warranty repairs must be returned freight prepaid and insured to Patton Electronics. All returns must have a Return Materials Authorization number on the outside of the shipping container. This number may be obtained from Patton Electronics Technical Service at **(301) 975-1007**; **http://www.patton.com**: or, **support@patton.com**.

NOTE: Packages received without an RMA number will not be accepted.

1

Introduction

Table of Contents

Warranty Information

Patton Electronics warrants all 2800 Series components to be free from defects, and will—at our option—repair or replace the product should it fail within one year from the first date of shipment.This warranty is limited to defects in workmanship or materials, and does not cover customer damage, abuse, or unauthorized modification. This product contains no serviceable parts; therefore the user shall not attempt to modify the unit in any way. If this product fails or does not perform as warranted, your sole recourse shall be repair or replacement as described above. Under no condition shall **Patton Electronics** be liable for any damages incurred by the use of this product. These damages include, but are not limited to, the following: lost profits, lost savings and incidental or consequential damages arising from the use of or inability to use this product. **Patton Electronics** specifically disclaims all other warranties, expressed or implied, and the installation or use of this product shall be deemed an acceptance of these terms by the user.

Why Develop a Remote Access Server?

More and more companies are using the Internet as a vital channel for communicating with customers, employees and business partners. In fact, traffic on the Internet is doubling every 3 months. Much of this traffic is being generated by small-to-medium size companies, as well as a growing number of small ISPs (Internet Service Providers) springing up to provide access to the “e-hungry” masses on the Superhighway.

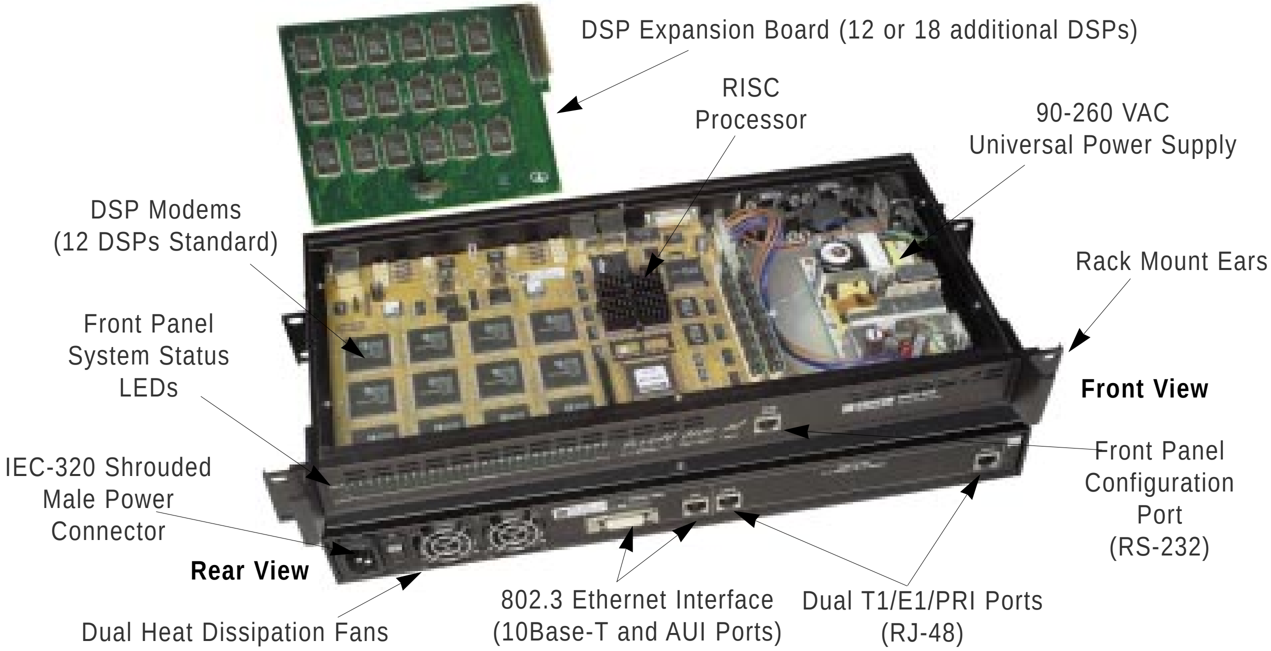
As this new wave of small-to-medium size corporate Internet users and ISPs comes online, it is clear that the First Wave of expensive big-box access tools cannot provide the cost-effective remote access solution they need.

The Patton 2800 RAS (Remote Access Server) is designed to provide a Second Wave access solution: a compact, software upgradeable platform that allows dial-up access to Internet <u>and</u> intranet services, and has the flexibility to operate cost-effectively as a stand-alone or networked device.

Advantages of Patton’s Digital Modem Technology

- **Efficient & Consistent Performance** - because no signal information is lost, performance is repeatable (no “fudge factor”)
- **Migration Path** - Easily accommodated by <u>software</u> upgrade only!
- **Manageable** - On-the-fly programmability; real-time diagnostics
- **Low Power Consumption and Heat Dissipation** - High density packaging with minimal heat generation
- **Inherent Fault Tolerance** - DSP chips are dynamically allocated; no switching fabric
- **Distributed Processing** – Data processing is performed inside each DSP
- **Low Cost** - Minimal number of components = increased reliability

The 2800 RAS simultaneously consolidates analog modem and digital ISDN remote access connections (over PSTN digital trunks) using a completely digital approach. One or two T1/E1/PRI ports provide PSTN and/or PABX connectivity to terminate up to 30 analog modem and digital ISDN calls within a single chassis. The 2800 incorporates Channel Bank, Terminal Server, Router and Modem functionality in a self-contained, compact package.


DSP Expansion Board (12 or 18 additional DSPs)
RISC Processor
90-260 VAC Universal Power Supply
DSP Modems (12 DSPs Standard)
Rack Mount Ears
Front Panel System Status LEDs
Front View
IEC-320 Shrouded Male Power Connector
Front Panel Configuration Port (RS-232)
Rear View
Dual Heat Dissipation Fans
802.3 Ethernet Interface (10Base-T and AUI Ports)
Dual T1/E1/PRI Ports (RJ-48)

Chassis Architecture & Hardware At-a-Glance

- Single, compact 1U high chassis
- Dual T1/E1/PRI PSTN connections
- Redundant fans for cool operation
- Universal 90-260VAC power supply
- Console port for local management
- Up to 30 DSPs & 32 Meg of DRAM
- FLASH upgradeable through LAN or WAN ports
- 10Base-T and AUI Ethernet connections

Where to Use the 2800 RAS

The 2800 RAS provides dial-up access for digital (ISDN BRI) and analog (V.34+, V.90) calls, local and central site user authentication, call accounting and statistics, drop and insert functionality, and IP routing. With this feature set, the 2800 can assume a critical role in a variety of applications.

Preview Of Applications

#1

ISP Access

The 2800 RAS gives start-up ISPs a single-platform access solution that is compact., affordable and expandable.

#2

ISP Expansion

For the ISP expanding service to other calling areas, the 2800 RAS provides a cost-effective remote Point-of-Presence.

#3

Corporate Network Access

The 2800 RAS puts the corporate network just a phone call away, with Email, LAN and Web access available through a single box.

#4

Dial Access for Wide Area Networks

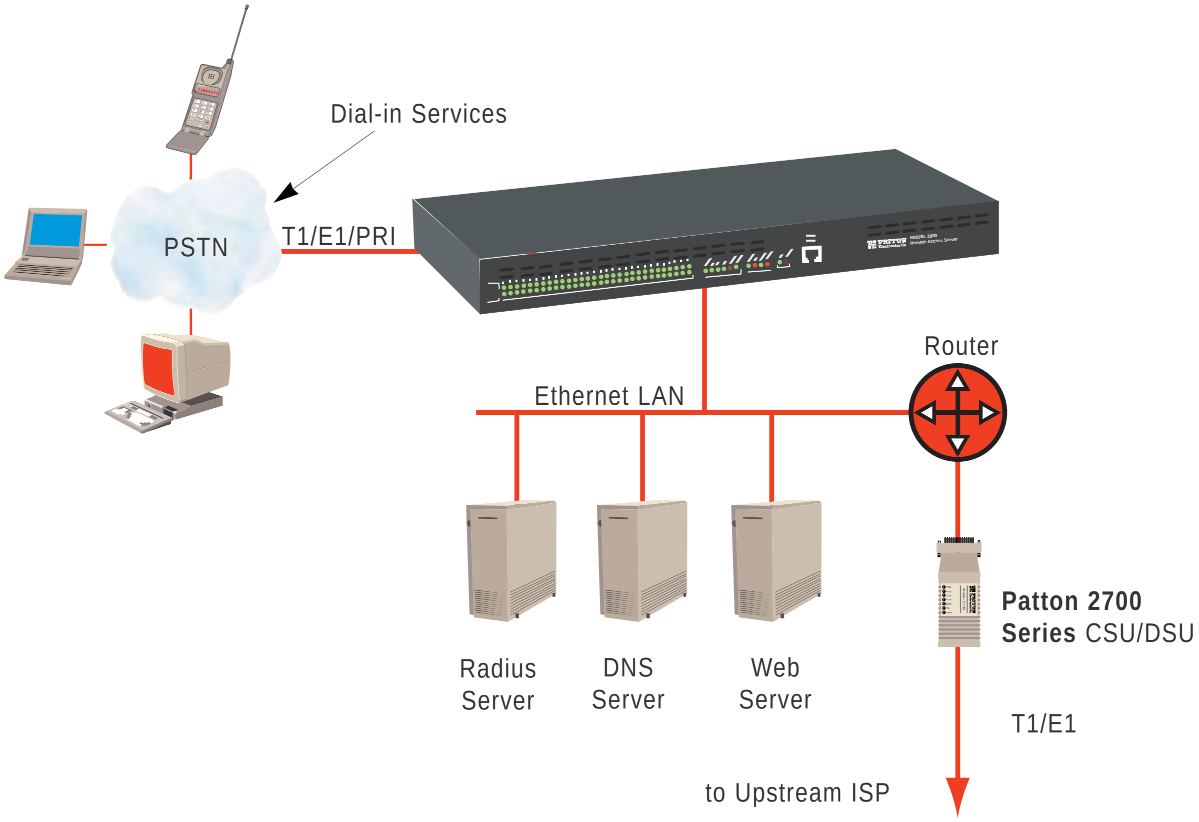
When dial-up network users cover a large region, several 2800s can be deployed in local calling areas and linked through Frame Relay.

#5

Corporate Voice/Data Integration

The 2800 RAS offers a drop and insert connection to the corporate PABX, allowing voice and data access through a single T1/E1 line.

#1 ISP Access

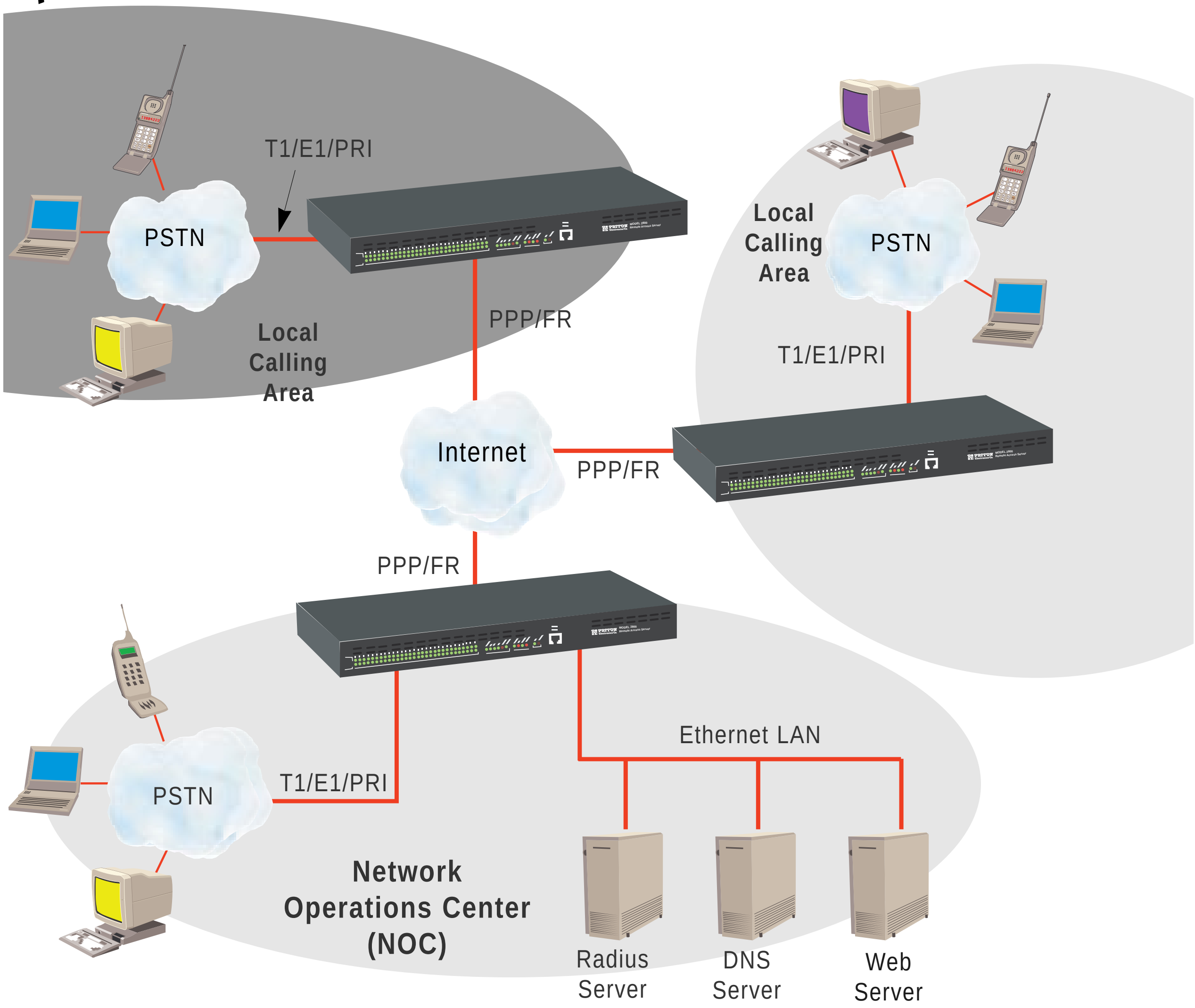


Most Internet Service Providers (ISPs) begin operations by offering service to smaller communities of individuals in a distinct geographical area. The 2800 Remote Access Server is ideal for this start-up situation. In the configuration above, the 2800 RAS provides dial-up analog and digital modem services for up to 24 users on a T1/PRI (or 30 users on an E1/PRI) port.

The 2800 RAS connects directly to the Public Switched Telephone Network (PSTN) through a T1/E1 or PRI port. With its built-in 10Mbps Ethernet port, the 2800 RAS also communicates directly to local servers through a low-cost Ethernet Hub. As users dial in to the 2800, modem calls are answered by one of the processors on the board. IP addresses are provided and users are authenticated.

The 2800 RAS provides an additional T1/E1 port for a direct up-link to an external Router or Frame Relay device by using PPP or Frame Relay, respectively. All required functionality--analog and digital modems, IP routing and WAN forwarding--is available in one compact rack-mountable package. Now, new ISPs are not forced to purchase high-end solutions to provide advanced Internet services to their customers!

#2 ISP Expansion

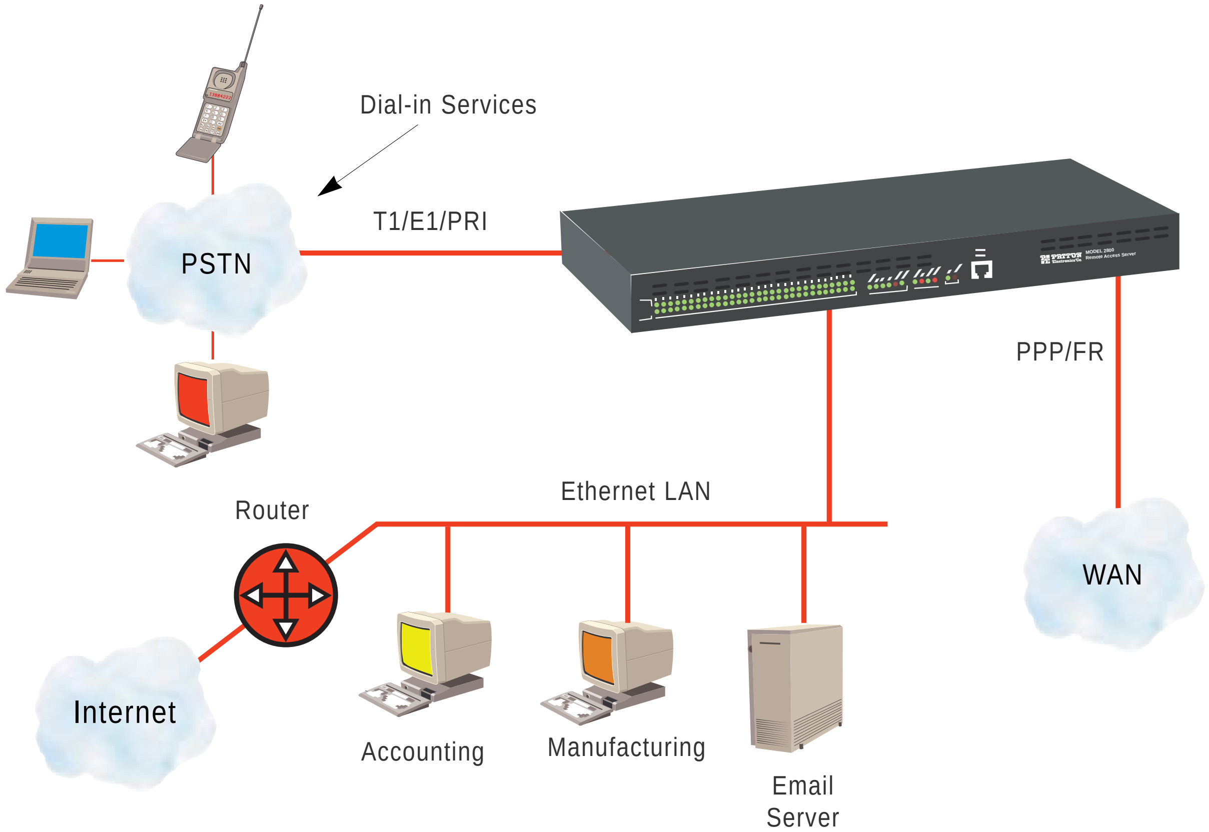


After providing service in a particular location, ISPs will typically expand their regional coverage by establishing a point of presence in another calling area--often through a local phone number in that new area.

In the new calling area, the 2800 RAS provides dial-up analog and digital modem services for up to 24 or 30 users over a T1/E1 or PRI port. For connection to the network operations center, the 2800 backhauls traffic through its second T1/E1 port using PPP or Frame Relay protocols.

To minimize service costs and potential disruptions, ISPs generally prefer to maintain their Web, authentication and email servers at a central site. The 2800 RAS allows ISPs to maintain a central NOC while expanding service into new calling areas. ISPs can aggressively expand service coverage while maintaining a low-cost operating profile.

#3 Corporate Network Access

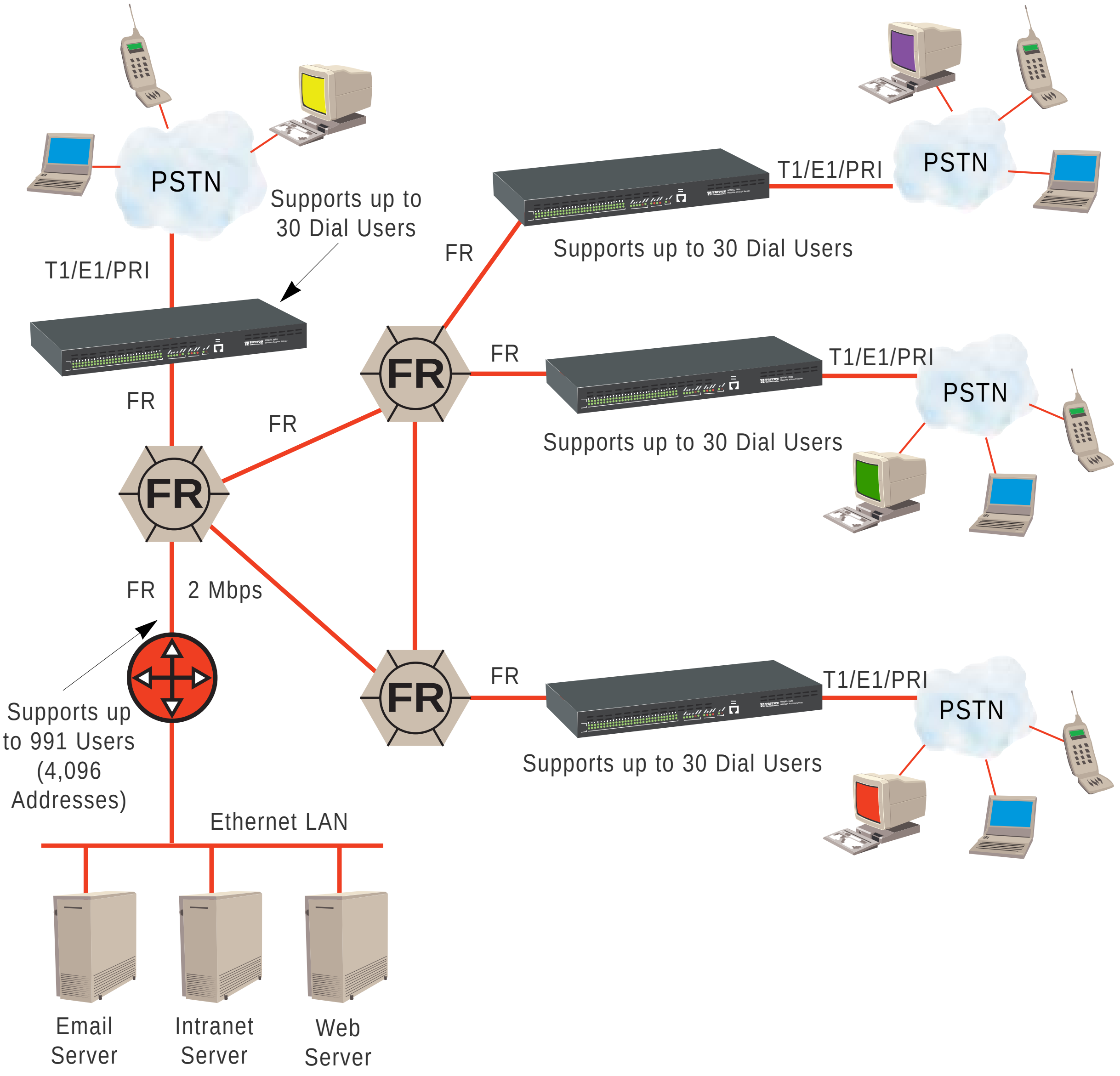


With the growth of work-at-home, remote offices, flexible work hours and email as a business communication tool, many businesses have selected Internet based technologies for their new corporate information networks (intranets). As these intranets have formed, employees need to use the corporate LAN for email, online information and Internet access. The 2800 RAS provides these vital corporate services.

Through a regular phone call to the 2800 RAS, up to 30 simultaneous users can access the corporate intranet with digital or analog modems. The 2800 answers these modem calls through its T1/E1 or PRI connection to the Public Switched Telephone Network (PSTN).

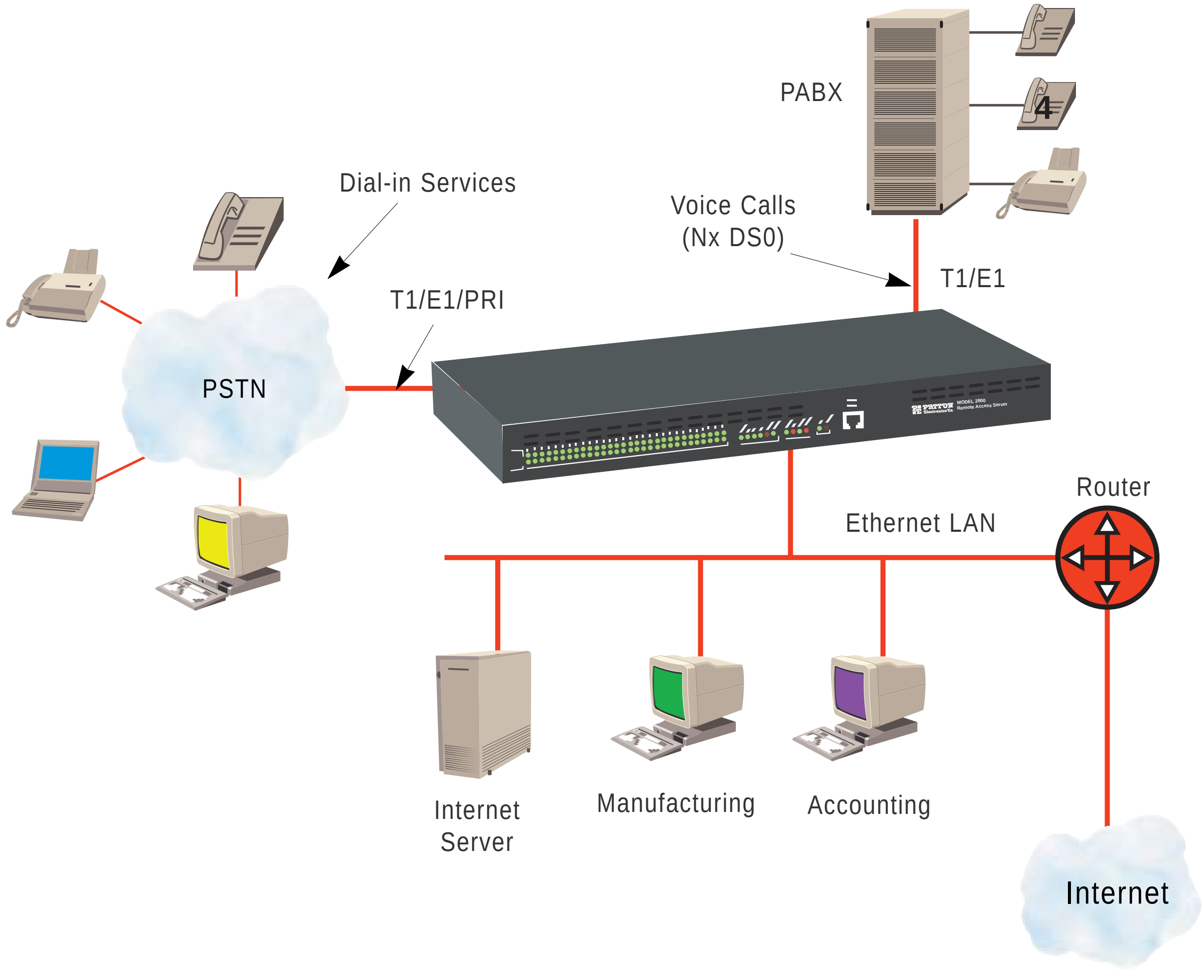
As users dial in to the 2800, modem calls are answered by one of the on-board processors. An integrated Ethernet port allows the 2800 to provide access to the corporate servers on the LAN. Authorization and authentication protect corporate information while accounting documents users of dial-in services. By connecting the 2nd T1/E1 port to a Frame Relay or a PPP link, 2800 RAS will also integrate a branch office into a larger corporate network or provide a link to Internet access.

#4 Dial Access for Wide Area Networks



As corporations opt to outsource their dial-up connections for travelling salespersons, dealer networks and remote users, telecommunication service providers are deploying remote access servers in local calling areas. The 2800 RAS can answer up to 30 calls and place the IP packets on a Frame Relay port to a FR switch (or send PPP packets to a router). With the 2800 and Frame Relay, corporate network users remove the complexity and use a simple IP router to receive dial-in calls. They also increase the density of user sessions on a T1/E1 port from 24-30 to 991.

#5 Corporate Voice/Data Integration



Prudent business practices dictate maintaining low costs while maximizing equipment and facilities usage. The 2800 RAS achieves this through the integration of both corporate voice and remote access services. By using the 2^{nd} T1/E1 and Drop-and-Insert functionality, the 2800 RAS supports both voice and data access on a single T1/E1 connection.

Connecting to the primary T1/E1, the 2800 RAS can be programmed to direct one or more channels (DS0s) of voice traffic onto a PABX. This allows the 2800 RAS to answer remote access calls and the PABX to handle corporate voice calls.

The 2800 RAS supports the flexible integration of voice service into the corporate data network, making better use of valuable corporate resources than ever before!

System Requirements

Before you can fully install and configure your 2800 please make sure you have these items available.

- One or more active T1/E1/PRI lines
- An Ethernet connection to your local LAN
- A locally connected workstation (e.g. PC) that you can use to PING and HTTP into the 2800
- A VT100 terminal or VT100 terminal emulation program for connecting to the EIA-232 configuration port
- An IP address and subnet mask for the Model 2800
- The network address space and netmask
- The IP address for the default gateway

Checking the Contents

The following are included at time of shipment. Please take a moment to account for the following items:

Model 2800 Contents

Quantity	Description
1	2800 Series Programmable Access Router (2800)
1	Operations Manual
1	UPC Standard Power Cable

Making Connections

The 2800 is equipped with two T1/E1/PRI ports, an Ethernet AUI port, and 10BaseT port, a front panel RS-232 configuration port, and an IEC power entry port. This section describes how to connect to each of these ports, as well as how to provision the T1/E1/PR1 ports. Figure 1-1 and 1-2 show the rear and front panels of the 2800, respectively.

Figure 1-1. 2800 Rear Panel

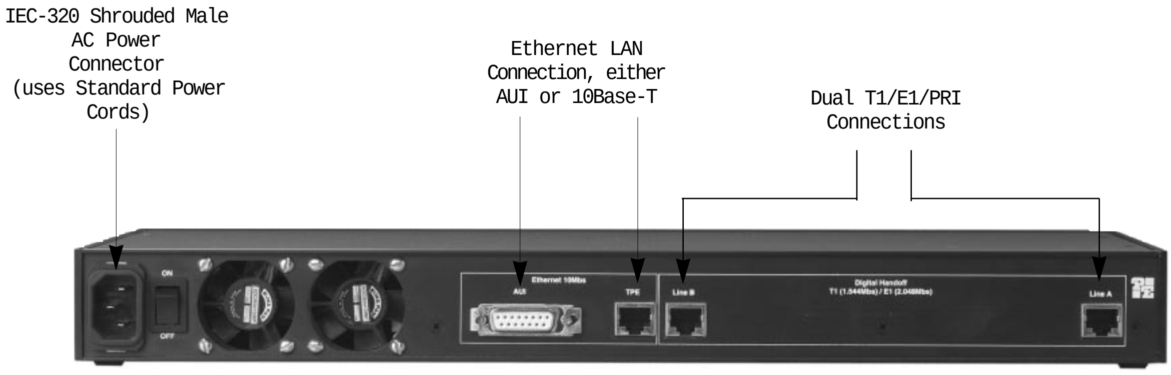
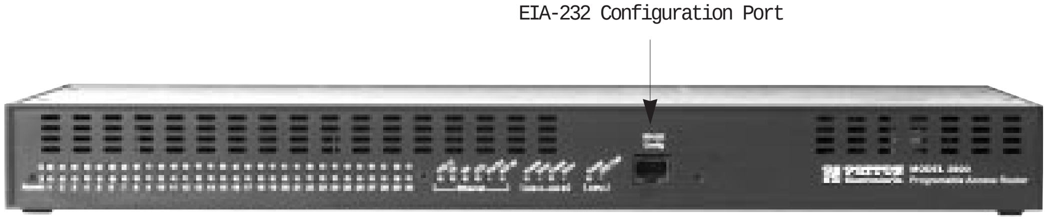

IEC-320 Shrouded Male AC Power Connector (uses Standard Power Cords)
Ethernet LAN Connection, either AUI or 10Base-T
Dual T1/E1/PRI Connections

Figure 1-2. 2800 Front Panel



Connecting the Ethernet Ports

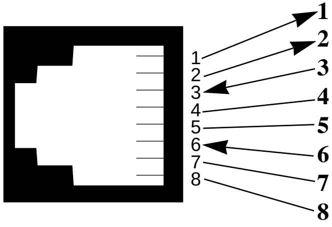
The 2800 has AUI and 10BaseT interfaces for connection to your Ethernet LAN. The 2800 may be connected directly to an Ethernet hub via RJ-45 cable, or to a host or backbone directly via DB-15 AUI cable or an AUI to 10Base2 transceiver. This section describes how to connect the 2800 to the Ethernet LAN using several different media types.

NOTE: Breaking LAN continuity by inserting a 10Base2 or 10Base5 cable segment or removing 50 Ohm terminations will disrupt and disable the Ethernet LAN. Therefore, we recommend that you disable 10Base2or 10Base5 network operations prior to installing the Model 2800.

Connecting the 10BaseT Ethernet Port

The RJ-45 Ethernet port on the rear of the 2800 is designed to connect directly to a 10BaseT network. The diagram below shows the 10BaseT RJ-45 port pin description. Please refer to the instructions below when constructing cables to connect 10BaseT ports to the Patton 2800. You may make connections up to 330 feet using Type 4 or 5 cable.

Figure 1-3. 2800 10BaseT Ethernet Port

RJ-45 Jack	Signal Name	Direction
	**1 (TX+) Transmit Data +**	**Output**
	2 (TX-) Transmit Data -	**Output**
	3 (RX+) Receive Data +	**Input**
	4	
	5	
	6 (RX-) Receive Data -	**Input**
	7	
	8	

Connecting a 10BaseT Hub to the 2800

The Ethernet 10BaseT port on the rear of the 2800 is designed to connect directly to a 10BaseT hub or repeater using RJ-45 unshielded twisted pair cable that is wired straight *through* . Follow the diagram below to construct a *straight through* cable to connect a 10BaseT Hub to the 2800's 10BaseT port.

10BaseT Hub **RJ-45 Pin No.**		**2800 10BaseT Port** **RJ-45 Pin No.**
1 (RX+)	←	1 (TX+)
2 (RX-)	←	2 (TX-)
3 (TX+)	→	3 (RX+)
6 (TX-)	→	6 (RX-)

Connecting a 10BaseT Workstation to the 2800

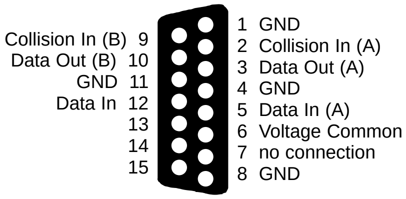
The 10BaseT port on the 2800 may also be connected directly to a 10BaseT workstation by means of a cross-connect cable. Follow the diagram below to build a cross-connect cable to connect the 10BaseT port on a workstations NIC to the 2800 10BaseT port.

10BaseT WorkStation **RJ-45 Pin No.**		**2800 10BaseT Port** **RJ-45 Pin No.**
1 (TX+)	→	3 (RX+)
2 (TX-)	→	6 (RX-)
3 (RX+)	←	1 (TX+)
6 (RX-)	←	2 (TX-)

Connecting to the AUI Ethernet Port

The 2800 incorporates one female (DTE) DB-15 AUI port for connection to a transceiver or other 802.3 DCE device. This port is located on the rear panel. Several different types of transceivers can be used—10BaseT, 10Base2, 10Base5 or FOIRL—and these may be plugged in directly or attached using an AUI cable up to 165 feet in length. We recommend that you use the shortest possible AUI cable.

Figure 1-4. 2800 AUI Interface



Connecting a Transceiver to the 2800 AUI Port

The DB-15 female AUI port on the 2800 is designed to interface directly with a DB-15 male AUI to 10BaseT, 10Base2, or FOIRL transceiver either directly or via an AUI cable (see below)

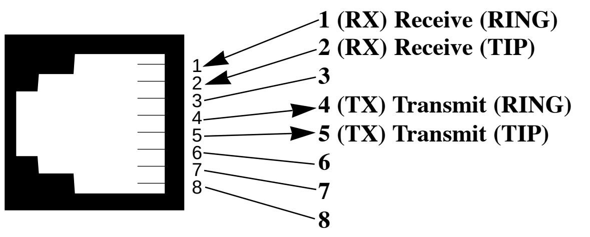
.

Tranceiver AUI Port **DB-15M Pin No.**		**2800 AUI Port** **DB-15F Pin No.**
3 Data Out (A)	◄────	3 Data Out (A)
10 Data Out (B)	◄────	10 Data Out (B)
5 Data In (A)	────►	5 Data In (A)
12 Data In (B)	────►	12 Data In (B)
2 Collision In (A)	────►	2 Collision In (A)
9 Collision In (B)	────►	9 Collision In (B)

Connecting the T1/E1/PRI Port

An active T1/E1/PRI is not necessary to configure the 2800. However, an active T1/E1/PRI connection is required to receive or make calls. The default configuration of the 2800 has the primary T1/E1 port enabled and the secondary T1/E1 port disabled. Figure 1-5, below, shows the pin assignments on the T1/E1 RJ48C jack of the 2800.

Figure 1-5. 2800 T1/E1/PRI Interface



1. Attach the T1 cable from the telephone network to the Primary T1/E1 port (RJ-45) on the 2800.
2. The Link A Frame LED should illuminate indicating the 2800 is synchronizing to the T1/E1 signal.
3. After five seconds the Link A Error LED will begin to flash indicating that the Modem 2800 is satisfied with the consistency of the T1 signal.
4. After ten seconds the Link A Error LED will go off indicating that the 2800 is satisfied with the T1 signal and the link is ready for use.

If the 2800 does not respond as described above then the most likely cause is that the default settings of the 2800 are not consistent with the T1/E1 line. In this case, use the RS-232 front panel port to modify the 2800 settings. This will require the examination of the T1/E1 Link section in the configuration pages in the 2800.

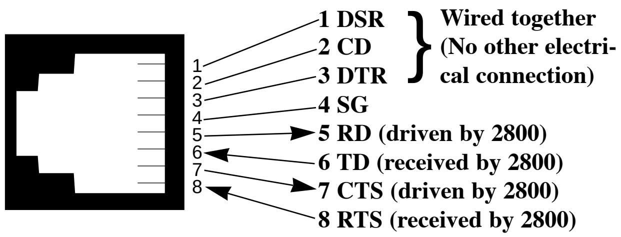
Connecting the Power Supply

Ensure that the 2800 is turned off. The power switch is on the back next to the power cable entry. The 2800 incorporates a 90-260 VAC 50/60/400 Hz universal input power supply. Use the power cable, provided with the 2800, to provide power to the Unit. Turn the 2800 on using the power switch. You should see the front panel LEDs flash as the 2800 runs through its bootstrap sequence.

Connecting the EIA-232 Configuration Port

The RS-232 configuration port on the front panel of the 2800 is configured as DCE. Using the enclosed RJ-45 serial cable, connect the 2800 Configuration port to the Personal Computer serial communications port.

Figure 1-6. 2800 RS-232 Front Panel Configuration Port



Using personal computer communications software (Procomm, Windows Terminal, BitCom, PC Anywhere, etc.), set the configuration of your communications software to the following parameters:

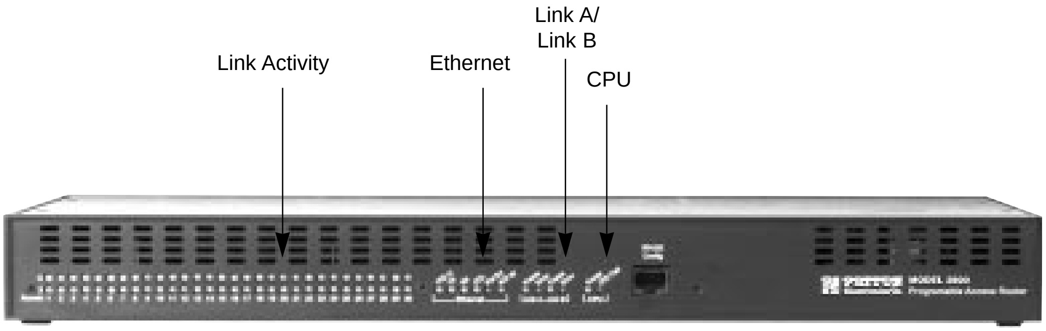
***Data Rate:=**	19,200 bps
Async. Character Format:=	8 Data Bits, 1 Stop Bit, No Parity
Terminal Emulation:=	VT-100 (or similar) terminal emulation

***NOTE:** 19.2 kbps is currently the only data rate supported on the EIA-232 configuration port.

Reading the LED Indicators

The 2800 front panel has numerous status LED's to visually inform of the current operations status and health of the 2800. Figure 1-7 shows the LED on the 2800 front panel.

Figure 1-7. 2800 Front Panel Showing LED Indicators



Link Activity LED Indicators

The first group of LED is the Link Activity group. There two rows of LED's, one row for LINK A and one row for LINK B. There is an LED for each channel, or time slot, on each WAN connection. If you have the T1 version of the 2800, only LED's 1-24 will be active. If you have the E1 version, LED's 1-30 will be active.

TABLE 1-1. Link Activity LED Status Indicators

LED	Function/Color	Description

Link A	Channel Link
	Green
		Off = Idle
		On= Active
		Double Pulse = ringing
		Flashing = connecting

Link B	Channel Link
	Green
		Off = Idle
		On= Active
		Double Pulse = ringing
		Flashing = connecting

Ethernet LED Indicators

The second group of LED is the Ethernet group. The Ethernet group LED's convey which interface is selected, activity and collisions on the Ethernet link.

TABLE 1-2. Ethernet LED Status Indicators

LED	Function/Color	Description
TPE LI	Twisted Pair Link Indication Green	On = 10Base-T Ethernet is the active LAN connection Off = 10Base-T is not the active LAN connection
TX	Transmit Data from PAR-1 to LAN Green	On = Data is being transmitted Off = No Data is being transmitted
RX	Receive Data to PAR-1 from LAN Green	On = Data is being received Off = No Data is being received

COL	Collision Detected on Ethernet
	Green
		On = Collision Detected
		Off = No Collision Detected

POL ERR*	Polarity Error Red	On = Polarity is reversed on 10BaseT connection Off = Polarity is correct on 10BaseT connection
AUI up	Attachment Unit Interface Green	On = AUI port is being used or no connection either Ethernet port

* **NOTE**: The 2800 will correct for polarity errors in the ethernet line automatically.

Link A/Link B LED Indicators

The third group of LED is the LINK A/LINK B group. This group of LED's monitor the Link A and Link B WAN connections and display the health status of the WAN connections.

TABLE 1-3. Link A/Link B LED Status Indicators

LED	Function/Color	Description

Frame	Frame
	Green
		On = WAN Link is in Frame
		Off = PAR-1 is not detecting a WAN signal
		Flashing = PAR-1 detects out of frame signal
		Flashing = connecting

Error	Error Condition Red	On = WAN link is unavailable communications Off = WAN link is available for communications

CPU LED Indicators

The forth group of LED's are the CPU group. The CPU group of LED's show that power is applied to the 2800 and that health of the CPU.

TABLE 1-4. CPU LED Status Indicators

LED	Function/Color	Description

Power	Power Condition
	Green
		On = Power is on
		Off = Power is off

CPU Fail	Channel Link Red	On = CPU Boot Failure Off = CPU executed internal bootstrap program successfully

Specifications

Architecture

1,023 MIPS (Million Instructions per Second) maximum sustained performance via integrated RISC CPU
Multiple DSPs (Digital Signal Processors)
4 Mbytes Flash
8 Mbytes DRAM, expandable to 32 Mbytes
Serial Connection: one RS-232 (RJ-45) configuration port
System monitoring with "watchdog" automatic reset
POST diagnostics of all sub-systems

PSTN T1/E1/PRI

Supports up to 24 (T1 μ-law PCM) or 30 (E1 A-law PCM) dial-in connections
Framing formats: T1 - ESF and D4; E1-double frame, CRC4 and multiframe
Line encoding: T1 - AMI, B8ZS; E1 – AMI, HBD3
Signalling: T1 - Robbed Bit (Ground start or Loop start) or Q.931 (PRI); E1 – ITU-T MFR2 or Q.931 (PRI)
T1/E1 Drop-and-Insert time slot passthrough (T1-to-T1 or E1/R2-to-E1/R2)
AIS (Alarm Indication Signal) and Yellow alarm detection and dynamic generation
Error monitoring of frame bit error, BPV and CRC error
Error monitoring of Lost Carrier, CRC error, Short Frame and others
Network loop diagnostics

LAN Connection

802.3 AUI and 10Base-T Ethernet Port with high speed 32-bit LAN coprocessor Auto-Polarity Correction

Physicals

Front panel: RJ-45 connector for control port; LED indicators monitor T1/E1 channel status, T1/E1 line status and errors, Ethernet Status and errors

Rear panel: Dual T1/E1/PRI network interface connections; one DB-15F and one RJ-45 802.3 Ethernet connection; one IEC-320 shrouded male power connector, dual independent cooling fans

Dimensions: 17" wide x 8" deep x 1.75" High (432 mm x 203 mm x 44 mm)

Weight: 4.5# (2.0 kg)

Environmental: 32–104F (0-40C); 0-15000' (0-4572 M); Operating Humidity 5-90% non-condensing

Power Supply: Internal Universal Input 90-260 VAC, 50/60/400 Hz, 35 Watts, IEC-320 shrouded male connector

Compliance: FCC Part 15, Class A; FCC Part 68; UL1950, Canadian cMET, Canadian CS-03, EMC Directive 89/336/EEC; Low Voltage Directive 73/23/EEC (EN60950); CTR-4; Year 2000 Compliant

Analog and Digital Modem Services

Supports up to 30 concurrent dial-up connections, either analog (V.34+) or digital (K56flex™/V.90/ISDN)
Modem modulations: K56Flex, V.34 Annex 12, V.34, V.8, V.32bis, V.32, V.22, V.22bis, V.23, V.21, Bell 212A, Bell 103, Bell 202, EIA PN-2330
Software sync/async receiver/transmitter for V.14
V.42/V.42bis error correction and compression

Protocol Services

TCP/IP Suite with extensive protocol statistics
ICMP/TFTP/FTP
Ethernet ARP, Proxy ARP and RARP protocols
Point-to-point protocol (PPP)
SLIP protocol
Van Jacobson TCP header compression
PPP address and protocol compression
RADIUS Authentication and Accounting with support for primary and secondary servers
Internal Call History/Progress and Statistics
RIP & RIPv2 dynamic route distribution
User configurable static routes
TCP clear connection

Management Services

Out-of-Band RS-232 configuration port for management and control
Remote software upgrade via TFTP or FTP to internal FLASH memory
SNMP version 1 configuration management
Support for MIB-II (RFC-1213), DS1 MIB (RFC-1406), RIPv2 MIB (RFC 1389), Ethernet MIB (RFC-1643) and Patton's enterprise MIB
System logging to configuration port, non-volatile FLASH, volatile RAM, SYSLOG Daemon, and SNMP trap
RADIUS Accounting
Dial-in dynamic IP address pool management
User configurable login prompts and banners
Status reporting of all Model 2800 parameters
Built in HTTP server for complete configuration and control using a standard Web browser

Security

Internal database of over 100 static users
RADIUS Client supporting dual Authorization and Accounting servers
Framed connections: PPP PAP & CHAP
Unframed connections: User name login and password
Dual SNMP/HTTP passwords for monitor and superuser access levels

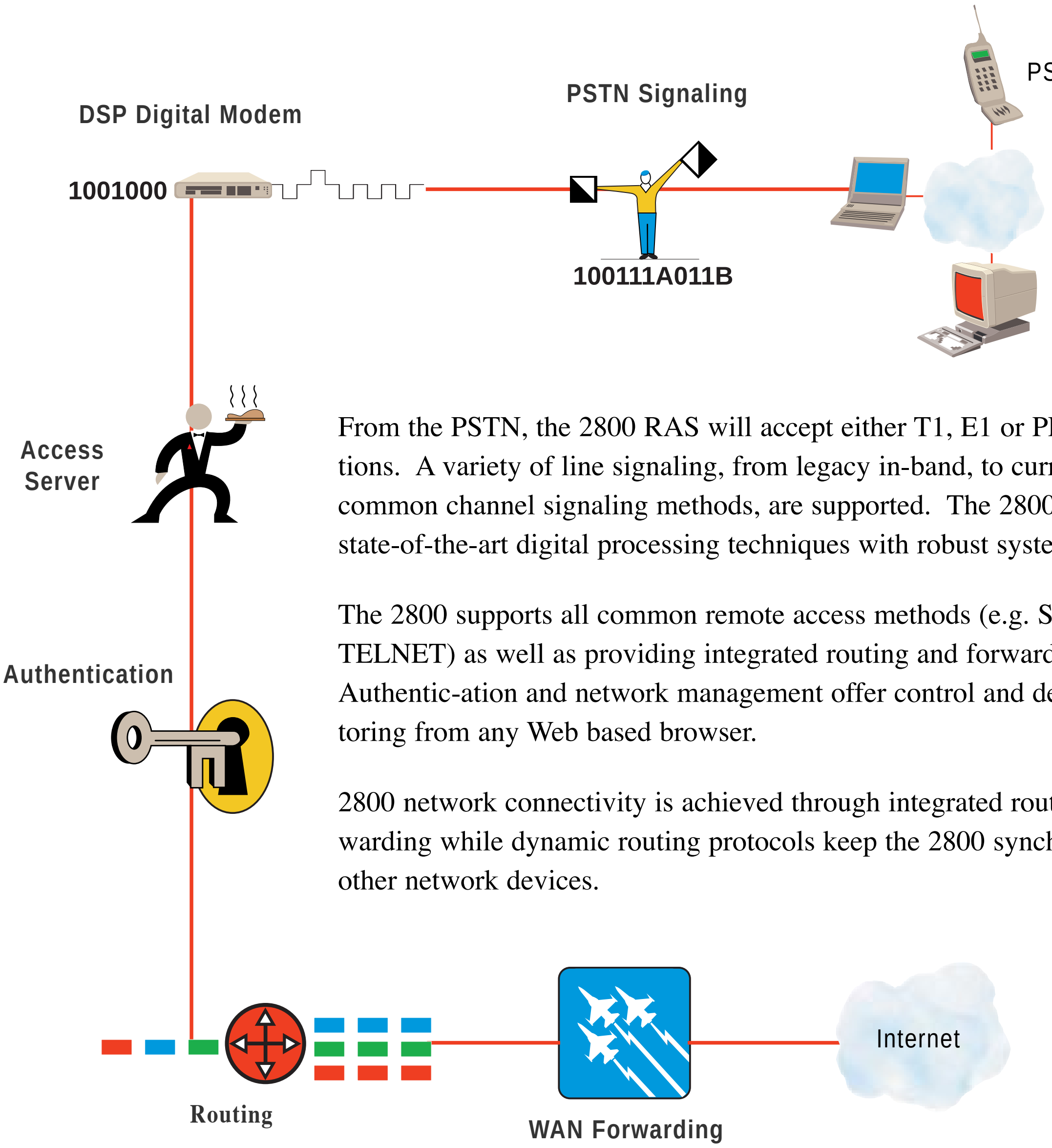
2

Getting Started

Table of Contents

How the 2800 Works

Legacy solutions using analog-to-digital conversion result in lower connection speeds. These same solutions also require separate analog modems and ISDN terminal adapters. The 2800's significant advantage is in the use of digital signal processors (DSPs) as dynamic communications processors. The 2800 DSPs terminate both analog and ISDN connections within the same hardware and using the same PSTN trunk--thus ensuring the highest possible connecting speeds.

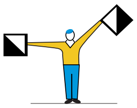


From the PSTN, the 2800 RAS will accept either T1, E1 or PRI connections. A variety of line signaling, from legacy in-band, to current ISDN common channel signaling methods, are supported. The 2800 combines state-of-the-art digital processing techniques with robust system software.

The 2800 supports all common remote access methods (e.g. SLIP, PPP, TELNET) as well as providing integrated routing and forwarding. Authentic-ation and network management offer control and detailed monitoring from any Web based browser.

2800 network connectivity is achieved through integrated routing and forwarding while dynamic routing protocols keep the 2800 synchronized with other network devices.

PSTN SIGNALLING



The PSTN trunk connections are terminated by the 2800 through one or two T1/E1 or PRI network line interfaces, according to ITU-T G.703/G.704 and ANSI T1.403 specifications. The 2800 provides two RJ-48C ports for the PSTN network connections and incorporates receive and transmit circuitry for T1/E1 long haul applications. Adaptively controlled receive equalization adjusts the incoming receive line for attenuation and crosstalk. The PSTN communicates call processing information to the 2800 using two basic signaling methods: Channel Associated Signaling (CAS) and Common Channel Signaling (CCS).

Channel Associated Signaling (CAS)

CAS is a method of signaling whereby call processing information is imbedded within the call. In T1 operation CAS is accomplished using Robbed-Bit signaling. This type of in-band signaling steals each DS0’s least significant bit every six frames. This allows the indication of the signaling state and is the method used to relay call information such as off-hook, busy, and ringing.In E1 environments, CAS is accomplished using MFR2 signalling. MFR2 is an international signaling system which uses six tones to provide end-to-end signaling of address (phone numbers) and call information. Time-slot 16 is used to convey signaling status such as answer, seizure and acknowledge. As R2 implementations within international regions can vary, the 2800 is designed to allow extensive user level configuration of R2 line and interregister signaling parameters. As an added feature, specific country profiles are preset in the 2800 to provided quick configuration on a country-by-country basis.

Common Channel Signaling (CCS)

CCS provides a separate data channel for call processing and is used in ISDN PRI service. The 2800 supports ISDN PRI for either T1 or E1 connections. In both T1 and E1 PRI service, a separate 64 kbps signaling channel is used by the PSTN to convey call processing information. Such information includes basic call control such as setup, maintenance and procedure messages and is independent of the path used for telephone call. The signaling also tells the 2800, at the time a call is placed, whether the call is an analog voice/modem or digital ISDN call. The 2800 is capable of supporting both types of calls on the same hardware by loading the appropriate firmware into the DSP on a per-call basis.

The ISDN Network Layer is specified by the ITU Q-series documents Q.930 through Q.939. This stan-

Switching Equipment Compatibility			
Line Interface	T1 Robbed-Bit	E1 – MFR2	T1/E1 PRI
Signaling	Robbed-Bit	MFR2	Q.931
Australia: AUSTEL TS014			
Europe: Euro ISDN (CTR 4)			
Japan: INS-1500			
North America: National ISDN-1, AT&T 5ESS, Northern Telecom DMS-10			

dard specifies how terminal equipment communicates with the central office switch through the call setup dialogue, although different switching equipment may require different dialogues. For Q.931 operation, the 2800 RAS supports CTR-4, NET5, TS014, INS1500, NI1, AT&T/Lucent and DMS switching equipment.

DSP DIGITAL MODEM

The 2800 T1/E1/PRI line termination connects to the DSPs via an internal PCM highway. The 2800's DSPs process the PCM channel information directly from the PSTN and are TDM time-slot aware--specifically designed to interface with T1/E1/PRI connections. Organized as a resource pool, the DSPs processes PCM data from the PSTN without analog to digital conversion. The DSP resource pool contains up to thirty DSPs: each with over 40 MIPS of processing power, and each is dynamically assigned to process a specific time-slot at call set-up. Functioning as full-duplex digital communications processors, the DSPs are not committed to performing a specific task. The same hardware can function as an analog V.34+ modem on one call, and process a digital ISDN call on the next. Being software driven, DSP processing provides an inherent migration path to future technologies.

Processing V.34+ Calls

At the time a modem call arrives, a DSP will be placed into service to process the call. The DSP will be assigned to respond to the PCM channel information for that time-slot. (PCM is simply the digital encoding of an analog waveform.) In a V.34+ or similar analog modem call, the DSPs will take this digital encoding and process the call as a V.34+ modem. The 2800 allows for configuration on how the DSP modems will negotiate an incoming call. The user can select maximum and minimum speeds, as well as which modulations should be allowed. Operational characteristics--such as transmit power, carrier loss duration, and V.42/V.42bis error correction and compression--can be user configured to permit flexibility.

Processing ISDN Calls

Integrated Services Digital Network (ISDN) provides a high-speed digital connection to the telephone company network. The B channel, which is a circuit switched connection, is a 64 kbps clear channel pipe. The complete bandwidth is available for data, as call setup and other signaling is done through the D channel. The 2800 RAS can support synchronous PPP to connect remote ISDN Terminal Adapters (TA) over B channels. Using Multilink PPP (MP), multiple 64kbps channels can be "glued" together to permit larger bandwidth connections as well as bandwidth on demand.

Processing 56K Calls

In an effort to bring faster connections to users, new standardized modem technology has been deployed. In the modernized all-digital infrastructure of the PSTN, most telephone calls now go through a single analog-to-digital conversion and thus remain in the digital domain. New modem standards, such as K56Flex™ and V.90, leverage this modern infrastructure to allow high-speed downstream data transfer. The 2800's DSPs negotiate these new modulations by loading V.8bis for call processing. The 2800, being a software-driven device, easily adapts to new modem standards as they develop--only a FLASH software upgrade is required.

The 2800's DSPs do more than process analog or digital modem calls; Layer 2 processing, data buffering, PPP escaping and V.42 flow control are also performed within the DSPs. This distributed processing model allows each individual DSP to process and buffer data without requiring the attention of the host processor for every bit received or transmitted.

ACCESS SERVER

After successfully negotiating a modem link, the 2800 allows the user to connect to protocol related services. Two types of connection to these services are available from the 2800: unframed and framed.

Unframed Connections

Unframed connections, or connections without any underlying protocol, will receive a login prompt. After the 2800 has received the login information, it will authenticate the user. The user may be authenticated against the internal user static database or through RADIUS. Upon successful authentication, the user will be granted service based on either preconfigured defaults or through specified configuration parameters.

Framed Connections

Serial Line IP (SLIP) provides an easy means to transmit IP packets from one computer to another over a serial line. In creating a SLIP connection, a login name and password are obtained and the 2800 will then authenticate the user. Upon authentication, the user will see a login "success" banner. This success banner is typically used to tell the caller what his IP address is, and to signify the start of the framed session. The 2800's success banner is user customizeable to guarantee interoperability with older SLIP clients.

The Point-to-Point Protocol (PPP) is implemented to provide a datalink connection that can establish, authenticate and manage a framed link. The 2800 RAS will automatically detect 7E flags and begin a PPP session. In the link establishment phase, the 2800 and the caller (also known as the *peer*) will negotiate network specific options.

Multilink PPP (MP) is similar to PPP in that it allows the aggregation of multiple smaller connections to create a single large bandwidth connection. (Basic Rate ISDN, supported by the 2800, offers users the possibility of opening these multiple simultaneous channels between systems. This gives users additional bandwidth on demand.) Multilink is based on an the initial LCP negotiation where each side indicates that it is capable of combining multiple physical links into a “bundle”.

Custom Configuration
The 2800 allows custom configuration of various connection parameters. For example, the 2800 can be configured to auto-detect a framed PPP connection or to initiate a specific (default) service for all callers. Other parameters, such as maximum session time, maximum idle time and login time, are also user-configurable.

AUTHENTICATION

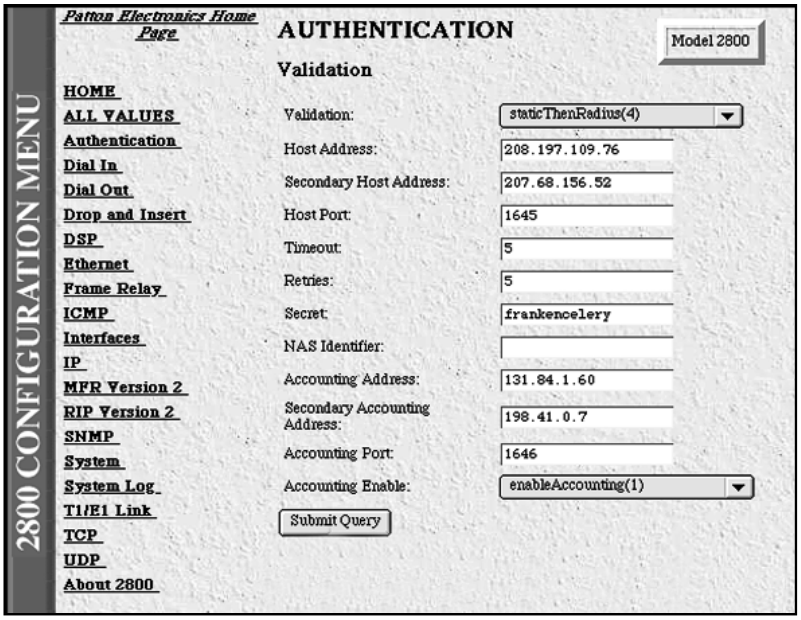
Each time a communications server permits access, the network becomes more vulnerable to security breaches. For user access control, the 2800 RAS provides two flexible authentication options: 1) local authentication by the 2800, and 2) centrally managed authentication using RADIUS.

Local Authentication

For local authentication, the 2800 RAS incorporates an internal database supporting over 100 users. Once the user connects, the 2800 will obtain the username and password of the calling party. This may be via a login prompt or as part of the PPP negotiation process. PPP authentication is processed using either the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP). In either case, the 2800 RAS will obtain the user information for processing by the 2800 authentication manager.

RADIUS Authentication

The 2800 RAS will also function as a Remote Authentication Dial-In User Service (RADIUS) client. As a RADIUS client, the 2800 is used to authenticate and authorize users via a RADIUS server.



AUTHENTICATION

Validation

Validation: staticThenRadius(4)
Host Address: 208.197.109.76
Secondary Host Address: 207.68.156.52
Host Port: 1645
Timeout: 5
Retries: 5
Secret: frankencelery
NAS Identifier:
Accounting Address: 131.84.1.60
Secondary Accounting Address: 198.41.0.7
Accounting Port: 1646
Accounting Enable: enableAccounting(1)

The RADIUS server is responsible for receiving user connection requests, performing authentication, and returning all configuration information needed by the client to deliver service to the user. All transactions between the client and server are authenticated through a shared secret. Additionally, any user passwords sent between the client and the RADIUS server in encrypted format.

The 2800 supports primary and secondary RADIUS servers for authentication and accounting. Both servers offer user-configurable timeout, retries and port selection. The 2800 supports RADIUS accounting by reporting connection initiations and terminations to the accounting server. This in turn generates reports for billing or auditing purposes.

ROUTING/FORWARDING

The 2800 IP routing mechanism is responsible for directing IP packets to their final destination by sending the packet to the “next hop.” This list of next hops is called the *routing table*. This table also holds additional routing information such as the destination, mask, and physical interface. When the 2800 receives a packet, it will scan the table for the best route. If no route is found by the 2800, the packet will be sent to the default gateway. The user can then configure static routes with the 2800, using either a gateway, host or interface route. To automatically locate the next hop for a packet, when that is possible, the 2800 RAS makes use of ARP and RIP routing protocols.

ARP

The Address Resolution Protocol (ARP) is the means by which IP addresses are associated with physical Ethernet address and is one of the two methods used by the 2800 for locating the next hop. The 2800 will respond to ARP requests for its own dialup addresses, with its IP address as the responsible router for delivering the packet. This functions even if the LAN and dialup IP addresses are on different IP networks.

RIP

To automatically update the routing table, adjacent routers must communicate using a dynamic routing protocol. The dynamic routing protocols supported by the 2800 are Routing Information Protocol (RIP) version 1 and version 2. These protocols identify which networks each router is currently connected to, and assist the 2800–along with ARP–in automatically locating the next hop for a particular IP packet.

Forwarding

Additional network connectivity can be achieved using the 2800’s second T1/E1 connection as a Frame Relay uplink. User bandwidth can be configured on a time-slot basis. Using RFC 1490 encapsulation and the 2800’s sub-interface architecture, each Data Link Connection Identifier (DLCI) is specified as its own point-to-point connection. The 2800 will then add entries in the routing table to forward packets to and from each DLCI.

NETWORK MANAGEMENT OVERVIEW

Standard network management demands nodes which can seamlessly integrate into existing network management topologies. Providing both system and user level management, the 2800 fits nicely within this model by simultaneously functioning as both a *managed node* and a *management application*.

The 2800 as a Managed Node (SNMP)

As a managed node, the 2800 RAS allows complete configuration and control using the Simple Network Management Protocol (SNMP) over the UDP protocol. SNMP defines the rules for management and the collection of management information. This model views a managed system as containing the following: managed nodes, management stations, the management protocol, and the management information. The 2800 RAS functions as a managed node using the SNMP version 1 management protocol and is compatible with management systems such as HP OpenView™ and Sun Solstice Enterprise Manager™.

The 2800 also supports industry standard Management Information Bases (MIBs), which are databases of information that a network management system can view or modify. (All object Identifiers fall under the iso.org.dod.internet tree structure.) Specifically, the 2800 supports MIB II and is able to access SNMP configuration and statistics information through standard SNMP MIBs. The 2800 also offers extended management functionality through the Patton Enterprise MIB.

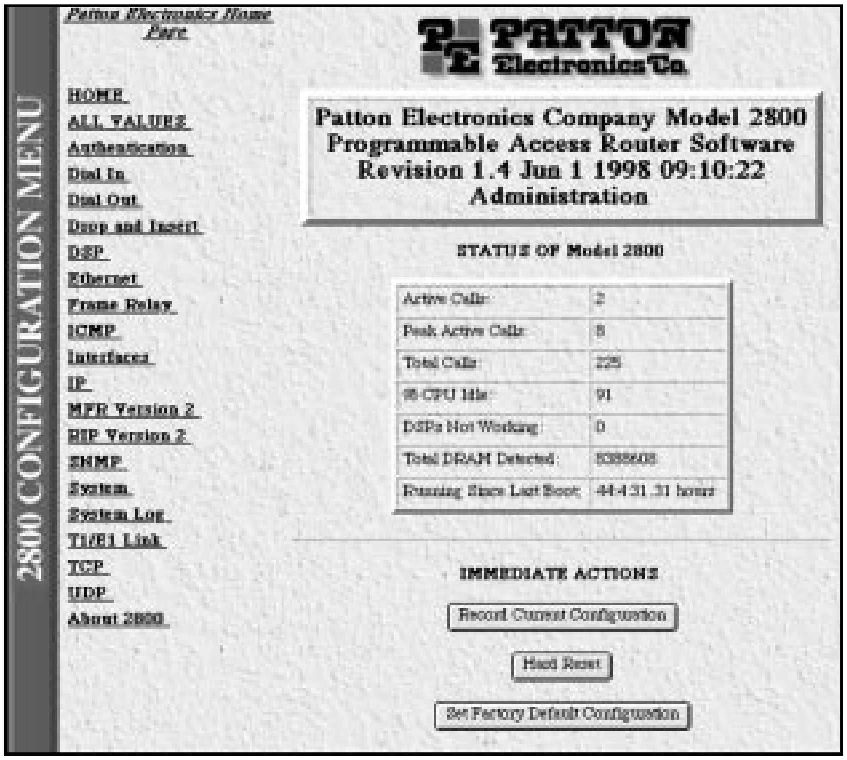
The 2800 supports two SNMP community names: one permits read-only access and the other permits read-and-write access. These community names also serve as the passwords for the Web based and control port interfaces.

The 2800 as a Management Application (HTTP)

The World Wide Web has given the computing world a graphical interface that is common and easy-to-use. Using a web browser, management and configuration information can be presented in an intuitive fashion while alleviating the need for dedicated management workstations.

As a management application, the 2800 RAS runs its own built-in HTTP (version 1.0) Web server. This allows systems equipped with standard browsers (e.g. Netscape® or Internet Explorer®) to become management stations without having to purchase expensive SNMP network management systems. They can thereby display relevant operating facts about the 2800 in an intuitive, graphical manner (see the sample screen below). Navigation using this management system is as simple as following a link or pressing “submit.” The 2800 main menu displays twenty-two separate configuration links. These links allow complete system configuration, as well as displaying all 2800 operating variables. Most variables that are configurable have drop down boxes for option selection. When the desired option is selected, it is simply submitted to the 2800 for immediate change.

Two levels of security are provided to allow controlled access to the 2800's built-in management system. A monitor level password allows viewing of all variables (except passwords). A super-user password allows complete access to all variables as well as allowing the manager to change 2800 configuration parameters.



Patton Electronics Company Model 2800
Programmable Access Router Software
Revision 1.4 Jun 1 1998 09:10:22
Administration

STATUS OF Model 2800

Active Calls:	2
Peak Active Calls:	8
Total Calls:	225
% CPU Idle:	91
DSPs Not Working:	0
Total DRAM Detected:	8388608
Running Since Last Boot:	44:4:31:31 hours

IMMEDIATE ACTIONS

Record Current Configuration
Hard Reset
Set Factory Default Configuration

User Level Management

Every time a communications server permits access from the public, the network becomes more vulnerable to security breaches. Network managers need tools to guard against intrusion while simplifying user management. As network access expands, administration of users' access and privileges creates the need for a centralized access database. For user level management, the 2800 RAS provides two options: 1) an internal database of 125 users; 2) a Remote Authentication Dial-In User Service (RADIUS) client. Depending on site size and requirements, users can be locally authenticated or the 2800 RAS can be connected to a larger, centrally located, server that multiple 2800s may use.

Booting the 2800

NOTE: If you are starting the 2800 for the first time, you must first log in via the front panel RS-232 Configuration port and set the LAN Address technique, IP address, and Subnet Mask.

1. Using personal computer communications software (Procomm, Windows Terminal, BitCom, PC Anywhere, etc.), set the configuration of your communications software to the following parameters:

***Data Rate:=**	19,200 bps
Async. Character Format:=	8 Data Bits, 1 Stop Bit, No Parity
Terminal Emulation:=	VT-100 (or similar) terminal emulation

2. Connect the RS-232/V.24 port of the terminal to the front panel RS-232 Configuration port of the 2800.

3. Turn On the 2800.

4. After the 2800 is turned on, it will enter a series of diagnostic tests to exercise the internal subsystems in the box. The terminal display during the power-up sequence will look something like the display below (the actual display will appear much longer. The following is only shown as an example):

5. The 2800 will continue on to test the DSP's, Ethernet LAN, T1/E1/PRI WAN and other interfaces. If the operational code (the code that actually runs the 2800) is verified to be valid, the 2800 will display the following login banner and user prompt:

```
Power Up
Begin: Func Test
End:   Func Test
Begin: Swap Process Control
Begin: Load fixed cache
DRAM: Configure Begin
```

```
Patton Electronics Company
PAR-1 Programmable Access Router

Username>
```

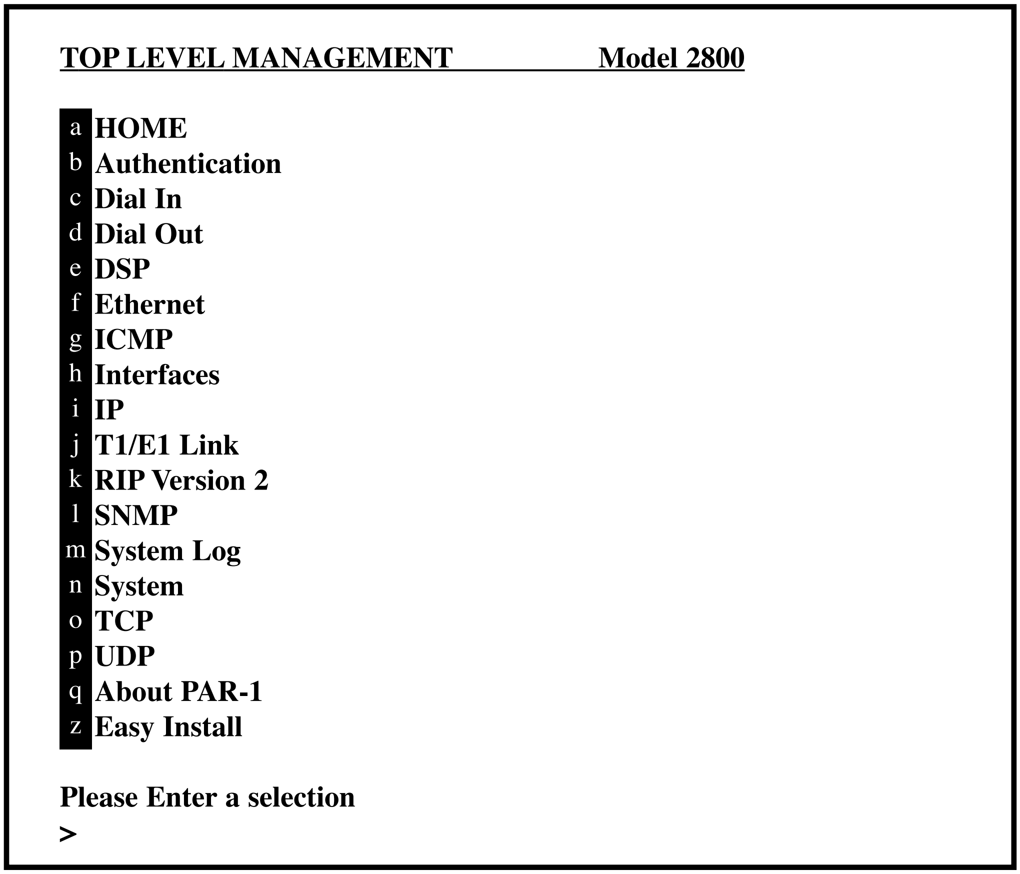
6. Enter the following Username and depress the return key:

```
Username: superuser <Enter/Cr>
```

7. Enter the following password and depress the return key:

```
Password: superuser <Enter/CR>
```

8. After you have successfully logged in, the 2800 will display the one of the main menu configuration screen. Figure 2-4 shows the configuration menu when using the front panel RS-232 configuration port.



```
TOP LEVEL MANAGEMENT              Model 2800

a HOME
b Authentication
c Dial In
d Dial Out
e DSP
f Ethernet
g ICMP
h Interfaces
i IP
j T1/E1 Link
k RIP Version 2
l SNMP
m System Log
n System
o TCP
p UDP
q About PAR-1
z Easy Install

Please Enter a selection
>
```

NOTE: All menu selections require you to depress the <Enter/CR> key after making a selection. To make a selection, depress the letter or number before the option stated. Use the left arrow key (on the PC keyboard) to return to the previous page.

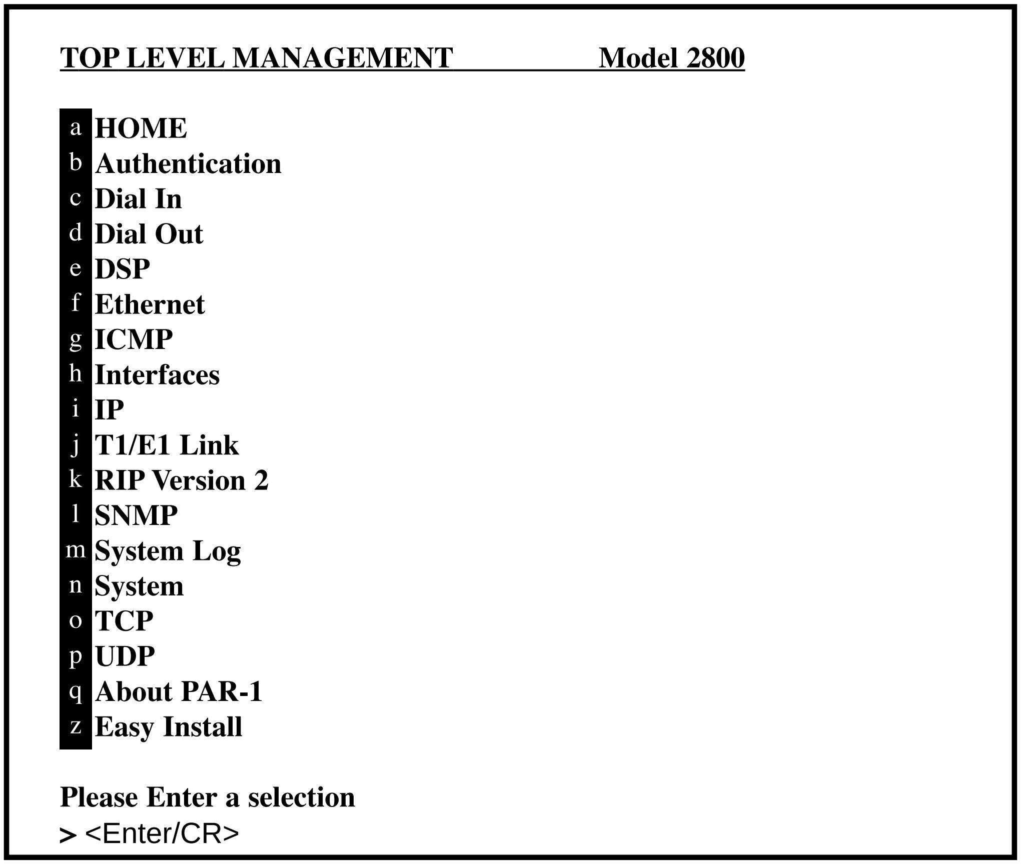
Initial Setup

In order to operate the 2800, you must define the LAN Address Technique, LAN IP address , and Subnet Mask to be dedicated for use in the 2800. You must log into the Front Panel RS-232 configuration port to complete the initial configuration. After setting the above parameters, you may change configuration settings via SNMP or HTTP management using the Front Panel RS-232 port, the LAN port or by making a remote connection to the T1/E1/PRI port.

This section describes how to set the LAN Address Technique, LAN IP Address, and Subnet Mask after you have turned on the 2800 and have successfully logged into the RS-232 Configuration port.

NOTE: Under normal circumstances, the RS-232 should be used only for 1) Initial setup; 2) Out of Band backup; and, 3) external network management.

1. Enter Option **n, System**, from the main menu, as shown below:



```
TOP LEVEL MANAGEMENT            Model 2800

a HOME
b Authentication
c Dial In
d Dial Out
e DSP
f Ethernet
g ICMP
h Interfaces
i IP
j T1/E1 Link
k RIP Version 2
l SNMP
m System Log
n System
o TCP
p UDP
q About PAR-1
z Easy Install

Please Enter a selection
> <Enter/CR>
```

2. Option **n System,** displays the following System menu.

```
SYSTEM                      Model 2800

Time Slices Fully Utilized:       60
Time Slices 90% Utilized:         19
% CPU Idle:                       99
DSPs Not Working:                 0
Running Since Last Boot:          0:10:22.17 hours

    1  Details...
    2  Test routines...
```

3. Select Option **1 Details ...** <Enter/CR>

4. Option **1 Details** displays the following system configuration information:

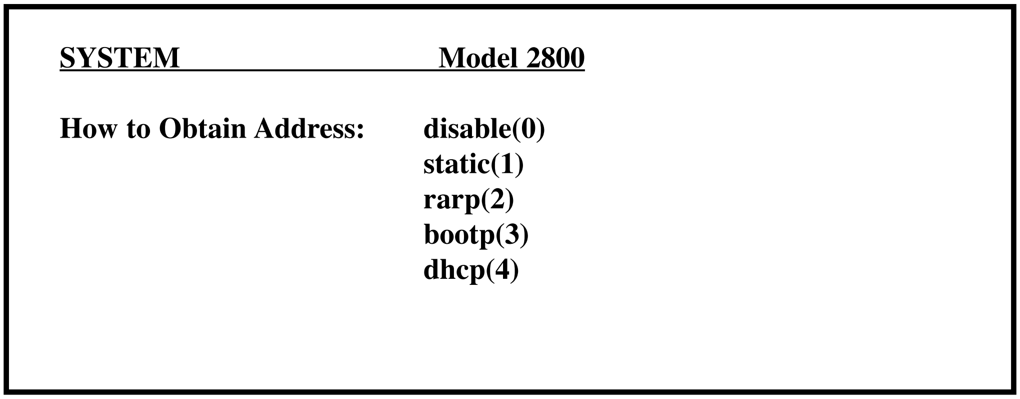
```
 SYSTEM                      Model 2800

a SNMP Version:              snmpv1(1)
b Super User Password:       superuser
c SuperUser Verification:
d User Password:             monitor
e User Verification:
f Lan address technique:     static(1)
g Lan address:               07.86.52.212
h Lan Mask:                  255.255.255.224
  Serial Number:             21.July,1997,1
  PCB Revision:              1
  General Information:
i Enable Payable Features:   0000000100000000
j Installation Country:      unitedStates(1)
  Total DRAM Detected:       8388608
  Running Since Last Boot:   0:10:48.43 hours
k System Manager:            Patton Electronics (301) 975-1000
```

5. You are now ready to set the LAN address technique, LAN IP address, and Subnet Mask as described below.

Setting the LAN Address Technique

You must select the LAN address technique in order for the 2800 to be able to determine the source of its IP address. Please refer to Chapter 16 - System for more information regarding LAN addressing. Follow the instructions below to set the LAN address technique for the initial installation of the 2800.

1 Select Option **f LAN address technique** from the SYSTEM menu.
2. The 2800 will display the following menu:



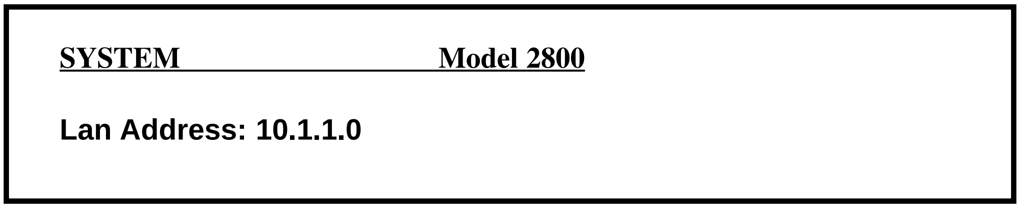
```
SYSTEM                     Model 2800

How to Obtain Address:    disable(0)
                          static(1)
                          rarp(2)
                          bootp(3)
                          dhcp(4)
```

3. Select **static(1)**
4. Press the left arrow key (<-) to return to the SYSTEM menu.

Setting the IP Address

The IP address must be the IP address dedicated to the 2800. If you will use a web browser, this will be the address that you will enter as the URL (Universal Resource Locator) in your web browser.

1. Select Option **g LAN address**, from the SYSTEM menu.
2. The 2800 will display the following:



```
SYSTEM                     Model 2800

Lan Address: 10.1.1.0
```

3. Enter the dedicated IP address for the 2800.
4. Press the left arrow key (<-) to return to the SYSTEM menu

Setting the Subnet Mask

To set the Subnet mask, select Option **h Lan Mask**, from the System Menu. If you have a class C IP address block this number will be 255.255.255.0 (also known in CIDR as /24)

1. Select Option **h Lan Mask**, from the System Menu
2. The 2800 will display the following menu:

```
SYSTEM                    Model 2800

Lan Mask:  255.255.255.0
```

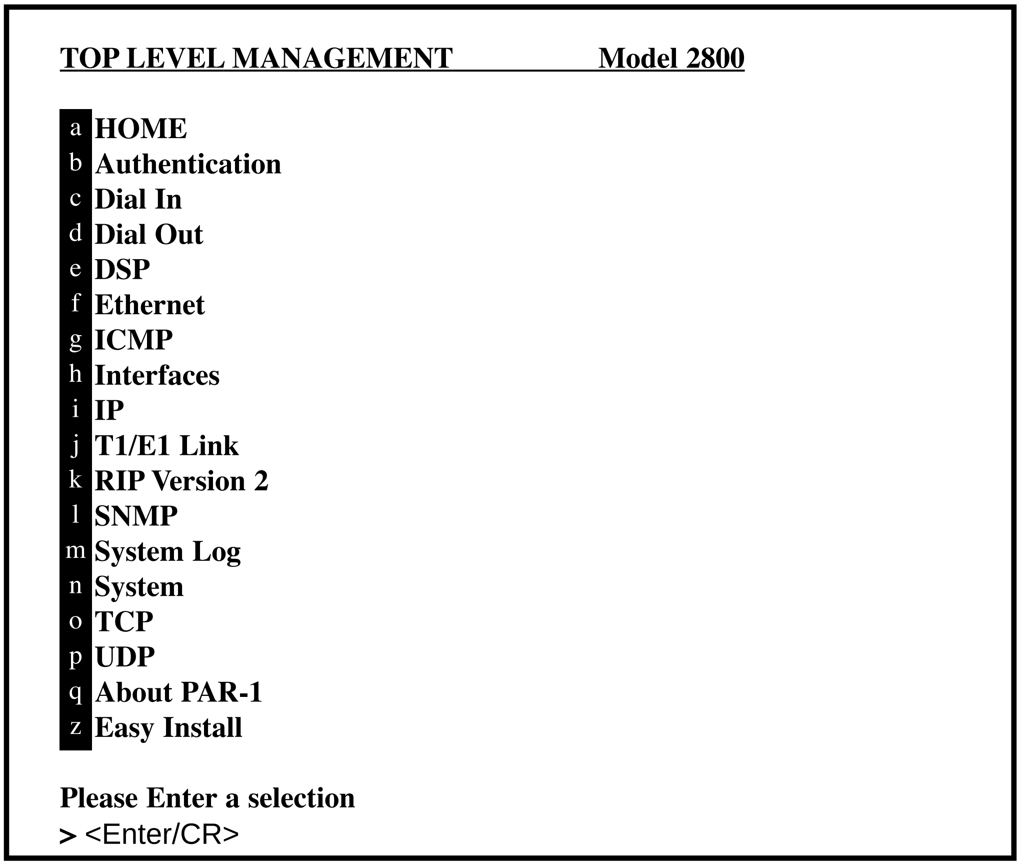
3. Enter the LAN subnet mask for the 2800
4. Press left arrow <   > to return to the Main Configuration menu

You may now configure the box by using a standard web browser such as Netscape Navigator™ or MicroSoft Explorer™ . To use the web configuration tool, connect your Ethernet port and enter the URL of your web browser ***http://your.box.ip.address***.

Saving, Re-booting and Re-setting

After setting the LAN Address Technique, IP Address, and Subnet Mask, you save the current system configuration prior to powering off the 2800. This section describes how to save the initial setup parameters, re-bootstrap the 2800, and re-install the default configuration.

1. Enter Option **a HOME**, from the main menu, as shown below:



```
TOP LEVEL MANAGEMENT              Model 2800

a HOME
b Authentication
c Dial In
d Dial Out
e DSP
f Ethernet
g ICMP
h Interfaces
i IP
j T1/E1 Link
k RIP Version 2
l SNMP
m System Log
n System
o TCP
p UDP
q About PAR-1
z Easy Install

Please Enter a selection
> <Enter/CR>
```

2. Option **n, System**, displays the following CURRENT STATUS menu:

```
CURRENT STATUS                    Model 2800

Patton Electronics Company
PAR-1 Programmable Access Router
Software Revision Aug 21 1997 16:10:52


Total Active Calls:        0
Time Slices Fully Utilized: 16
Time Slices 90% Utilized:   12
% CPU Idle:                98
DSPs Not Working:           0
Total DRAM Detected:        8388608
Running Since Last Boot:    0:58:57.49 hours

IMMEDIATE ACTIONS
storeConfig(1)
hardReset(2)
forceDefaultConfig(3)
forceDebugging(4)
```

3. You must store the initial system configuration prior to any further system configuration (**storeconfig(1)**). Otherwise, all changes will be reset to the prior system configuration the next time the 2800 is powered off or reset. You may also boot the 2800 (**hardReset(2)**); or re-install the default configuration (**forceDefaultConfig(3)**) as described below.

Saving the Current System Configuration

Any changes made to the PAR -1 configuration are stored in non-volatile RAM first. This allows you to establish a working configuration before committing any changes to FLASH, or stored memory. Any configuration changes will become permanent only after **storeConfig(1)** has been selected. Any changes made and not stored in FLASH memory will be lost when the 2800 is powered off or reset.

- Select **storeConfig(1)** from the HOME menu

Re-starting the system (warm boot)

If you would like to restart the system after making changes, select **hardReset(2)** from the CURRENT STATUS menu. After selecting **hardReset(2),** all current sessions will be dropped, the interfaces will be re-initialized and the configuration will be loaded from FLASH memory are not required to restart the system after making changes to the system configuration. All changes to the system configuration take place immediately.

- Select **hardReset(2)** from the HOME menu

Re-installing the Default Configuration

If you believe you have made an error in the initial configuration, you may reset to the default configuration of the 2800. Selecting this option will erase the configuration in FLASH memory and then load the factory default configuration into FLASH. However, in the default configuration, the LAN address technique, IP address and subnet mask are not defined. You must define these parameters to operate the 2800 over an IP network.

- Select **forceDefaultConfig(3)** from the HOME menu

T1/PRI (Message Oriented) Planning

Requesting Information from the T1/PRI Provider

Request the following information from your T1/PRI provider. This information will serve as the minimum required parameters that you will need to setting up the 2800.

- Switch Type. There are four basic switch types in North America:

TABLE 2-1. ISDN Switch Types

Switch	**Version (Protocol)**
NT DMS	Custom National ISDN-1
Siemens EWSD	National ISDN-1
AT&T 5ESS	Point-to-Point Point-to-Multipoint National ISDN-1
Other (North America)	National ISDN-1
ETSI (Other than North America)	Point-to-Point Multipoint

- One way (Inbound) Service or Two Way (Inbound/Outbound Service)
- Circuit-Switched Voice and Data (ISDN and modem calls) or Circuit Switched Data (ISDN only)
- Line Framing Type: T1/PRI = ESF or D4
  E1/PRI = CRC4
- Line Encoding Type: T1/PRI = B8ZS
  E1/PRI = HDB3
- Type of Physical Connection: U Interface, RJ-48C
- Type of Line Terminating Equipment

Setting up the 2800 for T1 Access

To make a dial in call into the 2800 for an T1 (DS1) line, you must configure the following variables. The Patton Enterprise/SNMP MIB objects are shown following each variable.

- LAN Address Technique **(boxIPAddressTechnique)**
- LAN Address **(boxIPAddress)**
- LAN Subnet Mask **(boxIPMask)**
- T1/E1 Line Type **(dsx1LineType)**
- Line Coding **(dsx1LineCoding)**
- Line Build Out **(linkLineBuildOut)**
- Signal Mode **(dsx1SignalMode)**
- Signalling Protocol **(dsx1SignallingProtocol)**
- T1/E1 Channel Assignments **(slotFunction)**
- IP Address Pool **(diIpPool)**
- Static User Name and Password **(suUsername), (suPassword)** (for static users only)

Setting up the 2800 for ISDN PRI Access

To make a dial in call into the 2800 for an ISDN PRI line, you must configure the following variables. The Patton Enterprise/SNMP MIB objects are shown following each variable.

- LAN Address Technique **(boxIPAddressTechnique)**
- LAN Address **(boxIPAddress)**
- LAN Subnet Mask **(boxIPMask)**
- T1/E1 Line Type **(dsx1LineType)**
- Line Coding **(dsx1LineCoding)**
- Transmit Clock Source **(dsx1TransmitClockSource)**
- Line Build Out **(linkLineBuildOut)**
- Signal Mode **(dsx1SignalMode)**
- Signalling Protocol **(dsx1SignallingProtocol)**
- Switch Type **(linkISDNSwitchType)**
- T1/E1 Channel Assignments **(slotFunction)**
- IP Address Pool **(diIpPool)**
- Static User Name and Password **(suUsername), (suPassword)** (for static users only)

3

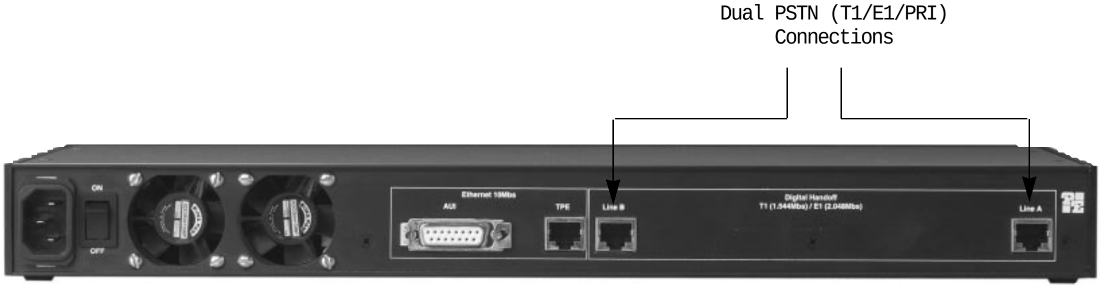
Configuring the PSTN Interface

Table of Contents

Introduction to the PSTN Interface

The 2800 RAS two built-in PSTN line connections are labeled "**Line A**" and "**Line B"** (see Figure 3-1, below). These line terminations function as both a CSU and a Channel Bank and contain all the necessary functions to properly terminate a T1/E1/PRI line. You must configure the 2800's PSTN interface to enable it to answer calls. This chapter describes how to configure the PSTN line interface using Patton's web-based management system. Consult RFC 1406 – Definitions of Managed Objects for the DS1 and E1 Interface types for more information on the T1/E1/PRI managed objects. For information on how to make physical connections to the PSTN interfaces, please refer to **Chapter 1 Introduction**.

Figure 3-1. 2800 Rear Panel



Things You Will Need to Know

In order to setup your 2800 during this initial configuration, you will need to know several parameters from your T1/E1/PRI provider. These are:

- Line Framing
- Line Coding
- Signaling Mode and Protocol Settings or if using PRI service, the switch type
- Any other PSTN line configuration parameters supplied by the Telco (e.g. LBO, FDL, etc)

Enabling the Web Browser

To set up the PSTN interface under the web management system, you must enter the 2800 Configuration Menu with a web browser. For information on how to enter the 2800 Configuration Menu, or for a description of 2800 managed objects, please refer to **Appendix A Using the Internal HTTP/HTML Management Pages**.

After logging on to the 2800 Configuration Menu, click "**T1/E1 Link**" to configure T1/E1 Link objects.

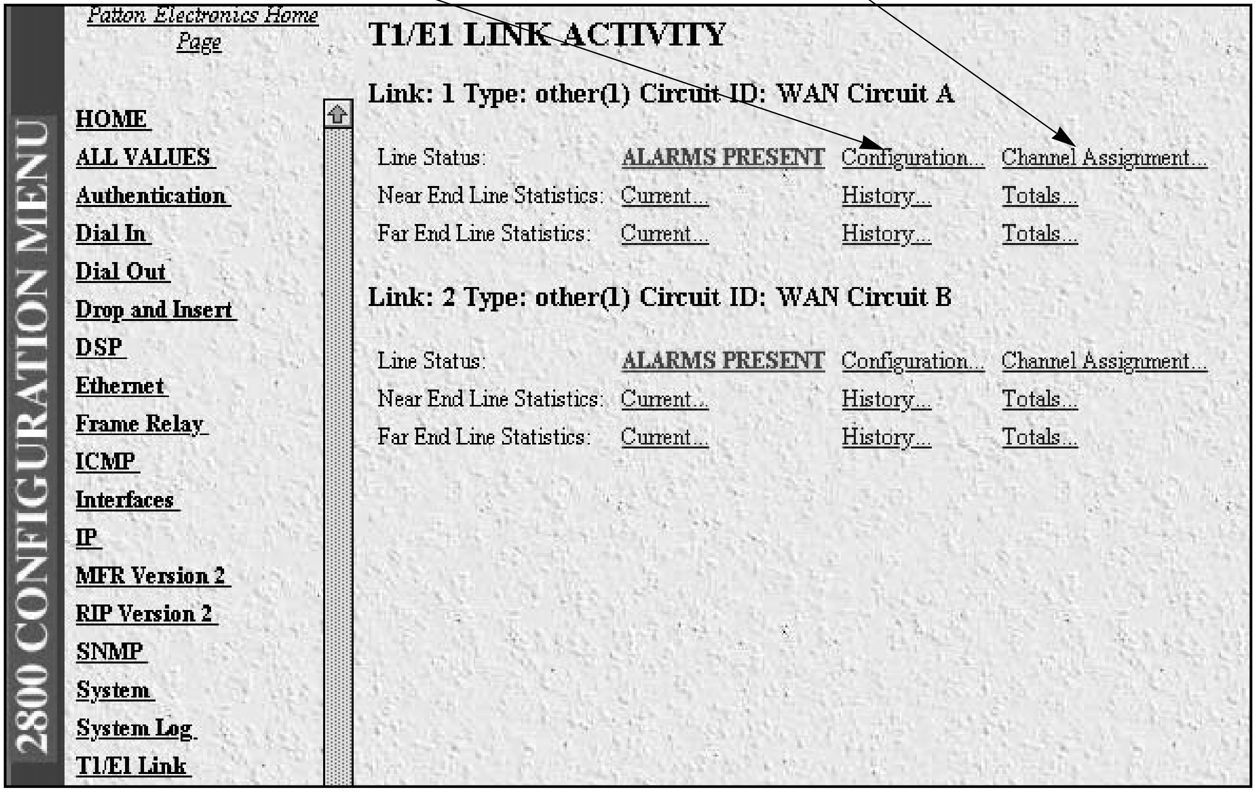
T1/E1 Link Activity

Each T1 line contains 24 channels or timeslots (E1 contains 30 timeslots). Each timeslot supports a single telephone call. Depending on the signaling mode used, all 24 channels on the T1 line may be available for user connections. When using ISDN PRI signaling, 23 channels will be available as one channel is used for out-of-band signaling. E1 lines always have 30 channels for telephone calls regardless of signaling mode.

The T1/E1 Link Activity Screen (shown in Figure 3-2, below) shows setup and statistical information for both **Link A** and **Link B**. Under each link are three sets of hyperlinks for Line Status, Near End Line Statistics, Far End Line Statistics. You must set up objects under each link **(Link A/Link B)** for:

1. **Configuration**
2. **Channel Assignment**

Figure 3-2. T1/E1 Link Main Screen



T1/E1 LINK ACTIVITY

Link: 1 Type: other(1) Circuit ID: WAN Circuit A

Line Status:	ALARMS PRESENT	Configuration...	Channel Assignment...
Near End Line Statistics:	Current...	History...	Totals...
Far End Line Statistics:	Current...	History...	Totals...

Link: 2 Type: other(1) Circuit ID: WAN Circuit B

Line Status:	ALARMS PRESENT	Configuration...	Channel Assignment...
Near End Line Statistics:	Current...	History...	Totals...
Far End Line Statistics:	Current...	History...	Totals...

1. To change Configuration objects, Click **Configuration**, then click **Modify** on the next screen.

2. To change Channel Assignment objects, click **Channel Assignment**

The following sections describe how to set up **Configuration** and **Channel Assignment**

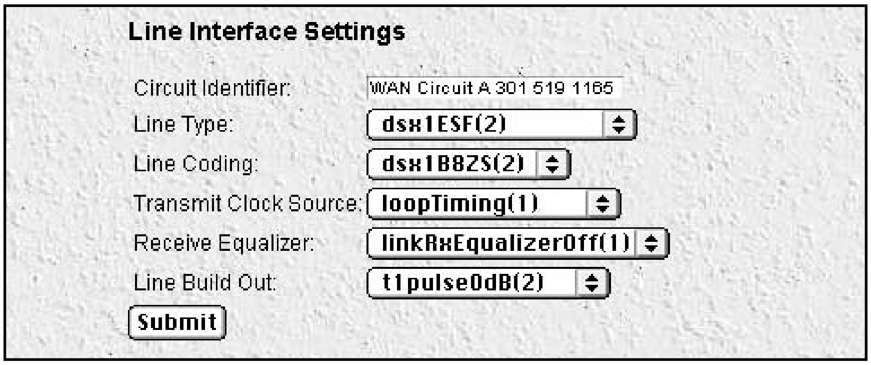
T1/PRI Line Interface Configuration

In order to receive incoming calls on a robbed-bit T1 or ISDN PRI line, you must set up the line interface, Test and Signalling settings.

Line Interface Settings

The line interface parameters dictate how the electrical signals will be presented by the telco and how the 2800 should act on those signals. These will apply whether the line is T1 or PRI.

Figure 3-3. Line Interface Settings



Line Interface Settings

Circuit Identifier: WAN Circuit A 301 519 1165
Line Type: dsx1ESF(2)
Line Coding: dsx1B8ZS(2)
Transmit Clock Source: loopTiming(1)
Receive Equalizer: linkRxEqualizerOff(1)
Line Build Out: t1pulse0dB(2)

Circuit Identifier

The Circuit Identifier is a text string and usually contains the circuit identifier as specified by the telco. Set this object to anything you would like in order to identify this circuit.

Line Type

The line type determines the framing of the T1 circuit. Set this object the same as your provider's setting. The selectable line code parameters are:

dsx1ESF	Extended SuperFrame DS1
dsx1D4	AT&T D4 format DS1

For ISDN PRI service, set the line type to **dsx1ESF**.

Line Coding

This variable describes the encoding of of the digital signals. This must match your providers setting. The most common options are:

dsx1B8ZS	Binary 8 Zero Substitution (B8ZS)
dsx1AMI	Alternate Mark Inversion (AMI)

For ISDN PRI service, set the line coding to **dsx1B8ZS**.

Transmit Clock Source

Set this option should to **loopTiming**. This means the 2800 will use the network as the clock source.

Receive Equalizer

Set this option to **linkRxEqualizerOFF** if you are within 655 feet of the providers network termination jack. If you are farther then 655 feet and experience excessive CRC errors, you may wish to turn on the equalizer.

Line Build Out

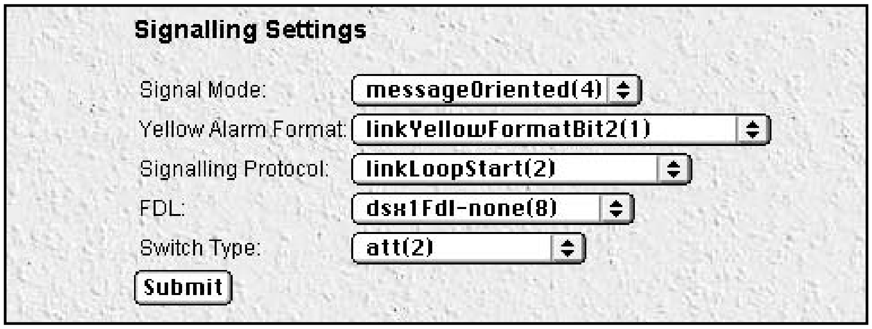
This setting controls the pulse shape of the transmitter into the line with different settings simulating longer cable lengths. In most cases this should be set to **t1pulse0dB**.

When all changes have been completed, select Submit to save the changes.

Signalling Settings

These parameters determine the how 2800 communicates with the providers switch.

Figure 3-4. Signalling Settings



Signalling Settings

Signal Mode: messageOriented(4)

Yellow Alarm Format: linkYellowFormatBit2(1)

Signalling Protocol: linkLoopStart(2)

FDL: dsx1Fdl-none(8)

Switch Type: att(2)

Signal Mode: This option is for selecting the signaling method whether in-band or out-of-band. For a robbed-bit T1, select **robbedBit**. For ISDN PRI, select **messageOriented**.

Yellow Alarm Format: This sets how the 2800 will handle Yellow alarms on the T1 link. For T1's with D4/AMI settings, this should be set to **linkYellowFormatBit**. For T1's with ESF/B8ZS this should be set to **linkYellowFormatDL**.

Signalling Protocol: For Robbed-Bit T1's, set this option to either **linkGroundStart** or **linkLoopStart**. This setting must match how the T1 link has been provisioned. This variable is *not used* in ISDN PRI service and can be left unchanged.

FDL: This variable selects how the Facility Data Link is processed and only applies to T1 circuits with ESF line type. The FDL is used by the service provider to monitor statistics and preform maintenance test.

The current standard ANSI T1.403. Older FDL protocols can be used by selecting **dsx1Att-54016**.

Select **dsx1Ansi-T1-403** unless advised by your service provider to change it.

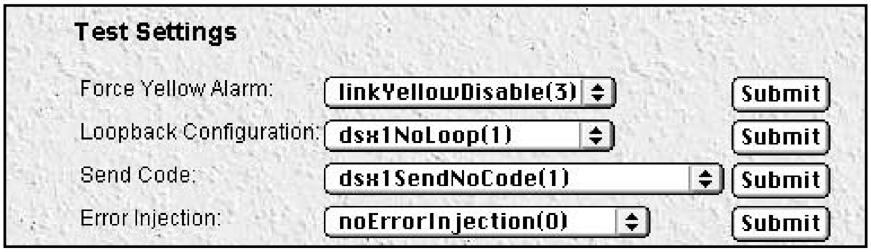
Switch Type This variable applies only if you have selected messageOriented Signal mode and determines the ISDN signaling protocol on the D channel of the PRI line. Set this to the type of switch that you are connected to. This will be either ni1 (National ISDN 1); dms (Nortel Switch); or att (AT&T Custom)

When all changes have been completed, select Submit to save the changes.

Test Settings

The 2800 allows for extensive testing of the T1/E1/PRI line. These options should be set to the factory defaults. In general you will not use these maintenance functions unless called upon by Patton Technical Support. Selecting these options may disable your link or activate alarms at the central office.

Figure 3-5. Test Settings



Test Settings

Force Yellow Alarm: linkYellowDisable(3)
Loopback Configuration: dsx1NoLoop(1)
Send Code: dsx1SendNoCode(1)
Error Injection: noErrorInjection(0)

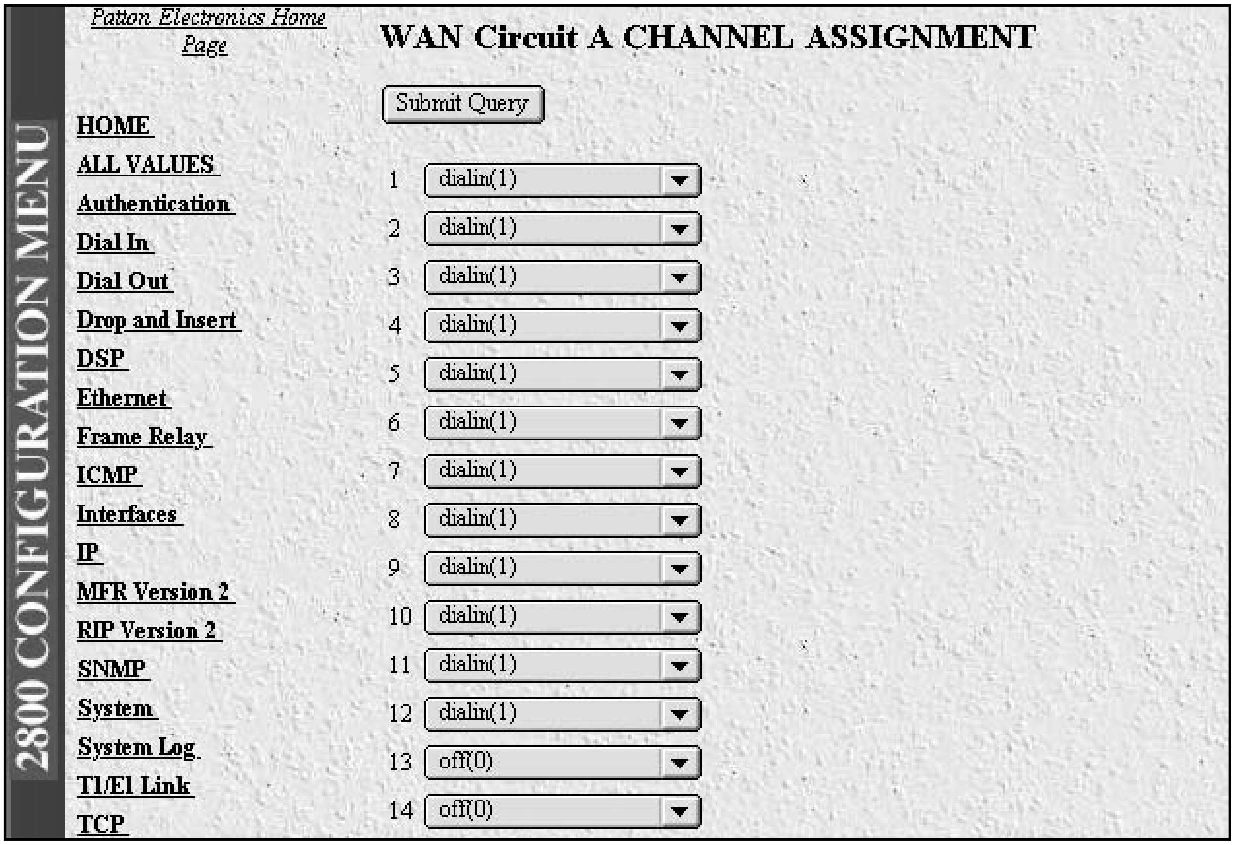
Force Yellow Alarm	**linkYellowDisable**
Loopback Configuration	**dsx1NoLoop**
Send Code	**dsx1SendNoLoop**
Error Injection	**noErrorInjection**

If any of these don't match the factory default, change and Submit the correct options.

Channel Assignment

Now that the link settings are established, you must now activate the channels on the T1/E1/PRI link for operation. From the T1/E1 Link Activity page; click on **Channel Assignment** for Link 1.

Figure 3-6. Channel Assigment



WAN Circuit A CHANNEL ASSIGNMENT

1 dialin(1)
2 dialin(1)
3 dialin(1)
4 dialin(1)
5 dialin(1)
6 dialin(1)
7 dialin(1)
8 dialin(1)
9 dialin(1)
10 dialin(1)
11 dialin(1)
12 dialin(1)
13 off(0)
14 off(0)

This page show each of the available channels. Turn on each channel for dial-in service by selecting **dialin** for each active channel. For T1 ISDN PRI service channel 24 is used as the signaling channel and can be left off.

You 2800 is now setup and ready to receive incoming calls.

4

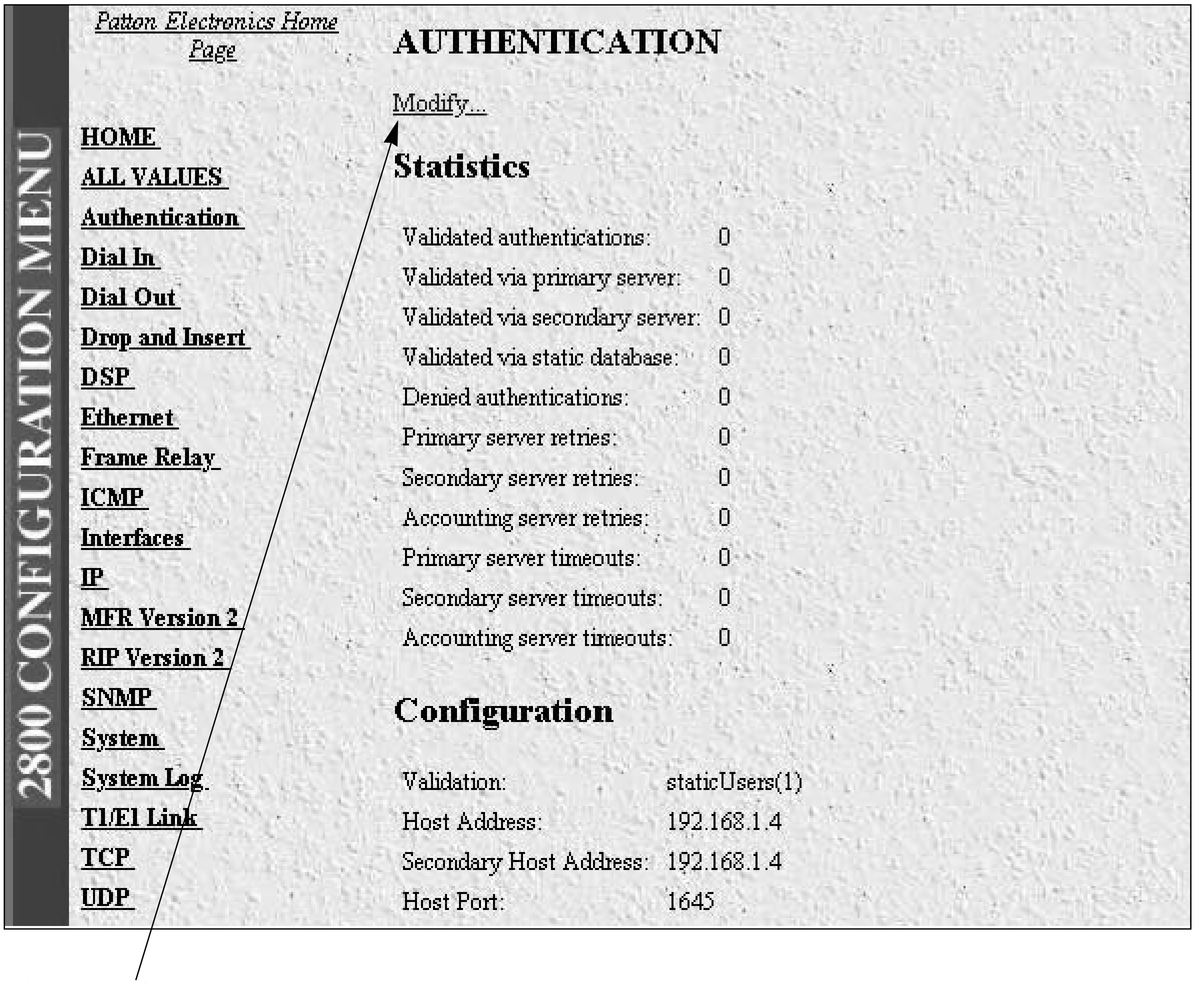
Configuring Authentication

Table of Contents

Introduction to Authentication

The HTTP/HTML Authentication Screens are set up to provide specific users with access to appropriate network services. Currently the 2800 uses Static or RADIUS™ Authentication methods to decide how users may gain access to the network. All objects listed in this section are Patton Enterprise MIB objects that may be accessed via these screens or an alternate SNMP manager.

Figure 4-1 Authentication Main Screen



AUTHENTICATION

Statistics

Validated authentications:	0
Validated via primary server:	0
Validated via secondary server:	0
Validated via static database:	0
Denied authentications:	0
Primary server retries:	0
Secondary server retries:	0
Accounting server retries:	0
Primary server timeouts:	0
Secondary server timeouts:	0
Accounting server timeouts:	0

Configuration

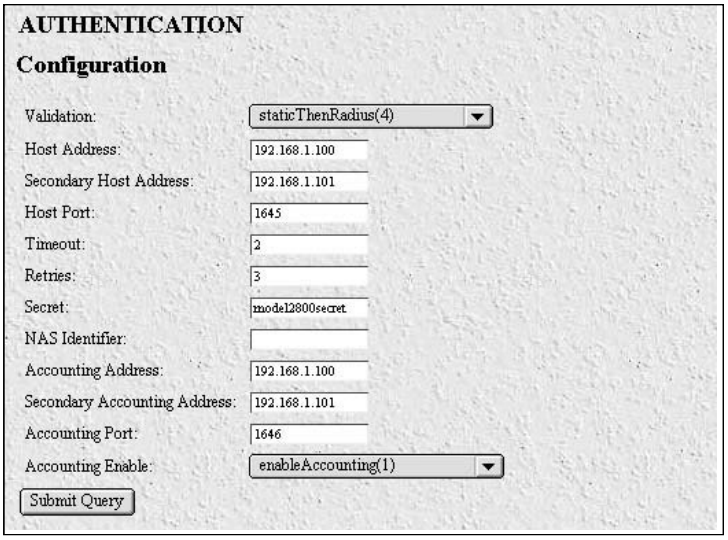
Validation:	staticUsers(1)
Host Address:	192.168.1.4
Secondary Host Address:	192.168.1.4
Host Port:	1645

Select Modify to change 2800 Authentication parameters.

Selecting the Authentication Method

After selecting Modify, you must choose the method the 2800 will use to validate users. Pull down the Validation sub-section and select from one of the available choices (see Figure 4-2, below). Following Figure 4-2 are descriptions for each variable on this page.

Figure 4-2. Authentication - Validation Screen



AUTHENTICATION

Configuration

Validation:	staticThenRadius(4) ▾
Host Address:	192.168.1.100
Secondary Host Address:	192.168.1.101
Host Port:	1645
Timeout:	2
Retries:	3
Secret:	model2800secret
NAS Identifier:	
Accounting Address:	192.168.1.100
Secondary Accounting Address:	192.168.1.101
Accounting Port:	1646
Accounting Enable:	enableAccounting(1) ▾

Validation (auValidation) Selects how the 2800 will authenticate an incoming call. Select from:

No Validation(0) = Select this to allow un-authenticated calls into the 2800, and on to your LAN, using the default service.

static Users(1) = Use the 2800 internal user database only to authenticate. Static users areusers and passwords entered into the 2800's internal users database.

radius Users(2) = Use RADIUS to authenticate and provision user services. RADIUS is a client-server system developed to manage the flexible requirements of remote dial-in users. The RADIUS protocol is specified under RFC 2138 for authentication and RFC 2139 for accounting. RADIUS servers are available as freeware for most computer platforms and is an excellent method for managing user dial-in security. Any RADIUS entries will require an associated server to process authentication requests from the 2800 or the 2800 will reject users access. For more information about RADIUS, see RADIUS User Authentication, below.

tacacs Users(3) = Use TACACS only to authenticate and provision user services *(Currently not implemented)*

static Then Radius(4) = Check the internal user database first, if no match is found, then use RADIUS to authenticate and provision user services.

static Then Tacacs(5) = Check the internal user database first, if no match is found, then use TACACS to authenticate and provision user services *(Currently Not Implemented)*.

NOTE: The following options apply only when using an external authentication server.

Host Address (auHostAddress) tells the 2800 the IP address of the external authentication server. This must be the IP as the 2800 will not resolve a FQDN.

Secondary Host Address (auSecondaryHostAddress) When using a remote authentication server (RADIUS or TACACS) this variable provides an alternative server IP address.

Host Port (auHostPort) This variable tells the 2800 which UDP port to use when connecting to the host specified in the Host Address variable. The RADIUS, as per RFC 2138, specifies a port 1812 for RADIUS authentication. Some older installations of RADIUS use port 1645.

Timeout (auTimeout) This option specifies the time, in seconds, before the 2800 will retransmit an authentication request to an external authentication server.

Retries (auRetries) This option specifies the number of times the 2800 will resend an authentication request to a RADIUS server after a TIMEOUT occurs. If this number is exceeded then the user will be authenticated via the secondary RADIUS server.

Secret (auSecret) The Secret variable sets the shared secret between the authentication client (2800) and the authentication server (RADIUS). It is used to secure communication between the client and server. The secret on the 2800 and the RADIUS server must match and must be 15 or fewer printable, non-space, ASCII characters.

NAS Identifier (auNASIdentifier) This variable is used to identify the 2800 to the remote authentication server. If this option is blank, then the 2800 will use the it's IP address to identify itself to the remote server.

Acct Address (auAcctAddress) is the IP address of the accounting server. RADIUS also allows for the recording of accounting information.

Secondary Acct Address (auSecondaryAcctAddress) When using a remote accounting server (such as RADIUS Accounting) this variable provides the IP address of the accounting server.

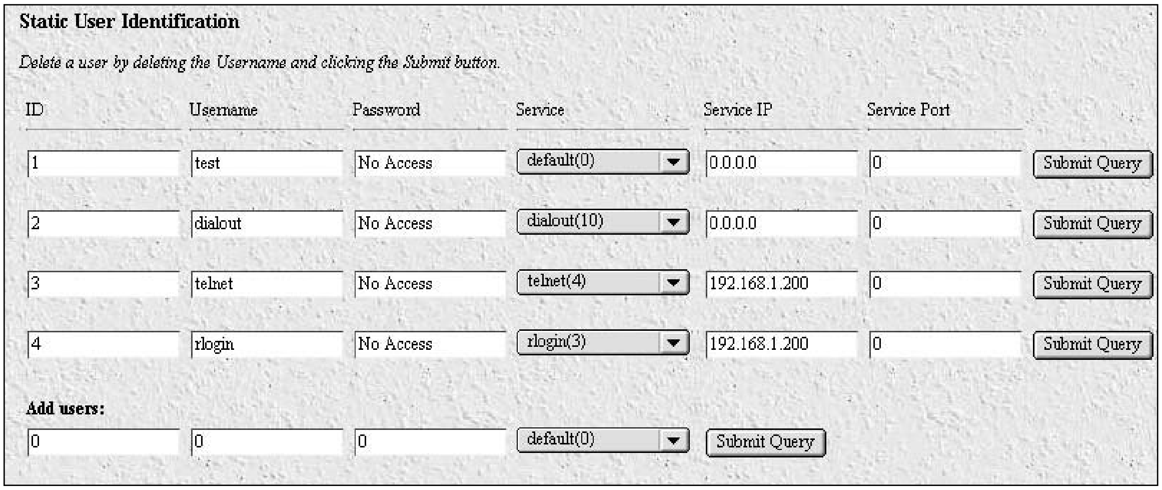
Acct Port (auAcctPort) is the UDP port on the accounting server specified in Acct Address that the 2800 should use to transfer accounting information. RFC 2139 calls out the port of 1813 as the standard RADIUS accounting port. Some older implementations of RADIUS use port 1646 as the accounting port.

Accounting Enable (auAccountingEnable) is a switch which allows the enabling or disabling the reporting of accounting information on the 2800. Select enableAccounting to begin accounting of RADIUS authenticated users. Select disableAccounting to disable the accounting feature.

Static User Authentication

Static users are simply users and passwords entered into the 2800's internal users database. The 2800 database will accept up to 100 users (see Figure 4-3, below). You must have **superuser** access make changes to the static user database. Following Figure 4-3 are descriptions for each variable on this page.

Figure 4-3. Authentication - Static User Identification Setup



Static User Identification

Delete a user by deleting the Username and clicking the Submit button.

ID	Username	Password	Service	Service IP	Service Port	
1	test	No Access	default(0)	0.0.0.0	0	Submit Query
2	dialout	No Access	dialout(10)	0.0.0.0	0	Submit Query
3	telnet	No Access	telnet(4)	192.168.1.200	0	Submit Query
4	rlogin	No Access	rlogin(3)	192.168.1.200	0	Submit Query

Add users:

0	0	0	default(0)	Submit Query

User ID (suID) Identifies the entry in the table of users. For the next user, select the next unused number. If you select a number that is already displayed in the Static User Indentification table, you will overwrite a current entry in user database.

Username (suUsername) This is a unique name, to be provided at login time.

Password (suPassword) This is the password above user

Service (suService) This option instructs the 2800 on how to service the incoming call. Select from:

default	This is the default service as specified under Dial-In (See Dial-In)
admin	*(Currently Not Implemented)*
monitor	*(Currently Not Implemented)*
rlogin	Causes the 2800 to Rlogin into another specified host
telnet	Causes the 2800 to Telnet into another specified host
ppp	2800 will to negotiate a PPP session
cppp	2800 will to negotiate a Compressed-PPP session (see note below)
slip	2800 will negotiate a SLIP connection

cslip 2800 will negotiate a Compressed-SLIP connection
dialout 2800 will give a dialout connection. The dialout connection is an AT command set driven connection into one of the 2800 modems. On line help is provided by typing ‘at help <cr>‘

NOTE: If a user attempts to login in using a different service then he/she has been provisioned with, the 2800 will reject the user. The exception to this is CPPP which will revert to PPP if CPPP is not available on the client.

To Add a User,

1) Select the next ID number
2) Enter in the Username
3) Enter the Password
4) Select the Service type for the user.
5) Select Submit to store the user information.

NOTE: All changes made to the running configuration must be saved to FLASH by selecting RECORD CURRENT CONFIGURATION under Immediate Actions on the HOME page of the 2800. **Failure to do so will cause all configuration information to be lost the next time the 2800 is re-booted.**

Service IP (suServiceIP) This is the IP of the Rlogin or Telnet host.

Service Port (suServicePort) This is the port number to connect to the service host. If the number is 0 then use the default values for Telnet (port number 23) and Rlogin (port number 513).

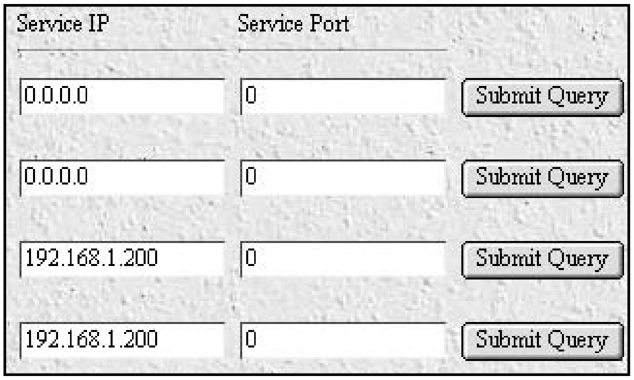
When all additions/changes have been completed, select Submit to save the user in the current running configuration.

NOTE: All change made to the running configuration must be saved to flash by using the Record Current Configuration under Immediate Actions on the HOME page of the 2800. Failure to do so will cause all configuration information to be lost the next time the 2800 is re-booted.

Setting up Authentication for Rlogin and Telnet Users

You must also enter the Service IP and Service Port if the user service is rlogin or telnet (see Figure 4-4, below). Following Figure 4-4 are descriptions for each variable on this page.

Figure 4-4 Authentication - Rlogin and Telnet Users



Service IP	Service Port	
0.0.0.0	0	Submit Query
0.0.0.0	0	Submit Query
192.168.1.200	0	Submit Query
192.168.1.200	0	Submit Query

Service IP (suServiceIP) This is the IP of the rlogin or telnet host.

Service Port (suServicePort) This is the port number to connect to the service host. If the number is 0 then use the default values for telnet (port number 23) and rlogin (port number 513).

When all additions/changes have been completed, select **Submit** to save the user in the current running configuration.

NOTE: All change made to the running configuration must be saved to flash by using the Record Current Configuration under Immediate Actions on the HOME page of the 2800. Failure to do so will cause all configuration information to be lost the next time the 2800 is re-booted.

RADIUS User Authentication

RADIUS is a client-server system that was developed to manage the flexible requirements of remote dial-in users. The RADIUS protocol is specified under RFC 2138 for authentication and RFC 2139 for accounting. RADIUS servers are available as freeware for most computer platforms and is an excellent method for managing user dial-in security. Any RADIUS entries will require an associated server to process authentication requests from the 2800 or the 2800 will reject users access.

How RADIUS Works

RADIUS is client-server authentication system which comprises of two parts:

1. The RADIUS client (your 2800)
2. RADIUS server.

The server is installed on or more central computers which multiple clients can access. The RADIUS server can be used for authentication, provisioning and accounting of dialed in users.

The RADIUS protocols have been accepted by the IETF as RFC 2138 and RFC 2139. RADIUS, being a transaction based protocol, uses UDP packets as its transmission medium. The UDP ports, as specified in the RFC, are: For RADIUS authentication are 1812, and for RADIUS accounting 1813.

RADIUS authenticates users through a series of communications between the 2800 and the RADIUS server. Once a user is authenticated, the 2800 provides the user with access to appropriate network services as specified by RADIUS.

Here are the typical sequence of events the 2800 uses to authenticate a user with RADIUS:

1. A user dials in to the 2800.

2. The 2800 obtains the username and password. This can be through the 2800 providing its prompt asking for the username and password, or it can be via PPP which will use either PAP or CHAP to obtain the username and password.

3. Once the 2800 has the username and password, the 2800 sends an access-request to the RADIUS server. The access-request contains such attributes as the user's name, the user's password, the ID of the client and the Port ID which the users has called. When a password is present, it is encrypted using the MD5 hashing algorithm.

4. The access-request is submitted to the RADIUS server via the network. If no response is returned within a length of time, the request is re-sent a number of times. The timeout and number of times the 2800 will retry is determined by the TIMEOUT and RETRIES options in the 2800 configuration. Once the RADIUS server receives the request, it will first validate the 2800 initiating the request. A request from a 2800 for which the RADIUS and the 2800's shared secret do not match will be discarded and the user rejected.

5. The RADIUS server will then validate the user in the RADIUS users database. If the username, password, and the specified requirements are correct, the server will send an access-accept response. The access-accept response can contain a list of configuration values for the user. This can be such options as what host the user should be connected to (Telnet) or what port and service the users is allowed to user. If any condition is not met, the RADIUS server sends and access-reject response indication that the user request is invalid.

Integrating RADIUS

To use the 2800 with RADIUS you will need the following:

1. A PC or UNIX system, with IP connectivity, to run the RADIUS daemon
2. The RADIUS binaries.

NOTE: This system running RADIUS does not have to be connected to the same LAN. The only requirement is that IP packets from the 2800 can be routed to and from the RADIUS server. This allows a centrally located RADIUS server to authenticate multiple 2800's in remote POPs, using the Internet to pass the IP packets.

Starting the RADIUS Daemon

Install the RADIUS binaries as per the instructions. To start the RADIUS daemon, from the command line enter in RADIUSD. The RADIUS daemon has many options which you can specify at execution time. If you wish to start RADIUS with some options then enter RADIUSD [options]. The most common options are:

radiusd -

-A <Options> This argument will instruct the RADIUS daemon to being RADIUS accounting

Options:

none The daemon does not create the accounting process services. An accounting process is executed if there is an entry in the /etc/services file defining which UDP port should be used for RADIUS accounting. If this is not found, then an accounting process is not executed

incr Creates the accounting process with the UDP port specified as the accounting port in the /etc/services file. If the port is not defined, then the daemon will increment by one the UDP port specified for authentication.

-a <path> Specifies and alternate directory path for RADIUS accounting information. The default path is /usr/adm/radacct.

-d <path> Specifies an alternate directory path for the RADIUS configuration

files. The default directory is /etc/raddb.

-v Causes the RADIUS daemon to report its software version without executing a RADIUS daemon.

-x This will run RADIUS in debug mode.

Configuring The Clients file

The clients file (typically found in /etc/raddb) defines the client machines which are allowed to make requests to the RADIUS server. It is a flat file and consists of a line with the client name (or address) and a shared secret. In order to authenticate a user, the clients file must have an entry for your 2800 and the shared secret. Here is the format:

client shared secret

To place the your 2800 in the clients file you would put the IP address of your 2800 and the same value as the SECRET as entered in the Authentication page on the 2800. If the system running the RADIUS daemon can resolve the IP address of your 2800 to a name, then you can put the name of your 2800 instead.

There is no limit to the number of clients a RADIUS daemon can handle. This allows a single server to authenticate many 2800's.

APPLICATION TIPS

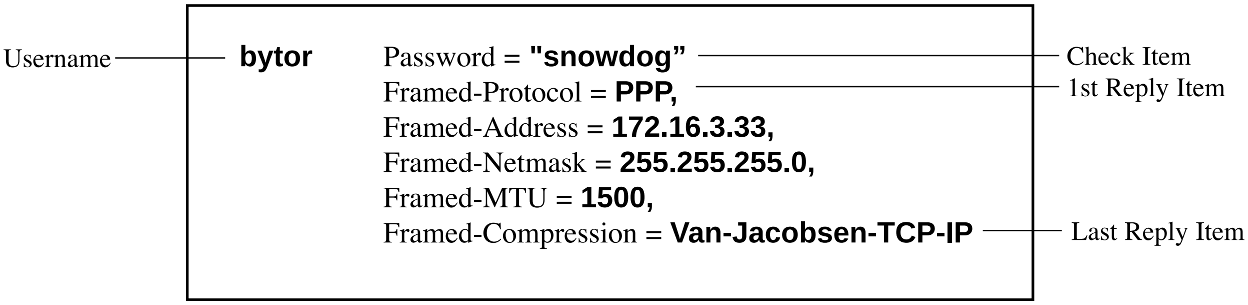
- *As an example of a staticThenRadius option of authentication, a network administrator can program several admin. static user ids with the bulk of the dial-up users authentication going to RADIUS. This allows the network admin access to the 2800 and the network in the event the RADIUS server is down.*
- *As an example to allow RADIUS to authenticate a PPP or SLIP user, but to let the Model 2800 give out an IP address to the dial-in user. Under <Dial-IN> -> <Settings> set the default IP address pool using you local IP addresses. In the RADIUS users file, add the following:*

```
username          Password="userspassword"
User-Service-Type = Framed-User
```

Configuring The Users file

The RADIUS users file (typically found in /etc/raddb) is a flat text file on the RADIUS server. The users file stores authentication and authorization information for all users authenticated with RADIUS and is called the user profile. For each user, you must create an entry that consists of three parts: the username, a list of check items, and a list of reply items.

Here is an example of a RADIUS user entry:



```
bytor     Password = "snowdog”
          Framed-Protocol = PPP,
          Framed-Address = 172.16.3.33,
          Framed-Netmask = 255.255.255.0,
          Framed-MTU = 1500,
          Framed-Compression = Van-Jacobsen-TCP-IP
```

Username The username (bytor) is the first word of each user profile. Usernames consist of up to 40 printable, non-space, ASCII characters.

Check Items Check items are listed on the first line of a user entry, separated by commas. For an access-request to succeed, all the check items in the user entry must be matched in the access-request. In the above example, bytor’s password is the only check item. Other check items might limit a user to a specific 2800 or to a specific interface on a 2800. In this case, to successfully authenticate a dialed-in user, the RADIUS server must receive the password in bytor’s access-request

Reply Items Reply items instruct the 2800 how to handle a user’s connection. In the above example, the user bytor will be a PPP connection. Bytor will use the IP address of 172.16.3.33 with a 255.255.255.0 netmask, a MTU of 1500 and use VJ header compression.

RADIUS Accounting

RADIUS accounting logs information about dial-in connections. This information is often used for billing purposes and can be processed by third party billing programs. RADIUS accounting consists of a client/server format. As transactions occur, they are recorded on the host as specified in in the Accounting Address parameter in the Authentication Page on the 2800. You must enable Mode 2800 accounting by selecting **Accounting Enable (auAccountingEnable)** on the Authentication page.

How RADIUS Accounting Works

RADIUS accounting consists of an accounting server and accounting clients (2800). The radiusd daemon for accounting is a child process of the radiusd authentication daemon; it starts automatically when radiusd is executed. The RADIUS accounting server uses the UDP protocol, and typically listens for UDP packets at port 1813. The port specified in the 2800 Accounting Port determines which port the 2800 will try to send to the accounting host and should match the number on the host. This number can be found in the /etc/services file.

RADIUS accounting consists of the following steps:

1. The 2800 sends an accounting-request packet containing the record of an event to the accounting server.

2. The accounting server sends an accounting-response packet back to the 2800 to acknowledge receipt of the request.

3. If the 2800 does not receive a response, it continues to send accounting-requests until it receives a response. A backoff algorithm is used to determine the delay between accounting-requests if an accounting-response is not received.

4. The 2800 records the number of seconds that have passed between the event and the current attempt to send the record; this number is the Acct-Delay-Time value. As additional time passes before an accounting-response is received, the Acct-Delay-Time is updated.

5. A Start Accounting record is recorded in the accounting file on the accounting host when the user is connected. The Start Accounting record typically contains the Session-Id, the User-Name, Service-Type, Login-Service, Login-IP-Host, Acct-Delay-Time, and other relevant information from a user's entry in the users file.

NOTE: A Stop Record is created when the user is disconnected. This record contains the same information as the Start record; However, it also includes Acct-Session-Time, and Acct-Input-Packets.

Here is an example of a 2800 RADIUS accounting start and stop information:

```
Start
Tue Jul  7 12:53:33 1998
        Acct-Status-Type = Start
        Acct-Session-Id = 00000151
        Acct-Multi-Session-Id = 00000151
        Acct-Authentic = RADIUS
        NAS-IP-Address = 210.48.111.101
        User-Name = juniorasparagus
        NAS-Port = 3
        Called-Station-Id = 3015551212
        Calling-Station-Id = 3019751000
        Service-Type = Framed
        Framed-Protocol = PPP

Stop
Tue Jul  7 12:57:37 1998
        Acct-Status-Type = Stop
        Acct-Session-Id = 00000151
        Acct-Multi-Session-Id = 00000151
        Acct-Authentic = RADIUS
        Acct-Session-Time = 257
        Acct-Input-Packets = 662
        Acct-Output-Packets = 532
        Acct-Input-Octets = 49694
        Acct-Output-Octets = 247463
        NAS-IP-Address = 210.48.111.101
        User-Name = juniorasparagus
        NAS-Port = 3
        Called-Station-Id = 3015551212
        Calling-Station-Id = 3019751000
        Service-Type = Framed
        Framed-Protocol = PPP
        Framed-IP-Address = 210.48.111.112
        User-Service = Framed-User
        Framed-Protocol = PPP
```

There are also scripts available which will generate usage statistics for each user.

Listing of RADIUS Authentication Attributes

There are four types of packets:

1. Access-Request — Access-Request packets are sent to a RADIUS server, and convey information used to determine whether a user is allowed access to a specific NAS, and any special services requested for the user.

2. Access-Accept — Access-Accept packets are sent by the RADIUS server, and provide specific configuration information necessary to begin delivery of service to the user.

3. Access-Reject — An access-Reject packet is sent from the RADIUS server in any value of the received attributes in no acceptable.

4. Access-Challenge — The RADIUS server my send the user a challenge requiring a response.

Within these packets there are attributes which carry specific authentication, authorization, information and configuration details for the request and rely. When the 2800 receives a call, It will send the RADIUS server as much of the attribute information that it can guess. If the RADIUS server sends back options that change these options, then the 2800 will act on those changes. If a service (e.g. Framed User) is specified then the 2800 will default to a the link default.

The listing below describes the configuration options as used in the /etc/raddb/users file that will work on the 2800. The RFC'd name (as would be used in the users file) is in bold. The RFC Type number is in parentheses.

User-Name (1) *string*

Description — The name of the user that the RADIUS server will authenticate
Message Type — Access-Request

Password (2) *string*

Description — The password of the user that the RADIUS server will authenticate
Message Type — Access-Request
NOTES — The transmission of the password from the 2800 to the RADIUS server

CHAP-Password (3) *string*

Description — The response value provided by a PPP CHAP users in response to the challenge.
Message Type — Access-Request

NAS-IP-Address (4) *ipaddress*

Indicates the identifying IP address of the NAS which is requesting authentication of the user

Packet Type Access-Request

NAS-Port (5) *integer*

Description Indicates the physical port number of the NAS which is authentication the user.

Message Type Access-Request

Notes: The 2800 port numbers range for a T1 system 0-23. For an E1 system it is 0-29, with ports 0 and 16 not used for user dial in service. These port number correspond to the timeslots on the incoming T1 or E1 line.

Service-Type (6) *integer*

Description The type of service the NAS is to provide to the users

Message Type Access-Request

Options Login-User (1) The user should be connected to a host

Framed-User (2) A framed protocol should be started to the user (either SLIP or PPP see Framed-Protocol for specifying a particular Protocol)

Framed-Protocol (7) *integer*

Description Indicates the the framed protocol to used for framed access.

Message Type Access-Request and Access-Accept

Options PPP (1) To specify PPP framing

SLIP (2) To specify SLIP framing

Framed-IP-Address (8) *ipaddress*

Description Indicates the framed IP address to be configured for the user.

Message Type Access-Request and Access-Accept

NOTES If the IP address is 255.255.255.255 then the 2800 will allow the user to specify the address. If the address is 255.255.255.254 then the PAR-1 will assign an IP from the IP pool of address in the 2800.

Framed-IP-Netmask (9) *ipaddress*

Description Indicates the framed IP address netmask to be configured for the users.

Message Type Access-Request and Access-Accept

Framed-MTU (12) *integer*

Description This attribute indicates the Maximum Transmission Unit to be config ured for the user, when it is not negotiated by some other means (such as PPP).

Message Type Access-Request and Access-Accept

Framed-Compression (13) *integer*

Description This attribute indicates a compression protocol to be used for the link.
Message Type Access-Accept
Options None (0) No compression
VJ TCP/IP (1) Header compression

Login-IP-Host (14) *ipaddress*

Description This attribute directs the 2800 which system to connect users to.
Message Type Access-Request and Access-Accept

Login-Service (15) *integer*

Description This attribute indicates the service which should be used to connect the user to the login host.
Message Type Access-Accept
Options Telnet (0) Specify Telnet as the login service
Rlogin (1) Specify Rlogin as the login service

Login-TCP-Port (16) integer

Description This attribute specifies which port the users is to be connected to in connection with the Login-Service attribute. Values range from 0 to 65535
Message Type Access-Accept

Reply-Message (18) *string*

Description This attribute indicates text which will be displayed to the user. When used with Access-Accept it will display a success message, When used with Access-Reject, it is the failure message, and when used with Access-Challenge, it will prompt the user for a response.
Message Type Access-Accept, Access-Reject and Access-Challenge.

State (24) *string*

Description This attribute is available to be sent by the server to the client in an Access-Challenge request
Message Type Access-request and Access-Challenge

Class (25) *string*

Description This attribute is available to be sent by the server in an Access-Accept message and is sent unmodified by the client to the accounting server as part of the Accounting-Request message.
Message Type Access-Accept

Session-Timeout (27) *integer*

Description	This attribute sets the maximum number of seconds of service to be provided to the user before termination of the session.

Message Type	Access-Accept and Access-Challenge

Idle-Timeout (28) *integer*

Description	This attribute sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session.

Message Type	Access-Accept and Access-Challenge

Termination-Action (29) *string*

Description	This attribute indicates what action the 2800 should take when the specified service is complete.

Message Type	Access-Accept

Options	Default (0)
RADIUS-Request (1)

Port-Limit (62) *string*

Description	This attribute sets the maximum number of ports to be provided to the user by the 2800.

Message Type	Access-Accept and Access-Request

A

Using the Internal HTTP/HTML Management Pages

Table of Contents

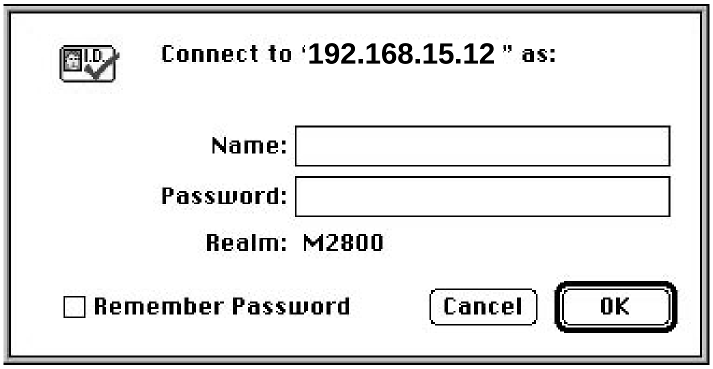
Introduction to the Internal HTTP/HTML Management Pages

You may configure the 2800 by using its internal HTTP/HTML Mananagement Pages. However, to enter into the HTTP/HTML pages, you must first define the LAN Address Technique, LAN IP Address, and LAN Subnet Mask for the 2800. If you have not done so, please return to Chapter 2. Getting Started, to do so.

Logging Into the HTTP/HTML Pages

To log into the HTTP/HTML Management pages, you must enter the 4-octet IP (i.e. 192.168.15.12) address as the URL (Universal Resource Locator) into a World Wide Web Browser. This address is the same address that you entered in **Chapter 2. Getting Started.** After you enter the IP address, the 2800 will ask for your user name and password. Example A-1 shows an example of the Login Screen.

Figure A-1. 2800 Login Screen



Connect to '192.168.15.12 " as:

Name:

Password:

Realm: M2800

There are two levels of administration passwords associated with the operation of your 2800. They are: **1. superuser**: allows full permission to change and view any parameters in the 2800; and 2. **monitor**. allows full viewing of any non-password oriented variables. We suggest that you change these passwords immediately after initial configuration.

HTTP/HTML and SNMP Object Format

In Appendix 3, we shall describe variables on each of the internal HTTP/HTML pages. This description will include brief descriptions of the Patton Enterprise MIB or SNMP MIB II object identifiers wherever pertinent. The format of the varibles will look like this:

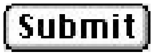
HTTP Variable

Patton Enterprise MIB or
SNMP MIB Object

Total Active Calls (diActive)

Saving HTTP/HTML Object Changes

Sometimes you will need to save changes that you have made in the HTTP/HTML pages. To make changes to read/write variables:

1. Select the appropriate Modify screen
2. Make the change to the parameter
3. Select 

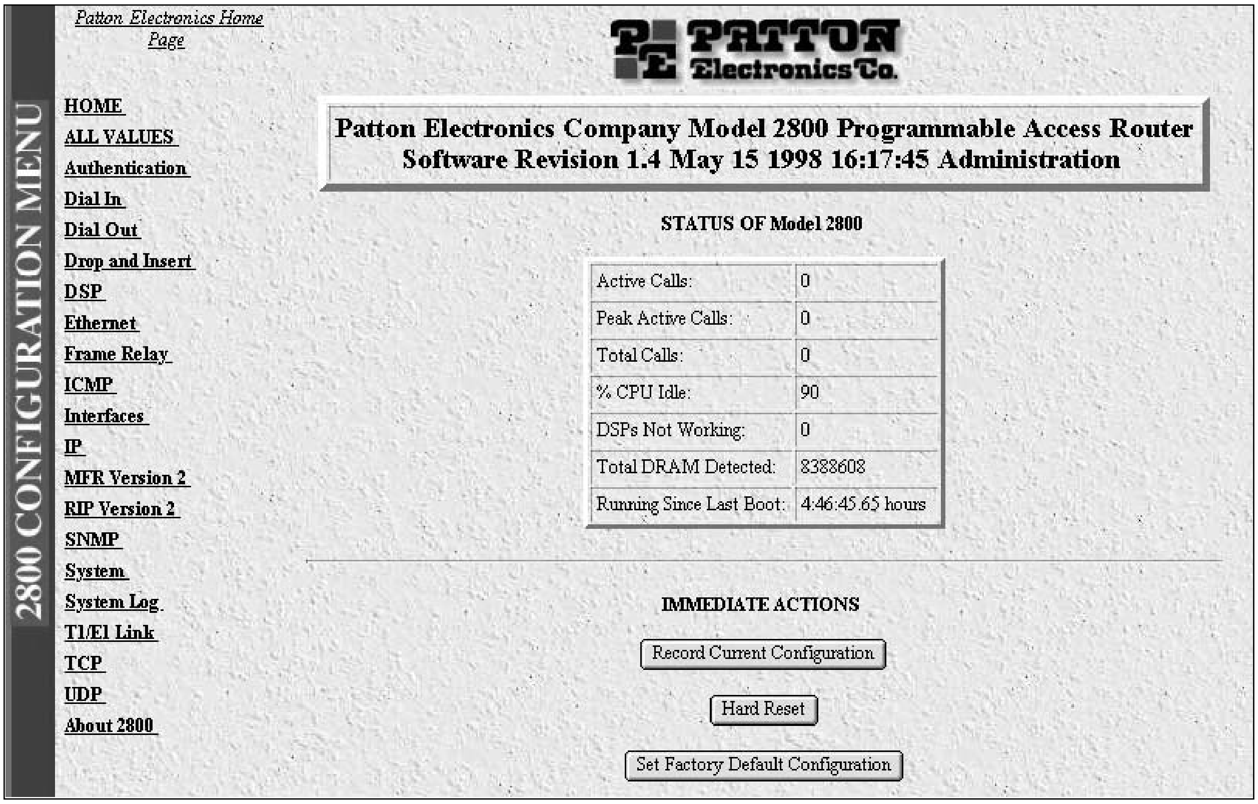
4. Return to the HOME screen
5. Select

NOTE: Failure to save changes in the manner shown above will result in lost changes when the 2800 RAS is power-cycled.

HOME

HOME is the first HTTP/HTML page that you will reach after you log into the 2800. From the HOME page you may monitor the current system status, save any system changes or reset the system without powering off the box. This section describes the HOME page.

Figure A-2. HOME Page



Patton Electronics Company Model 2800 Programmable Access Router
Software Revision 1.4 May 15 1998 16:17:45 Administration

STATUS OF Model 2800

Active Calls:	0
Peak Active Calls:	0
Total Calls:	0
% CPU Idle:	90
DSPs Not Working:	0
Total DRAM Detected:	8388608
Running Since Last Boot:	4:46:45.65 hours

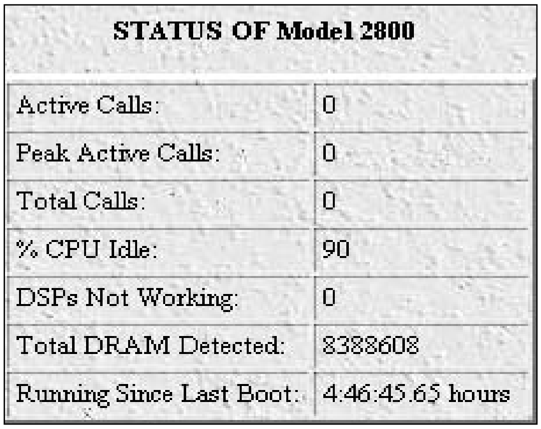
IMMEDIATE ACTIONS

Record Current Configuration
Hard Reset
Set Factory Default Configuration

Operating Status Variables

There are seven system variables which describe the immediate operating status 2800. These variables are shown in A-3, below, and are described in the section below.

Figure A-3. STATUS Menu



STATUS OF Model 2800	
Active Calls:	0
Peak Active Calls:	0
Total Calls:	0
% CPU Idle:	90
DSPs Not Working:	0
Total DRAM Detected:	8388608
Running Since Last Boot:	4:46:45.65 hours

Active Calls (diActive) This number, ranging from 0 to 60 displays the total number of calls being processed (connecting, dead, authenticating,etc...) in a 2800 at the time the HOME page was brought up.

Peak Active Calls (diMaxActive) The maximum number of active calls seen at one time.

Percentage CPU Idle (boxIdleTime) This is an indication of the amount of system CPU power which is not being utilized by the 2800. The return value is a percentage of free CPU cycles since the last time the variable was read.

DSPs Not Working (dspFailed) This number should always be zero. The DSP's in the 2800 are arranged as a resource pool and called upon at ring-time. Therefore, if a DSP does not work, chances are you'll never know, as the 2800 will automatically remove the defiant DSP from the resource pool. One symptom of a DSP failures is the 2800 isn't handling as many calls as it should. A DSP may be taken out of service if it fails to respond to the 2800 CPU. If a DSP isn’t available when a call comes in, the call will simply ring and not be answered.

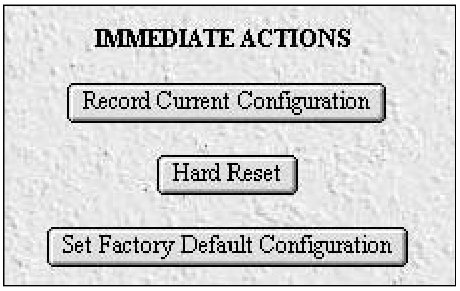
Total DRAM Detected (boxDetectedMemory) This number shows the total number of bits of installed and available DRAM.

Running Since Last Boot (sysUpTime) This tells you how long the 2800 has been running since the it was last reset. It displays the number of hours and rolls over after 1,193 hours (497 days).

Immediate Actions

There are several immediate actions which will be executed on the 2800, when in superuser mode, which will cause the box to act according to the descriptions below.

Figure A-4. 2800 Immediate Actions


IMMEDIATE ACTIONS
Record Current Configuration
Hard Reset
Set Factory Default Configuration

Record Current Configuration RECORD CURRENT CONFIGURATION causes the current configuration to be stored in FLASH memory. Any changes made to the 2800 configuration are stored in non-volatile RAM first. This allows the user to set the box up with a working configuration before commiting it to FLASH. Configuration changes become permanent when you select RECORD CURRENT CONFIGURATION. You will lose all changes not stored to FLASH the next time the 2800 is re-booted.

Hard Reset HARD RESET causes the 2800 to restart. When you select HARD RESET, the 2800 confirm that you want to execute this command. Then, the 2800 will disconnect all current sessions, re-initialize the interfaces, and re-load configuration parameters from FLASH.

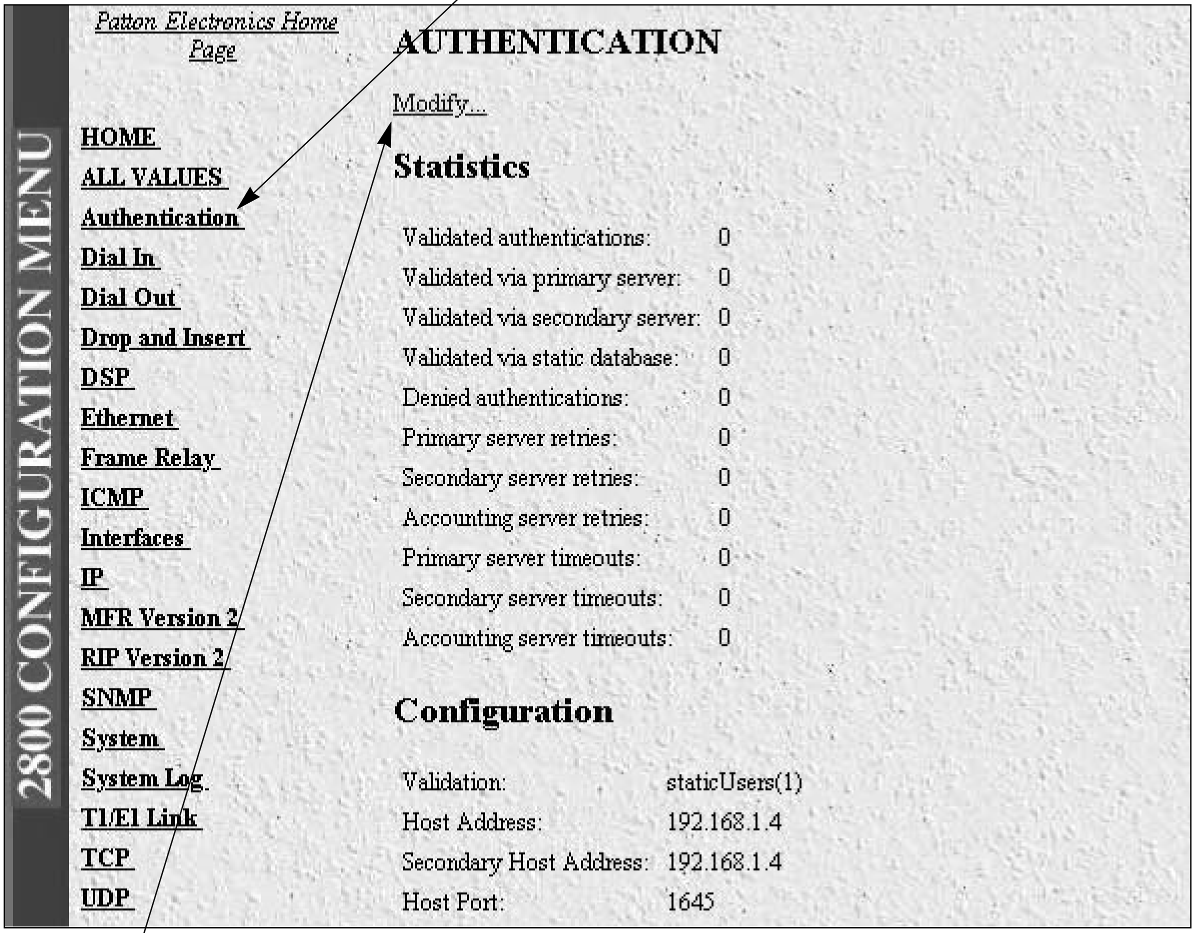
Set Factory Default Default Configuration SET FACTORY DEFAULT CONFIGURATION clears out the configuration in FLASH and loads the factory default parameters into FLASH memory. SET FACTORY DEFAULT CONFIGURATION *will not* execute on the 2800 until it is re-booted.

> **NOTE:** SET FACTORY DEFAULT CONFIGURATION will delete any routing information, the 2800's ethernet IP address, and any other site specific settings made for your particular installation. You will have to re-enter the 2800's ethernet IP address and netmask using the front panel control port in order to use the HTTP/HTML Management pages.

Authentication

Use the Authentication Pages to set up System security and to provide specific users with access to appropriate network services. This section describes the Authentication parameters. The 2800 uses Static or RADIUS Authentication to decide which users may gain access to the system. You may reach the main Authentication Page by selecting Authentication from the 2800 Configuration Menu as shown below. This section describes Static User and RADIUS parameters.

Figure A-5. Authentication Main Screen



AUTHENTICATION

Statistics

Validated authentications:	0
Validated via primary server:	0
Validated via secondary server:	0
Validated via static database:	0
Denied authentications:	0
Primary server retries:	0
Secondary server retries:	0
Accounting server retries:	0
Primary server timeouts:	0
Secondary server timeouts:	0
Accounting server timeouts:	0

Configuration

Validation:	staticUsers(1)
Host Address:	192.168.1.4
Secondary Host Address:	192.168.1.4
Host Port:	1645

Select Modify to set up or change 2800 Authentication parameters.

Statistics

Statistics listed on the main Authentication screen show running totals of statistics for RADIUS and Static User logins. Shown are statistics gathered since the last box reset.

Validated authentications (auAuthenticationsValidTotal) The total number of validated authentications since the last box reset.

Validated via primary server (auAuthenticationsValidPrimary) The number of authentications validated by the primary RADIUS authentication server since the last box reset**.**

Validated via secondary server (auAuthenticationsValidSecondary) The number of authentications validated by the secondary RADIUS authentication server since the last box reset.

Validated via static database (auAuthenticationsValidStatic) The number of authentications validated by the Static User database since the last box reset.

Denied authentications (auAuthenticationsDenied) The total number of authentication attempts requested but denied since the last box reset.

Primary server retrys (auPrimaryServerRetrys) The number of authentication attempts made by the 2800 to the primary RADIUS authentication server.

Secondary server retrys (auSecondaryServerRetrys) The number of authentication attempts made by the 2800 to the secondary RADIUS authentication server.

Accounting server retrys (auAccountingServerRetrys) The number of accounting attempts made by the 2800 to the RADIUS accounting server.

Primary server timeouts (auPrimaryServerTimeouts) The total number of authentication timeouts by the primary RADIUS authentication server.

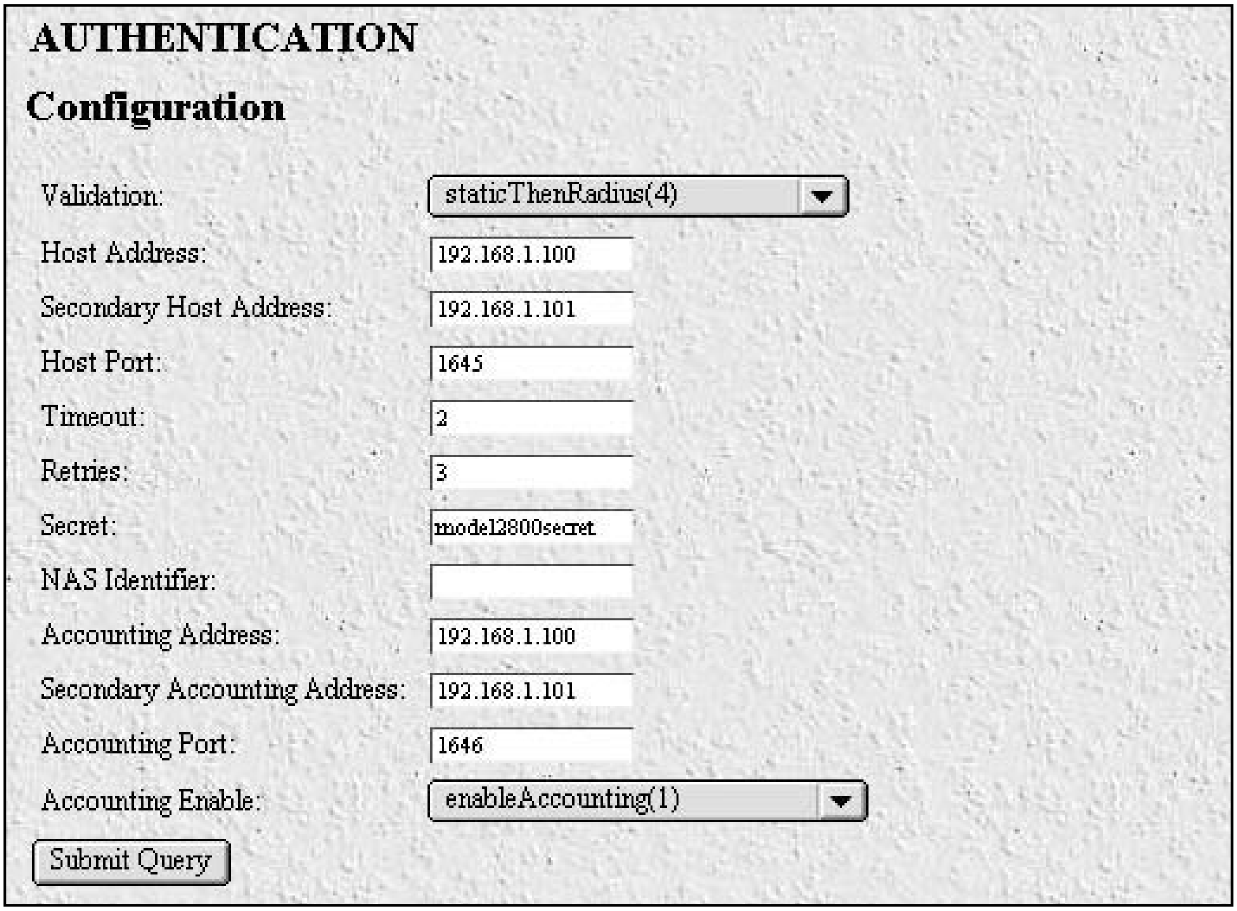
Secondary server timeouts (auSecondaryServerTimeouts) The total number of authentication timeouts by the secondary RADIUS authentication server.

Accounting server timeouts (auAccountingServerTimeouts) The total number of accounting timeouts by the primary RADIUS accounting server.

Configuration

After selecting Modify from the main Authentication screen, you may set up or change authentication parameters for both RADIUS users and Static users. After configuring the Validation method (See **Validation (auValidation)**, below), configure the additional parameters as shown in Figure A-6 below to configure RADIUS parameters. See below to set up Static users.

Figure A-6. Configuration Screen



AUTHENTICATION

Configuration

Validation:	staticThenRadius(4)
Host Address:	192.168.1.100
Secondary Host Address:	192.168.1.101
Host Port:	1645
Timeout:	2
Retries:	3
Secret:	model2800secret
NAS Identifier:	
Accounting Address:	192.168.1.100
Secondary Accounting Address:	192.168.1.101
Accounting Port:	1646
Accounting Enable:	enableAccounting(1)

Validation (auValidation) Selects how the 2800 will authenticate an incoming call. Select from:

No Validation(0) = Select this to allow un-authenticated calls into the 2800, and on to your LAN, using the default service.

static Users(1) = Use the 2800 internal user database only to authenticate. Static users are simply users and passwords entered into the 2800's internal users database.

radius Users(2) = Use RADIUS to authenticate and provision user services. RADIUS is a client-server system developed to manage the flexible requirements of remote dial-in users. The RADIUS protocol is specified under RFC 2138 for authentication and RFC 2139 for accounting. RADIUS servers are available as freeware for most computer platforms and is an excellent method for managing user dial-in security. Any RADIUS entries will require an associated server to process authentication requests from the 2800 or the 2800 will reject users access. For more information about RADIUS, see RADIUS User Authentication, below.

tacacs Users(3) = Use TACACS only to authenticate and provision user services
static Then Radius(4) = Check the internal user database first, if no match is found, then use RADIUS to authenticate and provision user services.
static Then Tacacs(5) = Check the internal user database first, if no match is found, then use TACACS to authenticate and provision user services.

NOTE: The following options apply only when using an external authentication server.

Host Address (auHostAddress) tells the 2800 the IP address of the external authentication server. This must be the IP as the 2800 will not resolve a Fully Qualified Domain Name. Currently, you may specify only *one* authentication server.

Secondary Host Address (auSecondaryHostAddress) When using a remote authentication server (RADIUS or TACACS) this variable provides an alternative server IP address.

Host Port (auHostPort) This variable tells the 2800 which UDP port to use when connecting to the host specified in the Host Address variable. The RADIUS, as per RFC 2138, specifies a port 1812 for RADIUS authentication. Some older installations of RADIUS use port 1645)

Timeout (auTimeout) This option specifies the time, in seconds, before the 2800 will retransmit an authentication request to an external authentication server.

Retries (auRetries) This option specifies the number of times the 2800 will resend an authentication request to a RADIUS server after a TIMEOUT occurs. If this number is exceeded then the user will be rejected.

Secret (auSecret) The Secret variable sets the shared secret between the authentication client (2800) and the authentication server (RADIUS). It is used to encrypt an authentication request and to decrypt an incoming reply from the server. The secret on the 2800 and the RADIUS server must match and must be 15 or fewer printable, non space, ASCII characters.

NAS Identifier (auNASIdentifier) This variable is used to identify the 2800 to the remote authentication server. If this option is blank, then the 2800 will use the it's IP address to identify itself to the remote server.

Acct Address (auAcctAddress) is the IP address of the accounting server. RADIUS also allows for the recording of accounting information.

Secondary Acct Address (auSecondaryAcctAddress) When using a remote accounting server (such as RADIUS Accounting) this variable provides the IP address of the accounting server.

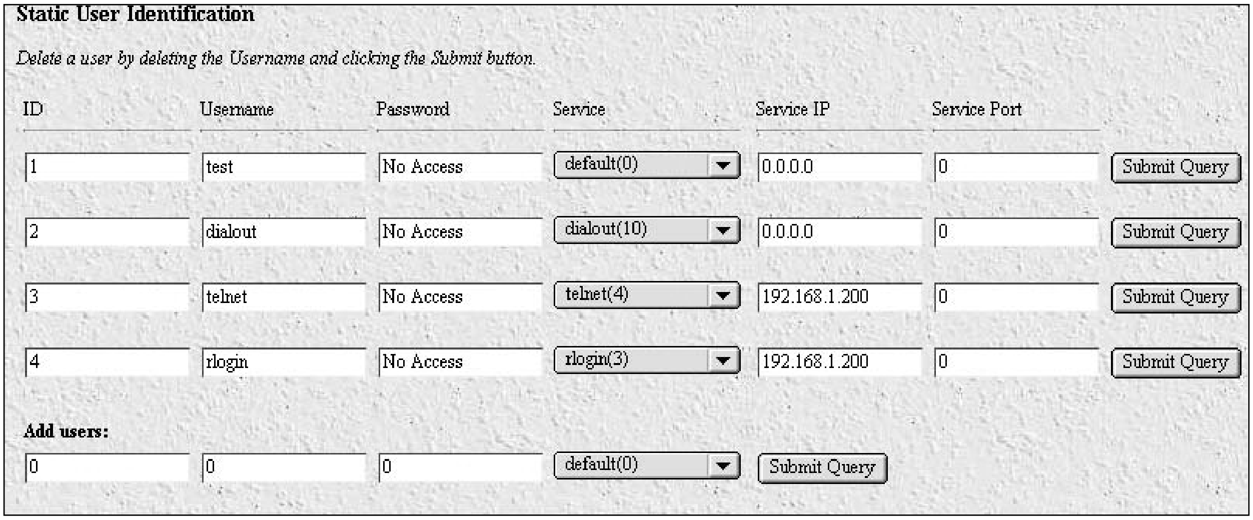
Acct Port (auAcctPort) is the UDP port on the accounting server specified in Acct Address that the 2800 should use to transfer accounting information. RFC 2139 calls out the port of 1813 as the standard RADIUS accounting port. Some older implementations of RADIUS use port 1646 as the accounting port.

Accounting Enable (auAccountingEnable) is a switch which allows the enabling or disabling the reporting of accounting information on the 2800. Select enableAccounting to begin accounting of RADIUS authenticated users. Select disableAccounting to disable the accounting feature.

Static User Authentication

After selecting Modify from the main Authentication screen, you may change authentication parameters for both RADIUS users and Static users. Static users are simply users and passwords entered into the 2800's internal users database. You may add up to are 100 static users in the 2800 (see Figure A-7, below). You must have **superuser** access make changes to the static user database. Following Figure A-7 are descriptions for each variable on this page.

Figure A-7. Static User Identification Setup



Static User Identification

Delete a user by deleting the Username and clicking the Submit button.

ID	Username	Password	Service	Service IP	Service Port	
1	test	No Access	default(0) ▼	0.0.0.0	0	Submit Query
2	dialout	No Access	dialout(10) ▼	0.0.0.0	0	Submit Query
3	telnet	No Access	telnet(4) ▼	192.168.1.200	0	Submit Query
4	rlogin	No Access	rlogin(3) ▼	192.168.1.200	0	Submit Query

Add users:

0	0	0	default(0) ▼	Submit Query

User ID (suID) Identifies the entry in the table of users. For the next user, select the next unused number. If you select a number that is already displayed in the Static User Identification table, you will overwrite a current entry in user database.

Username (suUsername) This is a unique name, to be provided at login time.

Password (suPassword) This is the password above user

Service (suService) This option instructs the 2800 on how to service the incoming call. Select from:

default	This is the default service as specified under Dial-In (See Dial-In)
admin	
monitor	
rlogin	Causes the 2800 to rlogin into another host
telnet	Causes the 2800 to telnet into another host
ppp	2800 will try to negotiate a PPP session
cppp	2800 will try to negotiage a Compressed-PPP session (see note below)
slip	2800 will negotiate a SLIP connection
cslip	2800 will negotiate a Compressed-SLIP connection

dialout 2800 will give a dialout connection. The dialout connection is an AT command set driven connection into one of the 2800 modems. On line help is provided by typing ‘at help <cr>‘

NOTE: If a user attempts to login in using a different service then he/she has been provisioned with, the 2800 will reject the user. The exception to this is CPPP which will revert to PPP if CPPP is not available on the client.

NOTE: All changes made to the running configuration must be saved to FLASH by selecting RECORD CURRENT CONFIGURATION under Immediate Actions on the HOME page of the 2800. Failure to do so will cause all configuration information to be lost the next time the 2800 is re-booted.

Service IP (suServiceIP) This is the IP of the rlogin or telnet host.

Service Port (suServicePort) This is the port number to connect to the service host. If the number is 0 then use the default values for telnet (port number 23) and rlogin (port number 513).

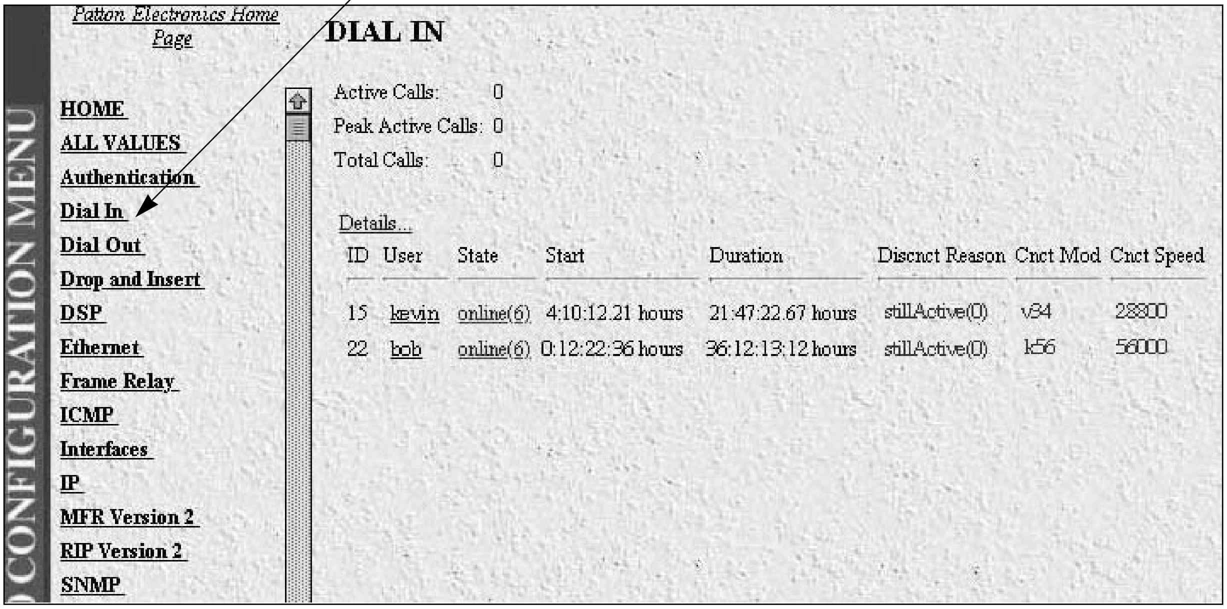
NOTE: All change made to the running configuration must be saved to flash by using the Record Current Configuration under Immediate Actions on the HOME page of the 2800. Failure to do so will cause all configuration information to be lost the next time the 2800 is re-booted.

Dial In

The Dial In Section contains items that are associated with dial in user connections. Dial In contains read only and read write parameters. This section covers items that are associated with the user dialing in, including call statistics, type of service used, modem specific statistics, write parameters for Login ,service, domain, attempts, configuration of link, maximum time, and modem configuration.

To reach the Dial In Section, select Dial In from the 2800 Configuration Menu. (see Figure A-8, below). Following Figure A-8 are descriptions for each variable on this page.

Figure A-8. Dial In Main Screen



Active Calls: 0
Peak Active Calls: 0
Total Calls: 0

Details...

ID	User	State	Start	Duration	Discnct Reason	Cnct Mod	Cnct Speed
15	kevin	online(6)	4:10:12.21 hours	21:47:22.67 hours	stillActive(0)	v34	28800
22	bob	online(6)	0:12:22:36 hours	36:12:13:12 hours	stillActive(0)	k56	56000

The Dial In Section covers two main topics:

1. **Dial In Details:** show modifiable settings common to all dial in users. To view or modify global settings, select Details from this page.

2. **User Statistics:** show statistics for individual users (i.e. user kevin, as shown above in Figure 3-9). To view or modify individual user settings, select an active user under the **State (diactState)** heading on this page.

These sections are described below.

Active Calls (diActive) The total number of active calls and calls that are initiating. If no calls are active then you will not see any User State Session Time parameters. This screen shows all current attached users, the users state, and time that the user has been on 2800.

Peak Active Calls (diMaxActive) The maximum number of active calls seen at one time.

Total Calls (diTotalCallAttempts) The total number of calls attempted since the last boot of the box.

ID (diactIndex) Unique identification of this active call for internal use.

User (diactusername) The user name that the caller entered. This can be a static user or a RADIUS user’s login name.

State (diactState) As the call comes into the RAS it can be in one of five states.

Ringing The call has been recognized by the RAS and is in process of going off hook.

Connecting The unit has assigned a DSP to the incoming call and is now in the process of negotiation of the modem type of modulation V.34 V.32 ISDN or 56K.

Authenticating The RAS is in the process of Verifying the users passwords by using the static or Radius authentication.

Online The RAS has completed authentication and we are ready to browse the Web.

Dead The user has been disconnected and this message will go away after the linger time is up .

Start (diactSessionStartTime) The number of seconds this call was/is active.

Duration (diactSessionTime) The number of seconds this call was/is active. Time in seconds the user has been connected.

Disconnect Reason (diactTerminateReason) The reason a call was disconnected.

Connect Mod (diactModulation) The modulation of the link.

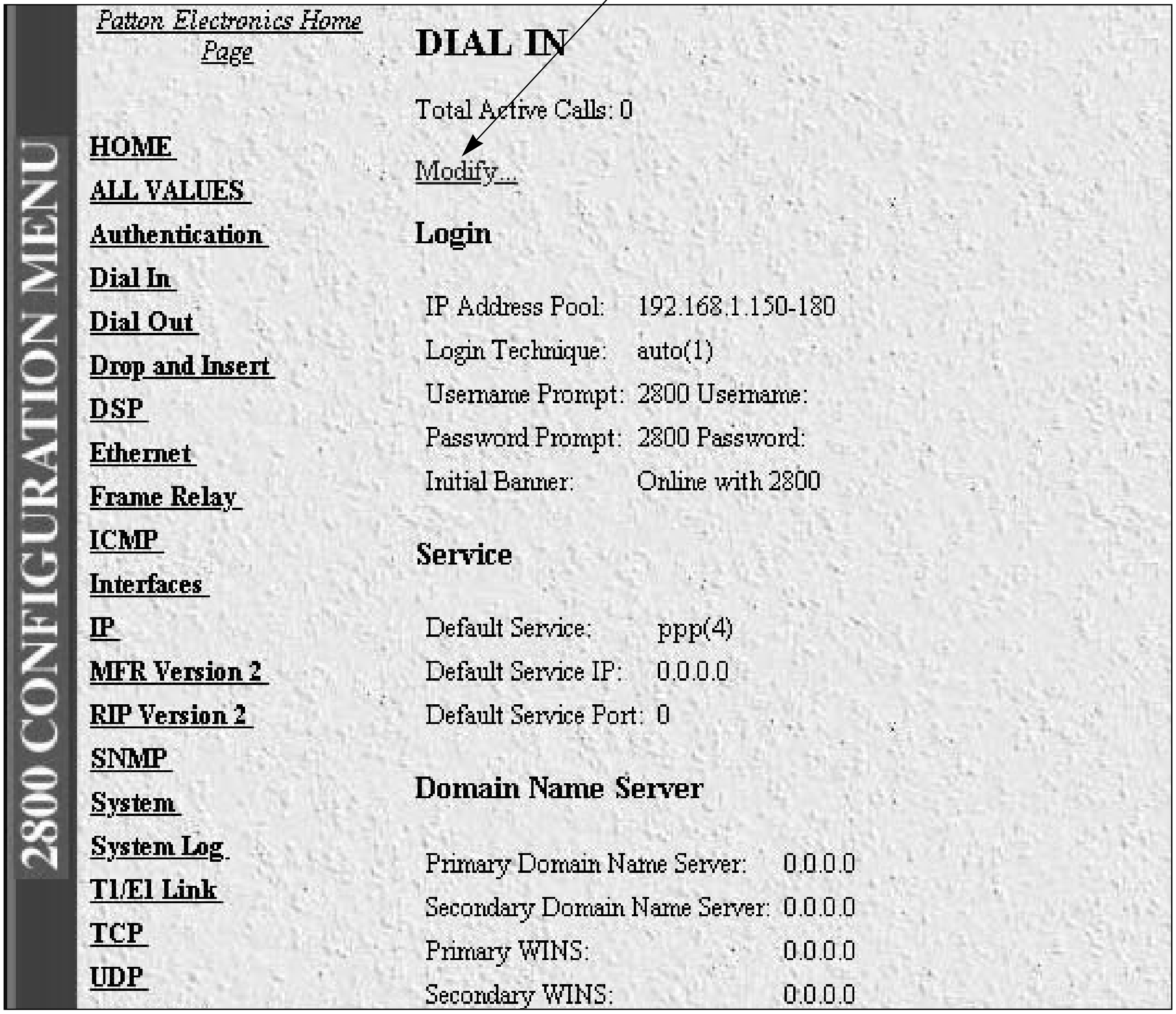
unknown(0),
v21(1),
v22(2),
v32(3),
v34(4),
k56(5),
x2(6),
vpcm(7),
v110(8),
isdn64(9),
isdn56(10)

Connect Speed (diactSpeed) The connected speed of the link.

Dial In Details

Dial In Details show how the system is currently set up to handle dial in users. To view this page, select Details from the main Dial In screen. Scroll down the screen to view additional Dial In parameters. You may also modify the Dial In parameters by selecting Modify from this screen as shown in Figure A-9, below.

Figure A-9. Dial In Details



DIAL IN

Total Active Calls: 0

Login

IP Address Pool: 192.168.1.150-180
Login Technique: auto(1)
Username Prompt: 2800 Username:
Password Prompt: 2800 Password:
Initial Banner: Online with 2800

Service

Default Service: ppp(4)
Default Service IP: 0.0.0.0
Default Service Port: 0

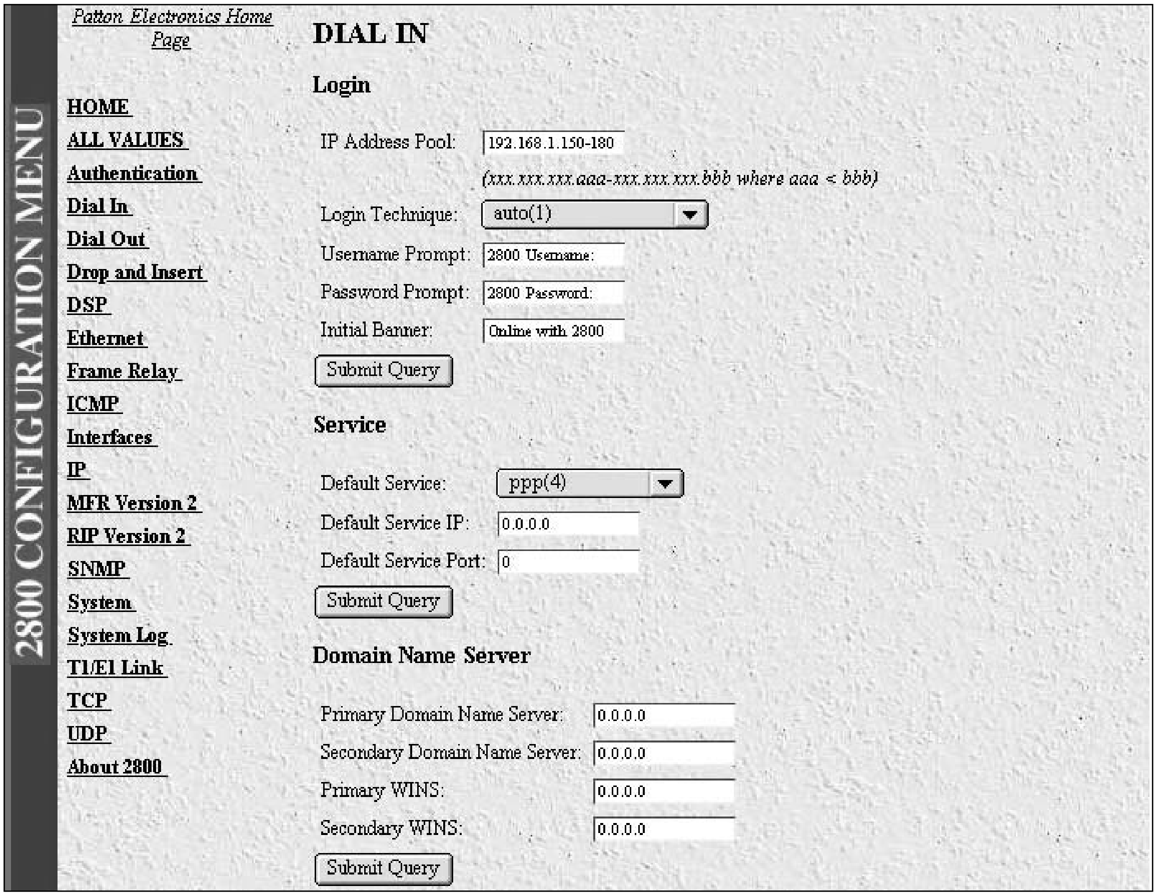
Domain Name Server

Primary Domain Name Server: 0.0.0.0
Secondary Domain Name Server: 0.0.0.0
Primary WINS: 0.0.0.0
Secondary WINS: 0.0.0.0

Dial In Details (Modify Login, Service and DNS)

From this screen you can modify Login, Service and Domain Name Server parameters for dial in users (see Figure A-10, below). To reach this screen, select Modify from the main Dial In Details screen.

Figure A-10. Dial In Details (Modify Login, Service and DNS Objects)



DIAL IN

Login

IP Address Pool: 192.168.1.150-180
(xxx.xxx.xxx.aaa-xxx.xxx.xxx.bbb where aaa < bbb)
Login Technique: auto(1)
Username Prompt: 2800 Username:
Password Prompt: 2800 Password:
Initial Banner: Online with 2800

Service

Default Service: ppp(4)
Default Service IP: 0.0.0.0
Default Service Port: 0

Domain Name Server

Primary Domain Name Server: 0.0.0.0
Secondary Domain Name Server: 0.0.0.0
Primary WINS: 0.0.0.0
Secondary WINS: 0.0.0.0

Login

Use this section to configure the IP address pool, login technique and general login information.

IP Address Pool (diIpPool) Enter a range of IP addresses separated by "-"
See example 209.49.110.151-155. String describing the IP address pool that will be used by this PAR. You can mix IP networks for example: 209.49.110.151-155 209. 49.110.160-165
209.49.110.3,10,13

Login Technique (diLoginTechnique) This variable defines the login sequence that a dial-up user will see. The various options are defined below:

auto(1) This is the most flexible. A username prompt is displayed. The received data is monitored for PPP content. If the received data looks like PPP packets then PAP or CHAP authentication will be allowed. If the received data looks like a username then a normal query Text login will continue.
text(2) A Username prompt is displayed and a username must be entered. If the received username is a static user with no password defined then the connection completes and no password prompt is issued. If a password is required then a password prompt is displayed and a password must be entered.
pap(3) This setting assumes that all calls will be PPP users. No username or password prompt will be displayed. The system will go directly to PPP processing. The dial-up user must be configured for PAP authentication. NOTE: If user is not configured for PAP he will be disconnected.
chap(4) This setting assumes that all calls will be PPP users. No username or password prompt will be displayed. The system will go directly to PPP processing. The dial-up user must be configured on his computer for CHAP authentication. NOTE: If user is not configured for CHAP he will be disconnected.
papORchap(5) This setting assumes that all calls will be PPP users. No username or password prompt will be displayed. The system will go directly to PPP processing. The dial-up user must be configured for PAP or CHAP authentication.

Username Prompt (diUsernamePrompt) This is what will be displayed when the user first connects after the Initial Banner is displayed. The string can be up to 39 characters. This should be a ASCII printable string and can include carriage returns and line feeds. This applies only for text users not PPP. See also Initial Banner
For example the prompt would be:

Enter user name ?

Password Prompt (diPasswordPrompt) This defines the character string that will be displayed at user authentication time to request the users password. The string can be up to 39 characters. This should be a ASCII printable string and can include carriage returns and line feeds. This applies only for text users not PPP. For example, the prompt would be:

Enter a password:

Initial Banner (diBanner) A string to initially display for the user. Attached text. What to display initially. The string can be up to 39 characters. This should be a ASCII printable string and can include carriage returns and line feeds. After this is displayed then the username prompt will be displayed.

Service

This section defines the user login service.

Default Service (diService) This object defines the default service that will be provided if the authentication technique does not specifically provide a service type If no service is specified on the static users list under Authentication. See Authentication.
The options are

rlogin(1)	User will be automatically given a rlogin prompt.
telnet(2)	User will be automatically given a telnet prompt.
ppp(3)	Only a PPP connection will be allowed.
slip(4)	Only a SLIP connection will be allowed.

Default IP Service (diServiceIP) This object defines the IP address which will be used for login connections (telnet, rlogin) when the authentication technique has not specifically provided an IP address to connect to. If no TCP port number is specifically provided by the authentication technique then the UNIX defaults will be used:

telnet port 23
rlogin port 513

Default Service Port (diServicePort) This object defines the IP port number which will be used for login connections (telnet,rlogin) when the authentication technique has not specifically provided a port number to connect to. If no TCP port number is specifically provided then the UNIX defaults will be used:
telnet port 23
rlogin port 513

Domain Name Server

This section defines the primary and secondary domain name servers for ip and Windows.

Primary Domain (diPrimaryDNS) The primary domain name server address to pass to the caller (Win95 PPP). The first place to try to resolve host names. I.e. IP address 204.91.99.128

Secondary Domain (diSecondaryDNS) The secondary domain name server address to pass to the caller (Win95 PPP). The next place to try to resolve the host name.

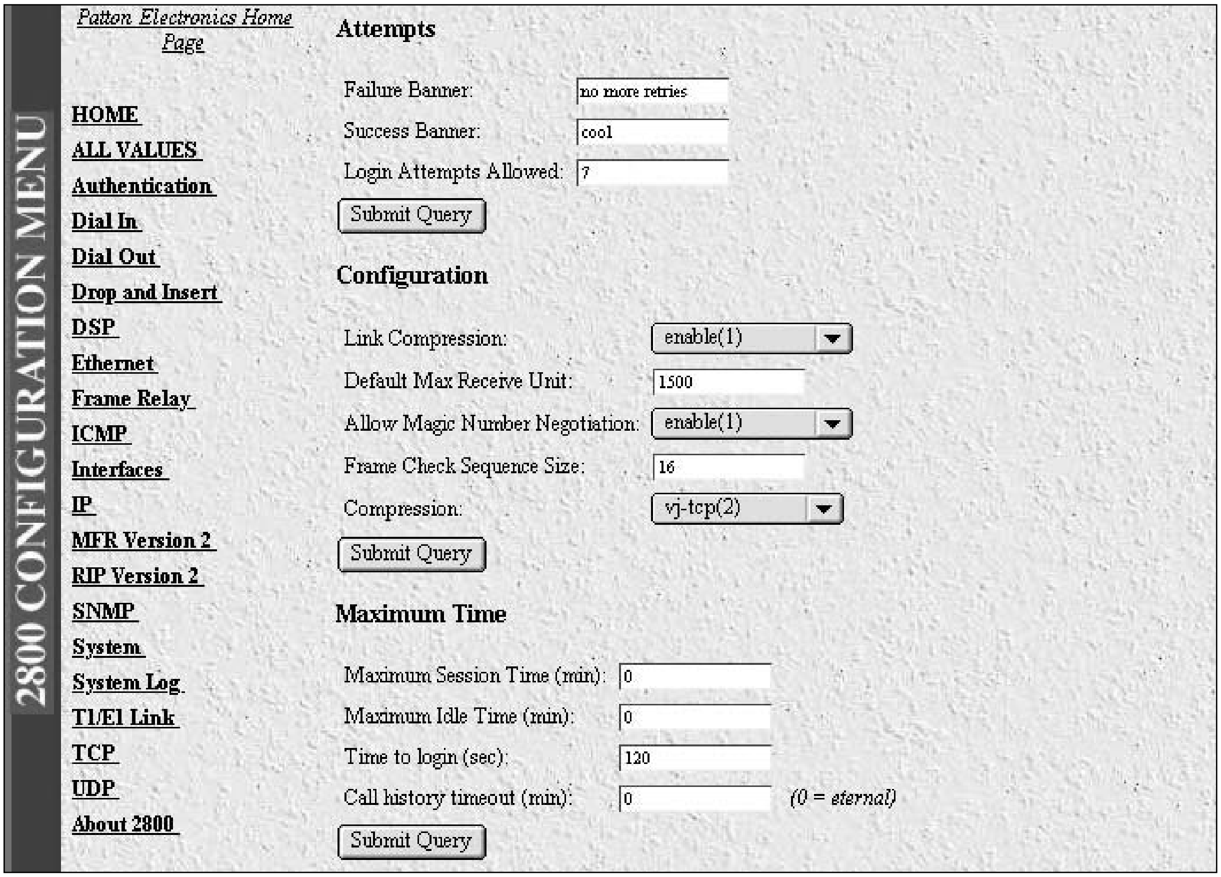
Primary WINS (diPrimaryWINS) The primary Windows name server address to pass to the caller (Win95 PPP). The Windows Internet Naming Service (WINS).

Secondary WINS (diSecondaryWINS) The secondary Windows name server address to pass to the caller (Win95 PPP). The Windows Internet Naming Service (WINS).

Dial In Details (Modify Attempts, Configuration, Maximum Time)

From this screen you can modify Attempts, Configuration, and Maximum Time parameters for dial in users (see Figure A-11, below). To reach this screen, scroll down from the previous screen.

Figure A-11. Dial In Details (Modify Attempts, Configuration, Maximum Time Objects)



Attempts

Failure Banner: no more retries

Success Banner: cool

Login Attempts Allowed: 7

Configuration

Link Compression: enable(1)

Default Max Receive Unit: 1500

Allow Magic Number Negotiation: enable(1)

Frame Check Sequence Size: 16

Compression: vj-tcp(2)

Maximum Time

Maximum Session Time (min): 0

Maximum Idle Time (min): 0

Time to login (sec): 120

Call history timeout (min): 0 *(0 = eternal)*

Attempts

This section shows failure to connect parameters.

Failure Banner (diFailureBanner) This defines a message that will be displayed to a user when authentication failed. This is only relevant when the authentication technique was Text.
Text string up to 254 characters.

Login Attempts Allowed (diAllowAttempts) The maximum number of attempts a user will be given to login before being disconnected. This applies to Text authentication only. PAP and CHAP authentication are only allowed a single attempt.

Configuration

Use this section to configure link compression, MRUs, and Asynchronous-Control-Character-Map (ACC) parameters.

Link Compression (diLinkCompression) This object enables the PPP link layer address and protocol field compression. When enabled the PPP negotiations will DESIRE link compression but may disable the compression due the other end of the link. When disabled the PPP negotiations will FORCE no compression on the PPP link. This is a default setting which may be overridden by the authentication of a specific user.
The two settings are:

enable(1)
disable(2)

Default Max Receive Unit (diConfigInitialMRU) Default setting for Maximum Receive Unit (MRU) if it's not changed by authentication or PPP.

Receive ACC Map (diConfigReceiveACCMap) Desired asynchronus character map for incoming. The Asynchronous-Control-Character-Map (ACC) that the local PPP entity requires for use on its receive side. In effect, this is the ACC Map that is required in order to ensure that the local modem will successfully receive all characters. The actual ACC map used on thereceive side of the link will be a combination of the local node's pppLinkConfigReceiveACCMap and the remote node's pppLinkConfigTransmitACCMap. Changing this object will have effect when the link is next restarted.

Transmit ACC Map (diConfigTransmitACCMap) Desired asynchronus character map for outgoing. The Asynchronous-Control-Character-Map (ACC) that the local PPP entity requires for use on its receive side. In effect, this is the ACC Map that is required in order to ensure that the local modem will successfully transmit all characters. The actual ACC map used on the transmit side of the link will be a combination of the local node's pppLinkConfigReceiveACCMap and the remote node's pppLinkConfigTransmitACCMap. Changing this object will have effect when the link is next restarted.

Allow Magic Number Negotiation (diConfigMagicNumber) Determines if magic number negotiation should be done. enable(1) then the local node will attempt to perform Magic Number negotiation with the remote node. disable(2) then this negotiation is not performed. In any event, the local node will comply with any magic number negotiations attempted by the remote node, per the PPP specification. This parameter is used to check whether a link is in a looped-back state. Changing this object will have effect when the link is next restarted."
REFERENCE "Section 7.6, Magic Number, of RFC1331."
The two settings are:

enable(1)
disable(2)

Frame Check Sequence Size (diConfigFcsSize) The size of the FCS, in bits, the local node will attempt to negotiate for use with the remote node. The size of the Frame Check Sequence (FCS) in bits that the local node will generate when sending packets to the remote node. The value of this object is meaningful only when the link has reached the open state (ifOperStatus is up).

Compression (diIpConfigCompression) If none then the local node will not attempt to negotiate any IP compression otherwise, the local node will attempt to negotiate compression mode indicated by the enumerated value. Changing this object will have effect when the link is next restarted.
REFERENCE Section 4.0, Van Jacobson TCP/IP Header Compression of RFC1332.
The two settings are:

none(1)
vj-tcp(2)

Maximum Time

This section contains the time out for the session idle time to login and the MIB data linger time.

Maximum Session Time (min) (diSessionTimeout) This is the maximum time in minutes which a connection is allowed to be maintained. After this time the connection will be terminated, even if there is active traffic on the connection. This is a default setting which may be overridden by the authentication of a specific user.

Maximum Idle Time (min) (diIdleTimeout) This is the maximum time in minutes which a connection is allowed to be maintained with no traffic. After this time, if no traffic is seen, the connection will be terminated. This is a default setting which may be overridden by the authentication of a specific user.

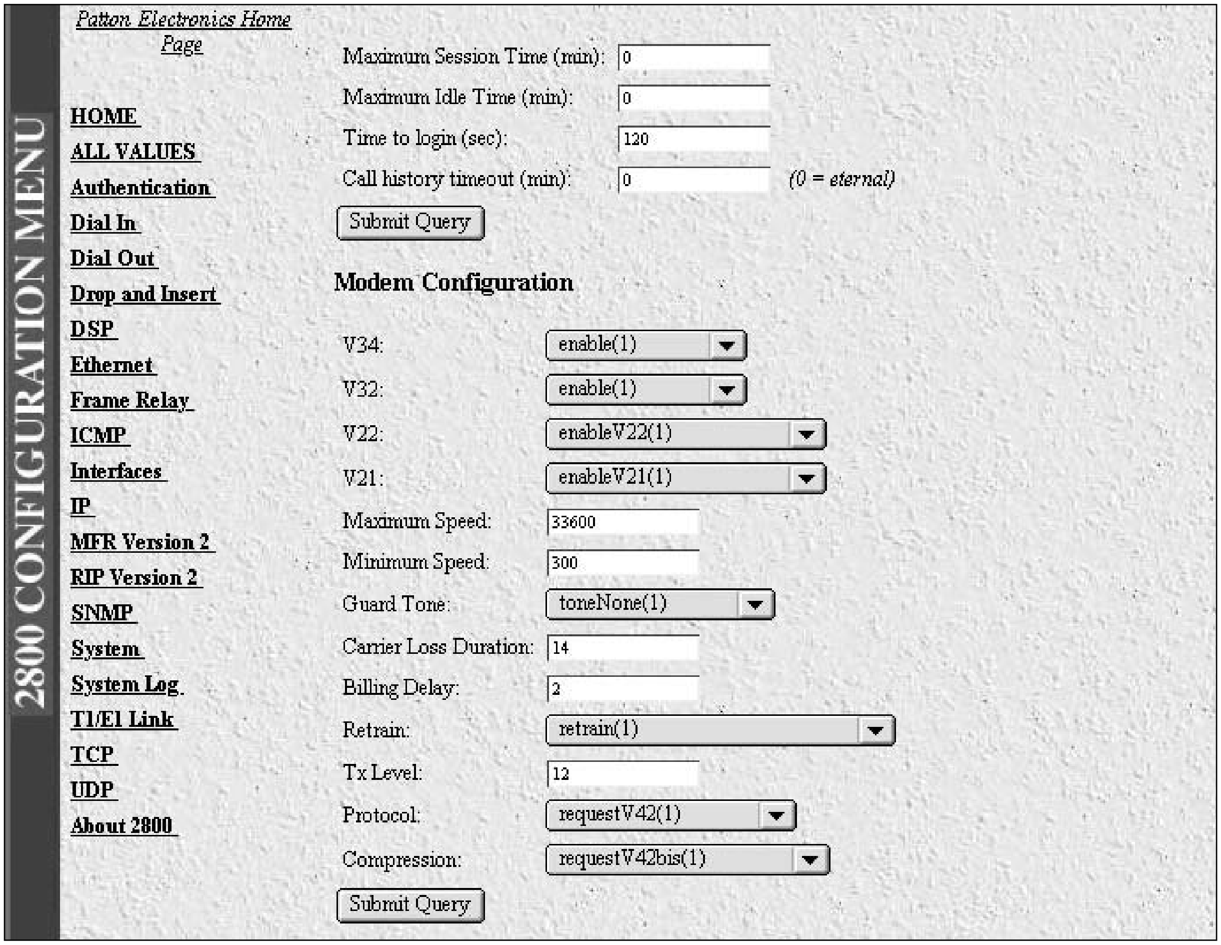
Time to login (sec) (diLoginTimeout) This is the maximum time in seconds which a user is given to login. This is only relevant before the user is authenticated. This setting should take into account any time required to query a remote authentication server (For example RADIUS).

Call History Timeout (sec) (diLingerTime) Number of seconds a MIB entry in the Active table will remain after the call is dead.

Dial In Details (Modify Modem Configuration)

From this screen you can modify Modem Configuration objects for dial in users (see Figure A-12, below). To reach this screen, scroll down from the previous screen.

Figure A-12. Dial In Details (Modify Modem Configuration Objects)



Maximum Session Time (min): 0
Maximum Idle Time (min): 0
Time to login (sec): 120
Call history timeout (min): 0 *(0 = eternal)*

Modem Configuration

V34: enable(1)
V32: enable(1)
V22: enableV22(1)
V21: enableV21(1)
Maximum Speed: 33600
Minimum Speed: 300
Guard Tone: toneNone(1)
Carrier Loss Duration: 14
Billing Delay: 2
Retrain: retrain(1)
Tx Level: 12
Protocol: requestV42(1)
Compression: requestV42bis(1)

Modem Configuration

Use this section to select the modem connetion parameters.

V34 (diModemV34Enable) Allow V.34, K56 Flex and V.90 options up to 56 kbps.

disable(0)
v34Only(1)
v34andK56(2)
v34andV90(3)

V32 (diModemV32Enable) Allow V.32 and V.32bis modulations up to 14.4 kbps.

disable(0)
enable(1)

V22 (diModemV22Enable) Allow V.22 or Bell 212 modulations

disable(0)
enableV22(1)
enableBell212(2)

V21(diModemV21Enable) Allow V.21 or Bell 103 modulations

disable(0)
enableV21(1)
enableBell103(2)

MaxSpeed (diModemMaxSpeed) This variable allows the selection of the fastest data rate that will be negotiated. The different rates are: 33600, 31200, 28800, 26400, 28800, 26400, 2400, 21600, 19200, 16800, 14400, 12000, 9600, 7200, 4800, 2400, 1200, 0-300

MinSpeed (diModemMinSpeed) This variable allows the selection of the slowest data rate that will be negotiated. The different rates are: 33600, 31200, 28800, 26400, 28800, 26400, 24000, 21600, 19200, 16800, 14400, 12000, 9600, 7200, 4800, 2400, 1200, 0-300

MinSpeed (diModemGuardTone) Normally a guard tone is not required. But, one can be inserted. This operates for Phase Shift Key modulations only. Not for V.32 or V.34.

tone None(1)
tone1800(3)

CarrierLossDuration (diModemCarrierLossDuration) The number of 100ms intervals the carrier must be lost before it is considered the connection dead. A setting of 255 indicates forever.
The range is (1..255)

Retrain (diModemRetrain) Allow the modem to monitor the line quality and request a fallback or retrain for poor quality and a fall forward for good quality.

none (0)	Do not allow modem to retrain, fallback or fall forward.
retrain(1)	Allow modem retrain.
fallForwardFallBack(2)	Allow the modem to fallback to a slower speed or forward to a faster speed.

TxLevel (diModemTxLevel) This variable should be set with caution; and normally only after talking to a factory representative. This sets the transmit level power level of the modem. The scale is 0 (0 dB) to 15 (-15 dB) in 1 db increments. Note that larger numbers mean less power. The range is (0..15)

Protocol (diModemProtocol) Selection of the data protocol to use on the modem. This allows the request of or forcing of V.42 error correction protocol.

Direct(0)	No error correction will be used.
requestV42(1)	Enable V.42 if this is selected then the modem will negotiate V.42 or no correction.
requrieV42(2)	V.42 is mandatory if this is not a V.42 modem then disconnect.

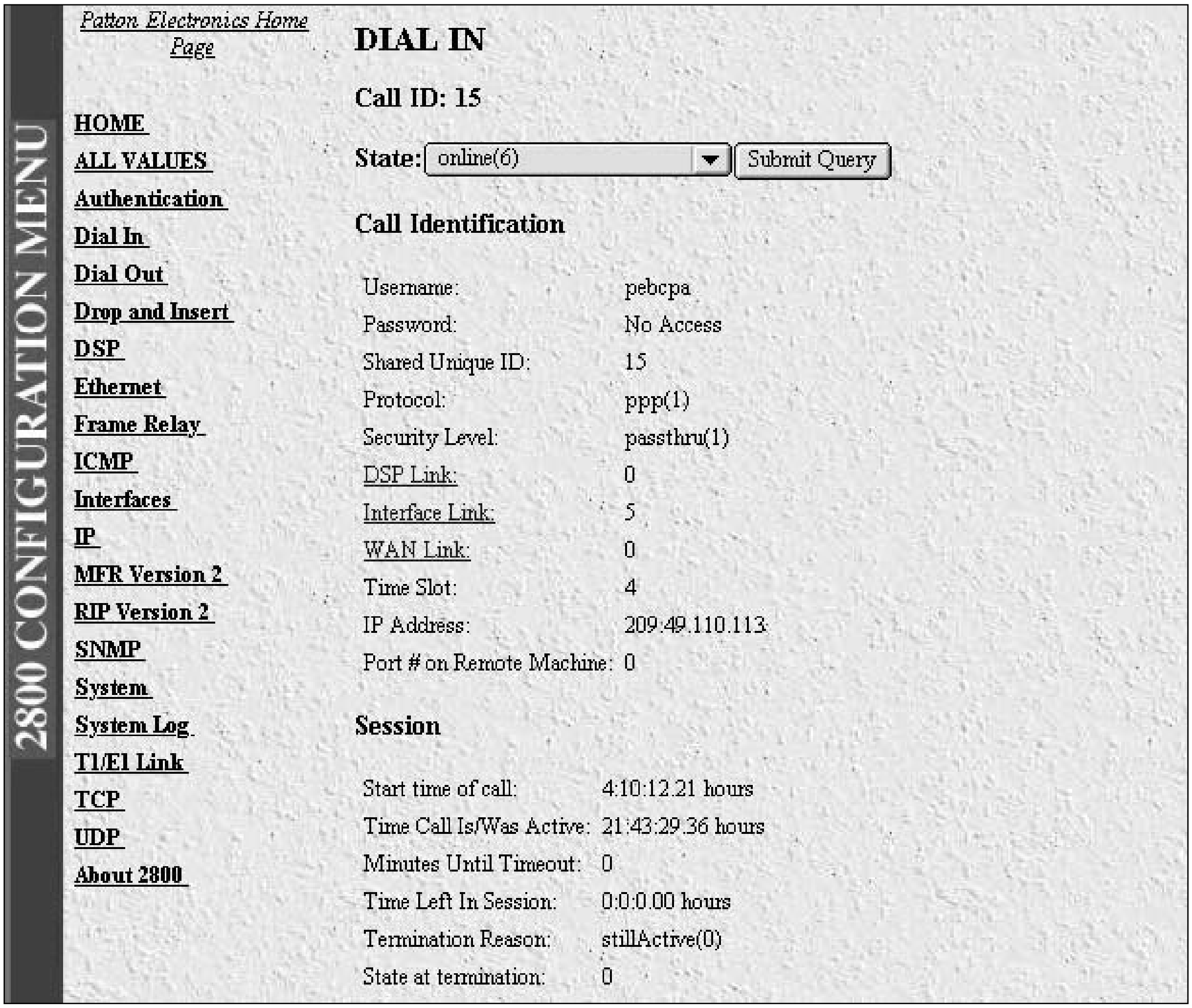
Compression (diModemCompression) Selection of the data compression protocol to use on the modem. This allows the request of or forcing of V42 compression protocol. This will only be used if V42 error correction is active.

Direct(0)	No compression will be used.
requestV42bis(1)	Enable V.42 if this is selected then the modem will negotiate V42 or no correction.
requestV42bis(2)	V.42bis is mandatory if this is not a V.42bis modem then disconnect.

User Statistics (Call Identification, Session)

This screen shows statistics for individual dial in users. To view individual user statistics, select an active user under the User heading on the main Dial In screen (user statistics will only be available for currently connected users. If there are no current Dial In users, the screen will be blank. Figure A-13, below, shows user information for a Unique ID. The Headings DSP Link, Interface Link, WAN Link, and Time Slice Link shown below pertain to a unique time slot defined on each of these links. For specific details on the function of parameters defined under these sections, refer to each under the 2800 Configuration Menu.

Figure A-13. User Statistics (Call Identification, Session)



DIAL IN

Call ID: 15

State: online(6)

Call Identification

Username:	pebcpa
Password:	No Access
Shared Unique ID:	15
Protocol:	ppp(1)
Security Level:	passthru(1)
DSP Link:	0
Interface Link:	5
WAN Link:	0
Time Slot:	4
IP Address:	209.49.110.113
Port # on Remote Machine:	0

Session

Start time of call:	4:10:12.21 hours
Time Call Is/Was Active:	21:43:29.36 hours
Minutes Until Timeout:	0
Time Left In Session:	0:0:0.00 hours
Termination Reason:	stillActive(0)
State at termination:	0

Call ID: (diactIndex) Unique identification of this active call for internal use.

Current Progress (diactState) Indicates current progress of the caller and reason for termination.

Ringing	The call has been recognized by the PAR and is in the process of going off hook
Connecting	The unit has assigned a DSP to the incoming call and is now in the process of negotiation of the modem type of modulation V.34 V.32 ISDN or 56K.
Authenticating	The PAR is in the process of verifying the users passwords by using the static or Radius authentication.
Online	The PAR has completed the authentication and we are now ready to brows the Web.
Dead	The user has been disconnected and this message will go away after the linger time is up.
Kill	The administrator can manually disconnect the user by setting this para meter.

Username (diactUsername) The username that the caller entered.

Password (diactPassword) The password that the caller entered.

Shared Unique ID (diactMultiIndex) Unique identification shared between multi-link active calls. This is used for multi link PPP.

Protocol (diactProtocol) This lets you know what type of service or link is being provided on this call.

PPP	The user has a PPP link running.
Slip	The user has a Slip link running
Telnet	The user has a telnet session running
Rlogin	The user has a rlogin session running

Security Level (diactAccessLevel) This is the security level given to this call all users will have the default of PASSTHRU. Monitor and change will be used by the PAR administrator.

Passthru	No read or write access to configuration.
Monitor	Read only access to the configuration screens.
Change	Read and Write access to the configuration screens.

DSP Link (diactDSPIndex) This is the physical DSP chip that this user is on. This is a number (0 to 29.)

Interface Link (diactIFIndex) This is the Ethernet LAN connection 0 is the physical 10baseT port. There is only one for now. This will have only one value 0.

WAN Link (diactLinkIndex) This is the T1/E1 WAN port that this call is on 1 or 2.
Each T1 can have up to 24 calls on it.
Each E1 can have up to 30 calls on it.
The PAR has two T1/E1 ports.
This is a number 1 or 2.

Time Slot Link (diactSlotIndex) This describes which channel that this call is on the T1/E1.
T1 1-24 channels. This is a number from 1-30.

IP Address (diactIP) The current assigned IP address from the IP address pool. The remote users PC is assigned to this address. This is a IP address 0.0.0.0 format.

Port # (diactPort) The port number that is used by this connection. This is the TCP port number they range from 0 to 65,535. Ports in the range of 0 to 1023 are well-known ports used to access standard services. TELNET uses port 23 RLOGIN uses port 513.

Session

Start time of call (diactSessionStartTime) The number of seconds this call was/is active.

Time Call Is/Was Active (diactSessionTime) The number of seconds this call was/is active.

Minutes Until Timeout (diactRemainingIdle) Number of minutes until idle timeout (counts down).

Time Left In Session (diactRemainingSession) Number of seconds left in this session (counts down).

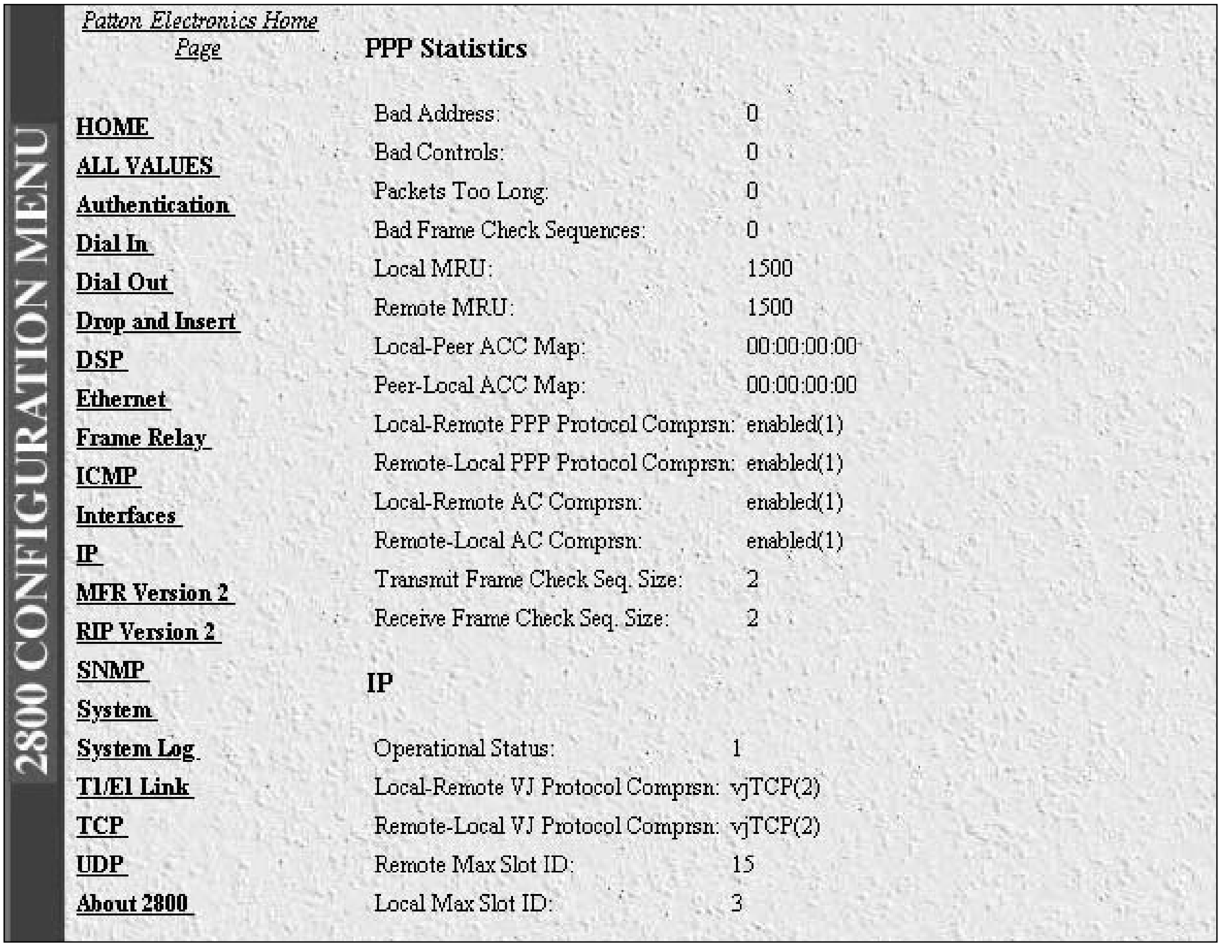
Termination Reason (diactTerminateReason) The reason a call was disconnected.

State at termination (diactTerminateState) Indicates the value of diactState when the call was terminated.

User Statistics (PPP Statistics, IP)

This screen shows statistics for individual dial in users. Figure A-14, below, shows PPP Statistics and IP statistics for a specific dial in user. To reach this screen, scroll down from the previous screen.

Figure A-14. User Statistics (PPP Statistics, IP)



PPP Statistics

Bad Address:	0
Bad Controls:	0
Packets Too Long:	0
Bad Frame Check Sequences:	0
Local MRU:	1500
Remote MRU:	1500
Local-Peer ACC Map:	00:00:00:00
Peer-Local ACC Map:	00:00:00:00
Local-Remote PPP Protocol Comprsn:	enabled(1)
Remote-Local PPP Protocol Comprsn:	enabled(1)
Local-Remote AC Comprsn:	enabled(1)
Remote-Local AC Comprsn:	enabled(1)
Transmit Frame Check Seq. Size:	2
Receive Frame Check Seq. Size:	2

IP

Operational Status:	1
Local-Remote VJ Protocol Comprsn:	vjTCP(2)
Remote-Local VJ Protocol Comprsn:	vjTCP(2)
Remote Max Slot ID:	15
Local Max Slot ID:	3

PPP Statistics

This is the section on IP statistics of the current user selected. It is a 32bit number for all the variables.

Bad Address (diStatBadAddresses) The number of packets received with an incorrect Address Field. This counter is a component of the ifInErrors variable that is associated with the interface that represents this PPP Link.

Bad Controls (diStatBadControls) The number of packets received on this link with an incorrect Control Field. This counter is a component of the ifInErrors variable that is associated with the interface that represents this PPP Link.

Packets Too Long (diStatPacketTooLongs) The number of received packets that have been discarded because their length exceeded the MRU(Maximum Receive Unit). This counter is a component of the ifInErrors variable that is associated with the interface that represents this PPP Link. NOTE, packets which are longer than the MRU but which are successfully received and processed are NOT included in this count.

Bad Frame Check Sequences (diStatBadFCSs) The number of packets received on this link with an incorrect Control Field. This counter is a component of the ifInErrors variable that is associated with the interface that represents this PPP Link.

Local MRU (diStatLocalMRU) The current value of the MRU for the local PPP Entity. This value is the MRU that the remote entity is using when sending packets to the local PPP entity. The value of this object is meaningful only when the link has reached the open state (ifOperStatus is up).

Remote MRU (diStatRemoteMRU) The current value of the MRU for the remote PPP Entity. This value is the MRU that the local entity is using when sending packets to the remote PPP entity. The value of this object is meaningful only when the link has reached the open state (**ifOperStatus** is up)."
This is a number.

Local-Peer ACC Map (diStatLocalToPeerACCMap) The current value of the ACC Map used for sending packets from the local entity to the remote entity. The current value of the ACC Map used for sending packets from the local PPP entity to the remote PPP entity. I know which characters need to be mapped in order to be received through my modem safely. I send you my map. The value of this object is meaningful only when the link has reached the open state (**ifOperStatus** is up).

Peer-Local ACC Map (diStatPeerToLocalACCMap) The current value of the ACC Map used for sending packets from the remote entity to the local entity. The ACC Map used by the remote PPP entity when transmitting packets to the local PPP entity. You know which characters need to be mapped in order to be received through your modem safely. You combine my map with yours. The value of this object is meaningful only when the link has reached the open state (**ifOperStatus** is up).

Local-Remote PPP Protocol Comprsn (diStatLocalToRemoteProtComp) Indicates whether the local PPP entity will use Protocol Compression when transmitting packets to the remote PPP entity. The value of this object is meaningful only when the link has reached the open state (**ifOperStatus** is up)." This has two states:

PPP compression is enabled
PPP compression is disabled

Remote-Local PPP Protocol Comprsn (diStatRemoteToLocalProtComp) Indicates whether the remote PPP entity will use Protocol Compression when transmitting packets to the local PPP entity. The value of this object is meaningful only when the link has reached the open state (**ifOperStatus** is up).” This has two states:

PPP compression is enabled
PPP compression is disabled

Local-Remote AC Comprsn (diStatLocalToRemoteACComp) Indicates whether the local PPP entity will use Address and Control Compression when transmitting packets to the remote PPP entity. The value of this object is meaningful only when the link has reached the open state (**ifOperStatus** is up).” This has two states.

ACC is enabled
ACC is disabled

Remote-Local AC Comprsn (diStatRemoteToLocalACComp) Indicates whether the remote PPP entity will use Address and Control Compression when transmitting packets to the local PPP entity. The value of this object is meaningful only when the link has reached the open state (**ifOperStatus** is up). This has two states:

ACC is enabled
ACC is disabled

Transmit Frame Check Seq. Size (diStatTransmitFcsSize) The size of the Frame Check Sequence (FCS) in bits that the local node will generate when sending packets to the remote node. The value of this object is meaningful only when the link has reached the open state (**ifOperStatus** is up). The values are from (0..128)

Receive Frame Check Seq. Size (diStatReceiveFcsSize) The size of the Frame Check Sequence (FCS) in bits that the remote node will generate when sending packets to the local node. The value of this object is meaningful only when the link has reached the open state (**ifOperStatus** is up).” The values are from (0..128)

IP

This section contains the operational status and the type of IP compression used.

Operational Status (diIpOperStatus) The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed.

up(1),	ready to pass packets
down(2),	unable to pass packets

testing(3)	in some test mode

The values are from (0..128)

Local-Remote VJ Protocol Comprsn (diIpLocalToRemoteCompProt) The IP compression protocol that the local IP entity uses when sending packets to the remote IP entity. The two settings are :

none	no compression
vjTCP	enabled

Remote-Local VJ Protocol Comprsn (diIpRemoteToLocalCompProt) The IP compression protocol that the remote IP entity uses when sending packets to the local IP entity.
The two setting are :

none	no compression
vjTCP	enabled

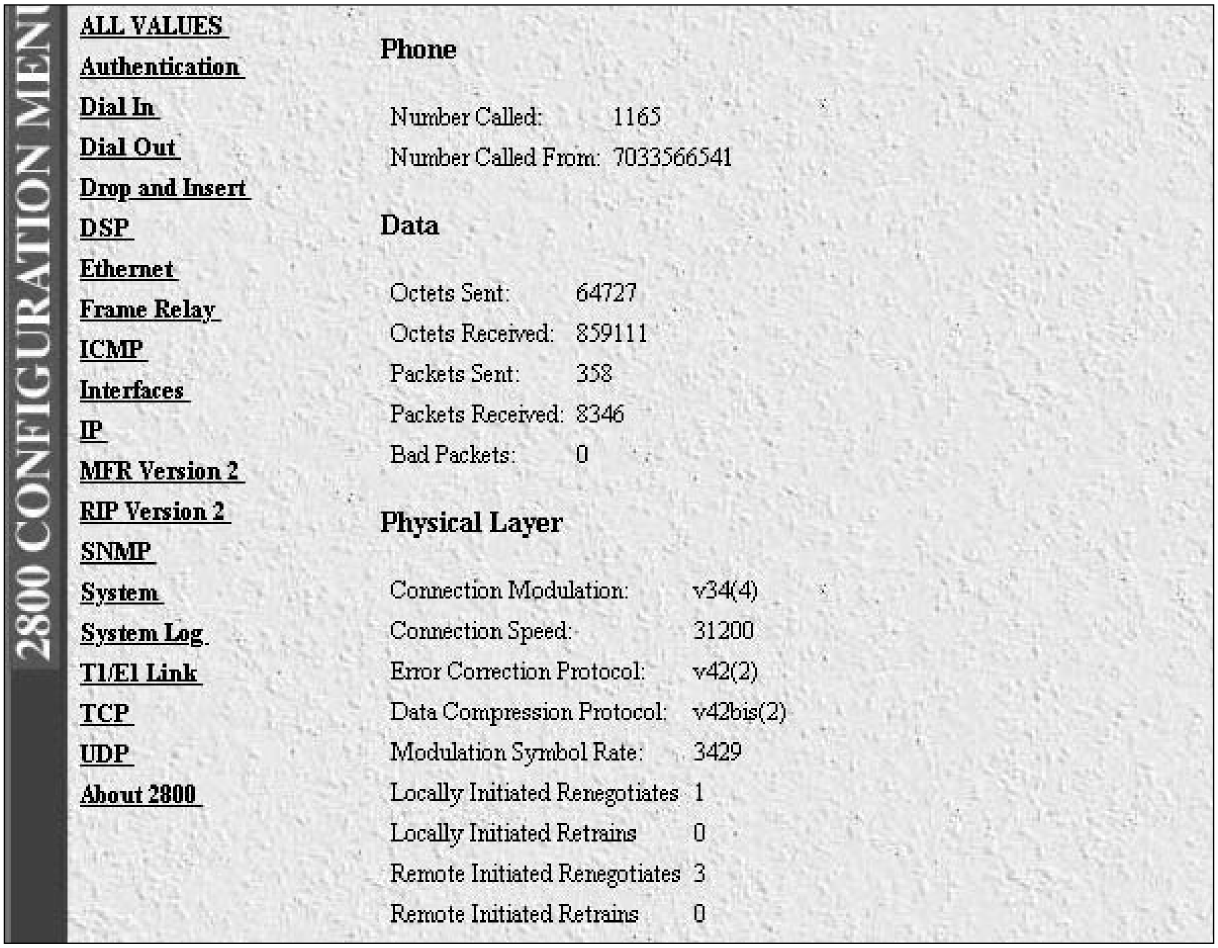
Remote Max Slot ID (diIpRemoteMaxSlotId) The Max-Slot-Id parameter that the remote node has advertised and that is in use on the link. If vj-tcp header compression is not in use on the link then the value of this object shall be 0. The range is from (0..255).

Local Max Slot ID (diIpLocalMaxSlotId) The Max-Slot-Id parameter that the local node has advertised and that is in use on the link. If vj-tcp header compression is not in use on the link then the value of this object shall be 0. The range is from (0..255).

User Statistics (Phone, Data, Physical Layer)

This screen shows statistics for individual dial in users. Figure A-15, below, shows Phone, Data, and Physical Layer parameters for a specific dial in user. To reach this screen, scroll down from the previous screen.

Figure A-15. User Statistics (Phone, Data, Physical Layer)



Phone

Number Called:	1165
Number Called From:	7033566541

Data

Octets Sent:	64727
Octets Received:	859111
Packets Sent:	358
Packets Received:	8346
Bad Packets:	0

Physical Layer

Connection Modulation:	v34(4)
Connection Speed:	31200
Error Correction Protocol:	v42(2)
Data Compression Protocol:	v42bis(2)
Modulation Symbol Rate:	3429
Locally Initiated Renegotiates	1
Locally Initiated Retrains	0
Remote Initiated Renegotiates	3
Remote Initiated Retrains	0

Phone

This section covers the phone numbers that were used for this caller.

Number Called (diactNumberDialed) The phone number that was dialed into. The number that the home user dialed to get in to the PAR. This is the called number.

Number Called From (diactCallingPhone) The phone number that was dialed from. The user's home phone number. This is the same a caller ID. This is the calling number.

Data

This section describes the amount of PPP data sent and received by this user. Bad packets and Bit Error Rate of the modem.

Octets Sent (diactSentOctets) The number of octets (bytes) sent on this call.

Octets Received (diActReceivedOctets) The number of octets (bytes) received on this call.

Packets Sent (diactSentDataFrames) The number of sent packets on this call out to the user. Version 6 nomenclature for a packet is Ipv6 header plus payload.

Packets Received (diactReceivedDataFrames) The number of received packets on this call in from the user. Version 6 nomenclature for a packet is Ipv6 header plus payload.

Bad Packets (diactErrorFrames) Number of bad received packets (CRC error incorrect Length,...).

Bit Error Rate (diactBER) The running bit error rate of the call.

Physical Layer

This section contains statistics about the modem connection. It includes modulation, levels and other modem related statistics helpful in trouble shooting modem issues. This section covers only modem type statistics and does not pertain to ISDN connections.

Connection Modulation (diactModulation) The modulation type of the modem link i.e. V.34. The modem link can have three modulation or data types.

ISDN	digital service 1B 64
V.32	Modem modulation with data rates up to 14.4
V.34	Modem modulation with data rates up to 33.6

Connection Speed (diactSpeed) The connected speed of the modem link. I.e. 28.8 BPS
These are the values in bits per second 33600, 31200, 28800, 26400, 28800, 26400, 2400, 21600, 19200, 16800, 14400, 12000, 9600, 7200, 4800, 2400, 1200, 0-300.

Error Correction (diactErrorCorrection) The modem error correction scheme used on this call.

none	No error correction on the call.
V42	Error correction mode
V120	mode for ISDN B

Compression Protocol (diactCompression) The modem compression technique used on this call.

None	No compression.
V42bis	Compression is running.
Stac	Compression is running.

Symbol Rate (diactSymbolRate) The symbol rate of the call. This is used only when in V.34 modulation type.

Locally Initiated Renegotiates (diactLocalRenegotiates) The number of times the local side (this unit) has initiated a modem speed renogotiate."
::= { diactEntry 60 }

Locally Initiated Retrains (diactLocalRetrains) The number of times the local side (this unit) has initiated a modem carrier retrain.

Remote Initated Renegotiates (diactRemoteRenegotiates) The number of times the far modem has initiated a modem speed renogotiate.

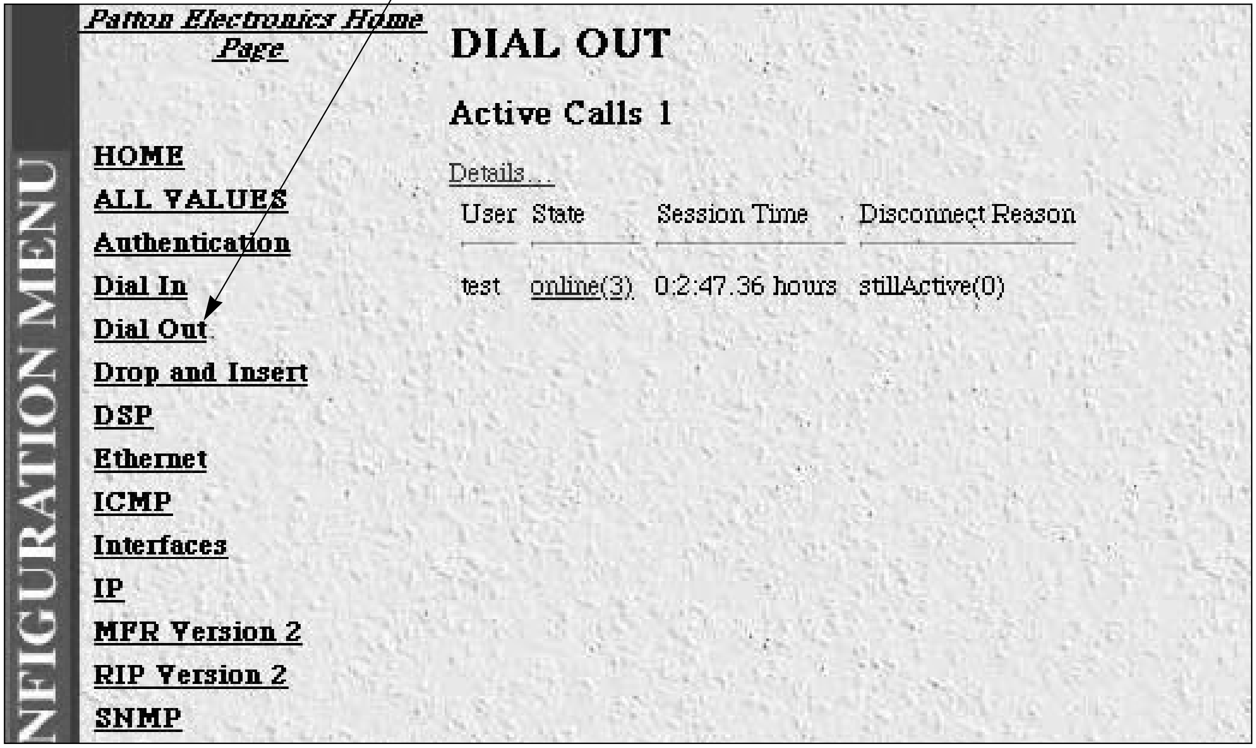
Remote Initated Retrains (diactRemoteRetrains) The number of times the far modem has initiated a modem carrier retrain.

Dial Out

The Dial Out Section contains items that are associated with making dial out connections from the 2800 to another office. This section contains read only and read/write login, maximum time, session, physical layer, and outgoing modem configuration information.

To reach the dial out Section, select Dial Out from the 2800 Configuration Menu (see Figure A-16, below). Following Figure A-16 are descriptions for each object on this page.

Figure A-16. Dial Out Main Screen



DIAL OUT

Active Calls 1

Details...

User	State	Session Time	Disconnect Reason
test	online(3)	0:2:47.36 hours	stillActive(0)

Details (contains Modifiable Dial Out Objects)

User (doactUsername) The username that the caller entered.

State (doactState) Indicates current progress

authenticating(0),
commandmode(1),
connecting(2),
online(3),
dead(4),
kill(5)

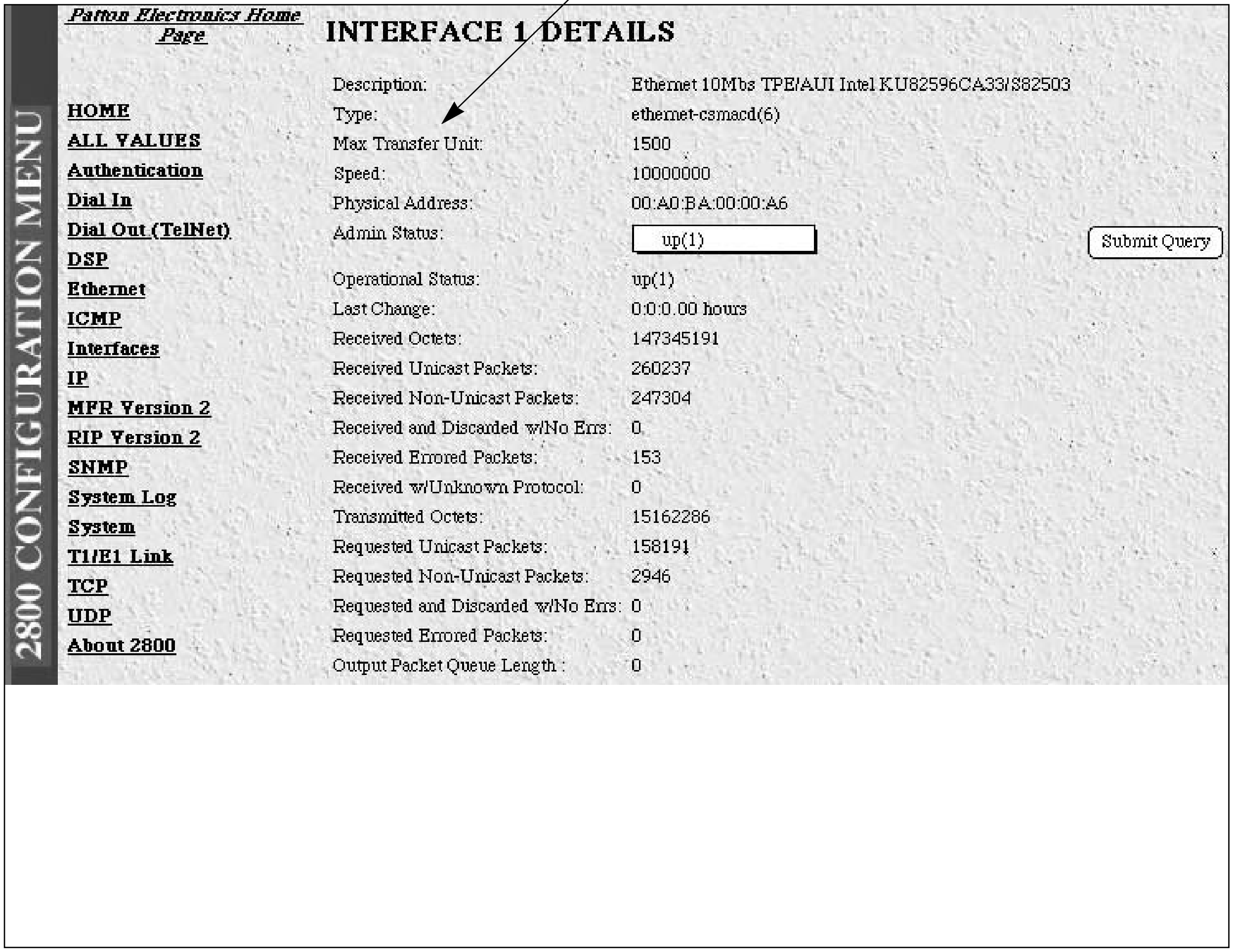
Session (doactSessionTime) The number of seconds this call was/is active.

Disconnect Reason (doactTerminateReason) The reason a call was disconnected.

Dial Out Details

Dial Out Details shows the active Dial Out configuration of the 2800. To view this page, select Details from the main Dial Out screen. Scroll down the screen to view additional Dial Out parameters. You may also modify the Dial Out parameters by selecting Modify from this screen as shown in Figure A-17, below. The objects on this screen will be discussed in the next section.

Figure A-17. Dial Out - Details



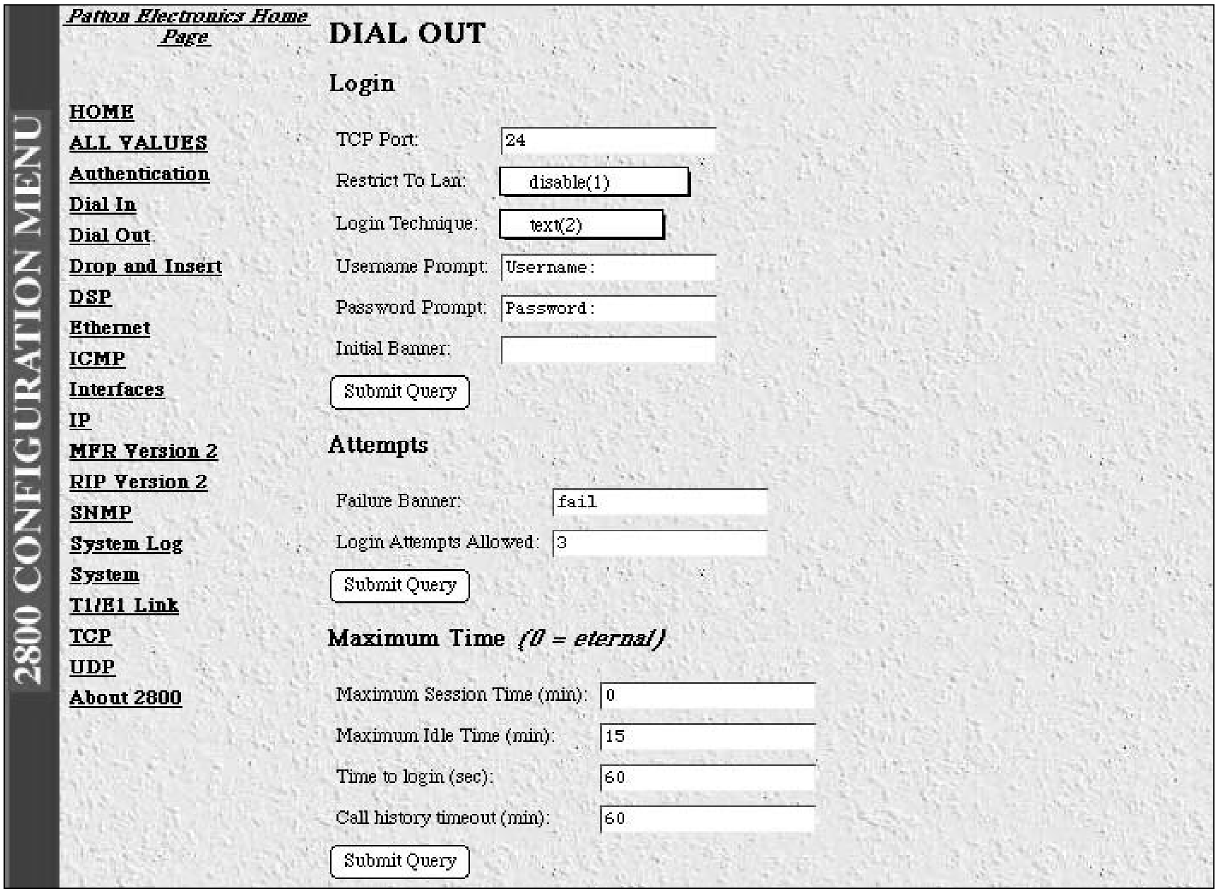
INTERFACE 1 DETAILS

Description:	Ethernet 10Mbs TPE/AUI Intel KU82596CA33/S82503
Type:	ethernet-csmacd(6)
Max Transfer Unit:	1500
Speed:	10000000
Physical Address:	00:A0:BA:00:00:A6
Admin Status:	up(1)
Operational Status:	up(1)
Last Change:	0:0:0.00 hours
Received Octets:	147345191
Received Unicast Packets:	260237
Received Non-Unicast Packets:	247304
Received and Discarded w/No Errs:	0
Received Errored Packets:	153
Received w/Unknown Protocol:	0
Transmitted Octets:	15162286
Requested Unicast Packets:	158191
Requested Non-Unicast Packets:	2946
Requested and Discarded w/No Errs:	0
Requested Errored Packets:	0
Output Packet Queue Length :	0

Dial Out Details (Modify Login, Attempts and Maximum Time)

From this screen you can modify Login, connection Attempt information, and Maximum Time objects for dial out connections from the 2800 (see Figure A-18, below). To reach this screen, select Modify from the Dial Out Details screen.

Figure A-18. Dial Out - Details (Modify Login, Attempts, Maximum Time Objects)



DIAL OUT

Login

TCP Port: 24
Restrict To Lan: disable(1)
Login Technique: text(2)
Username Prompt: Username:
Password Prompt: Password:
Initial Banner:

Attempts

Failure Banner: fail
Login Attempts Allowed: 3

Maximum Time *(0 = eternal)*

Maximum Session Time (min): 0
Maximum Idle Time (min): 15
Time to login (sec): 60
Call history timeout (min): 60

Total Active Calls (doActive) The total number of active calls.

Login

Use this section to configure the outgoing TCP port and general login information.

TCP Port (doTcpPort) The TCP port number which the dialout should listen on for connections.

Restrict to Lan (doRestrictToLan) Enabling the restriction to LAN will stop dialout attempts which originate at any port besides the LAN port.

disable(1),
enable(2)

Login Technique (doLoginTechnique) This variable defines the login sequence that a dial-up user will see. The options are defined below:

none(1)	Simply connection to the TCP pipe allows dialout.
text(2)	A Username prompt is displayed and a username must be entered. If the received username is a static user with no password defined then the connection completes and no password prompt. Otherwise a password prompt is displayed and a password must be entered.

Username Prompt (doUsernamePrompt) This defines the character string that will be displayed at user authentication time to request the users name. This should be a ASCII printable string and can include carriage returns and line feeds.

Password Prompt (doPasswordPrompt) This defines the character string that will be displayed at user authentication time to request the users password. This should be a ASCII printable string and can include carriage returns and line feeds.

Initial Banner (doBanner) A string to initially display for the user.

Attempts

Use this section to configure the maximum number of login attempts and the authentication failure banner.

Failure Banner (doFailureBanner) This defines a message that will be displayed to a user when authentication failed. This is only relevant when the authentication technique was Text.

Login Attempts Allowed (doAllowAttempts) The maximum number of attempts a user will be given to login before being disconnected. This applies to Text authentications only. PAP and CHAP authentications are only allowed a single attempt.

Maximum Time

Maximum Session Time (doSessionTimeout) This is the maximum time in minutes which a connection is allowed to be maintained. After this time the connection will be terminated, even if there is active traffic on the connection. This is a default setting which may be overridden by the authentication of a specific user.

Maximum Idle Time (doIdleTimeout) This is the maximum time in minutes which a connection is allowed to be maintained with no traffic. After this time, if no traffic is seen, the connection will be terminated. This is a default setting which may be overridden by the authentication of a specific user.

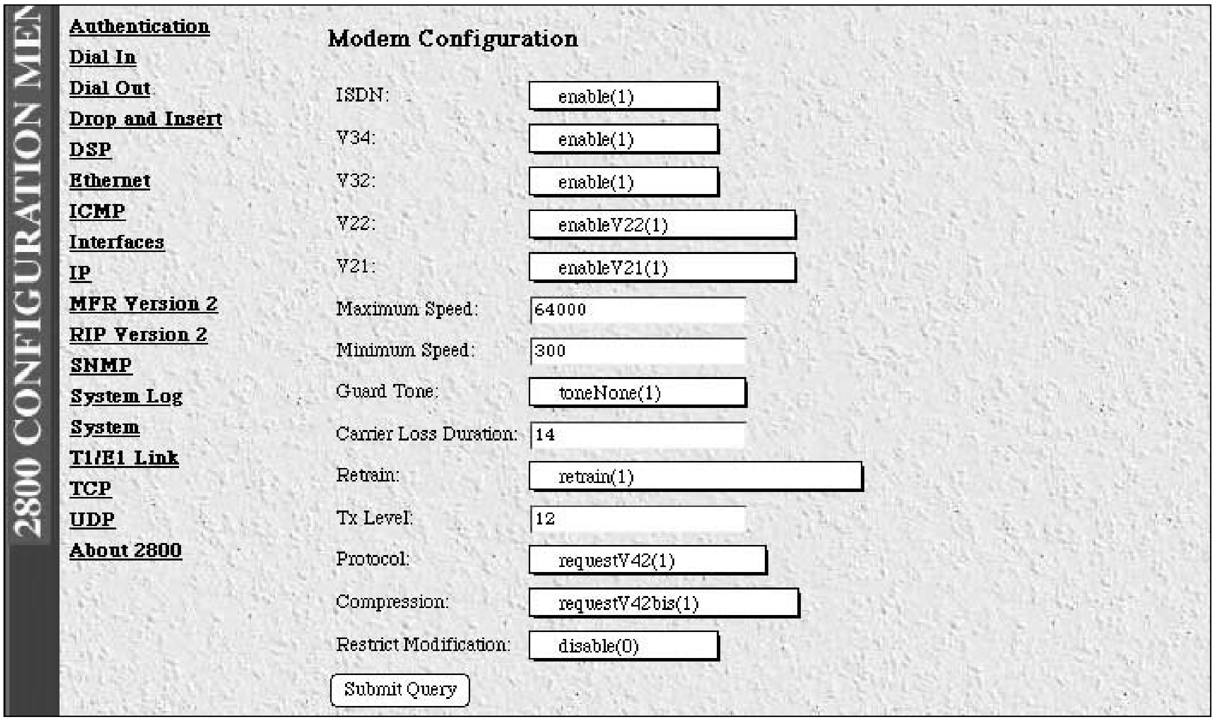
Time to Login (sec) (doLoginTimeout) This is the maximum time in seconds which a user is given to login. This is only relevant before the user is authenticated. This setting should take into account any time required to query a remote authentication server
(ie. RADIUS)**.**

Call history timeout (min) (doLingerTime) Number of seconds a MIB entry in the Active table will remain after the call is dead.

Dial Out Details (Modify Modem Configuration)

From this screen you can modify the outgoing Modem Configuration (see Figure A-19, below). To reach this screen, select Modify from the main Dial Out Details screen.

Figure A-19. Dial Out - Details (Modify Modem Configuration)



Modem Configuration

ISDN:	enable(1)
V34:	enable(1)
V32:	enable(1)
V22:	enableV22(1)
V21:	enableV21(1)
Maximum Speed:	64000
Minimum Speed:	300
Guard Tone:	toneNone(1)
Carrier Loss Duration:	14
Retrain:	retrain(1)
Tx Level:	12
Protocol:	requestV42(1)
Compression:	requestV42bis(1)
Restrict Modification:	disable(0)

Modem Configuration

Use this section to configure the outgoing modem configuration.

ISDN (doModemISDNEnable) Allow V34 and V34 annex 12 modulations

disable(0),
enable(1)

V34 (doModemV34Enable) Allow V34 and V34 annex 12 modulations

disable(0),
enable(1)

V32 (doModemV32Enable) Allow V32 and V32bis modulations

disable(0),
enable(1)

V22 (doModemV22Enable) Allow V22 or Bell 212 modulations

disable(0),
enableV22(1),
enableBell212(2)

V21 (doModemV21Enable) Allow V21 or Bell 103 modulations

disable(0),
enableV21(1),
enableBell103(2)

Maximum Speed (doModemMaxSpeed) This variable allows the selection of the fastest data rate that will be negotiated.

Minimum Speed (doModemMinSpeed) This variable allows the selection of the slowest data rate that will be negotiated.

Guard Tone (doModemGuardTone) Normally a guard tone is not required. But, one can be inserted. This operates for Phase Shift Key modulations only.

toneNone(1),
tone1800(3)

Carrier Loss Duration (doModemCarrierLossDuration) The number of seconds the carrier must be lost before it is considered the connection dead. A setting above 100 indicates forever.

Retrain (doModemRetrain) Allow the modem to monitor the line quality and request a fallback or retrain for poor quality and a fallforward for good quality.

none(0),
retrain(1),
fallForwardFallBack(2)

Tx Level (doModemTxLevel) This variable should be set with caution; and normally only after talking to a factory representative. This sets the transmit level power level of the modem. The scale is 0 (0 dB) to 15 (-15 dB). Note that larger numbers mean less power.

Protocol (doModemProtocol) Selection of the data protocol to use on the modem. This allows the request of or forcing of V42 error correction protocol.

direct(0),
requestV42(1),
requireV42(2)

Compression (doModemCompression) Selection of the data compression protocol to use on the modem. This allows the request of or forcing of V42 compression protocol. This will only be used if V42 error correction is active.

direct(0),
requestV42bis(1),
requireV42bis(2)

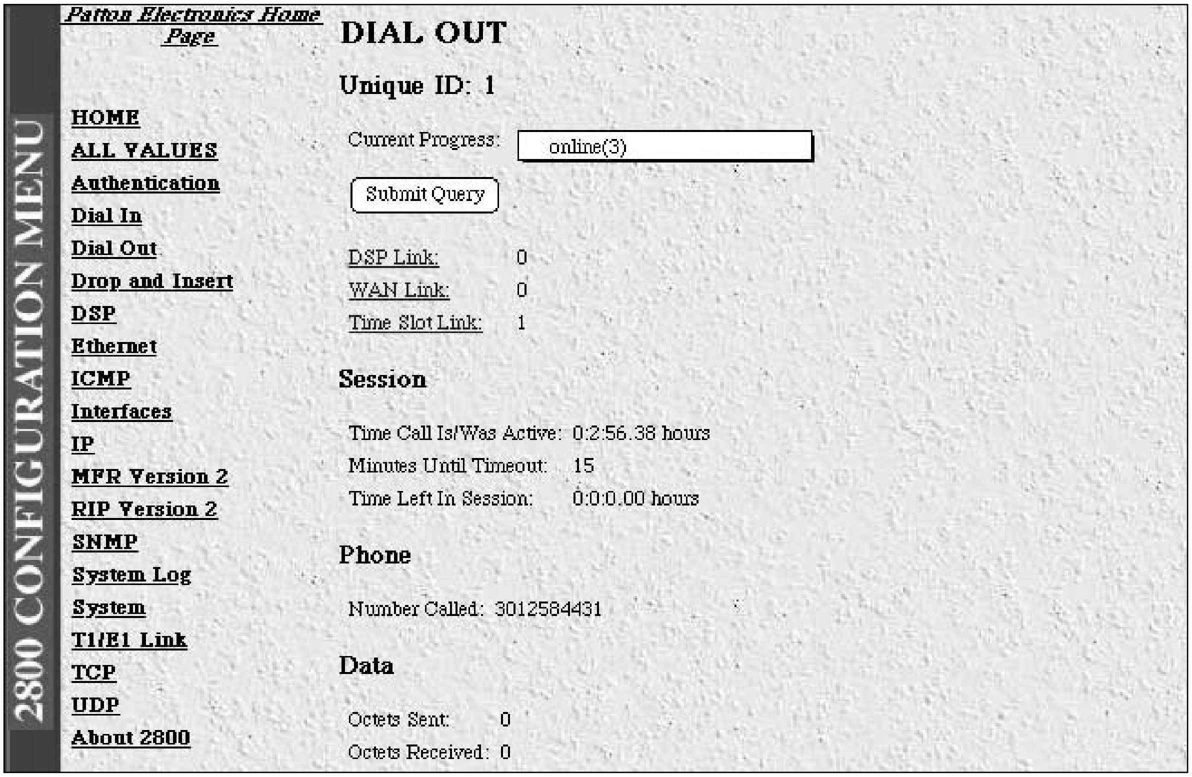
Restrict Modification (doModemRestrictMods) Enabling this feature will restrict the dialout user from modifying the modem settings. Normally the dialout user has the ability to alter the desired modem operation through the use of AT commands.

disable(0),
enable(1)

User Statistics (Unique ID, Session, Phone, Data)

This screen shows statistics for individual dial out users. To view individual user statistics, select an active user under the User heading on the main Dial Out screen (user statistics are only available for currently connected users. If there are no current Dial Out users, the screen will be blank. Figure A-20, below, shows user information for a Unique ID. The hyperlink headings DSP Link, WAN Link, and Time Slice Link shown below point to the DSP, Link and Fractional tables for a unique time slot defined on each of these links. For specific details on the function of parameters defined under these sections, refer to each under the 2800 Configuration Menu.

Figure A-20. Dial Out - Details (Unique ID, Session, Phone, Data)



DIAL OUT

Unique ID: 1

Current Progress: online(3)

DSP Link: 0
WAN Link: 0
Time Slot Link: 1

Session

Time Call Is/Was Active: 0:2:56.38 hours
Minutes Until Timeout: 15
Time Left In Session: 0:0:0.00 hours

Phone

Number Called: 3012584431

Data

Octets Sent: 0
Octets Received: 0

Current Progress (doactState) Indicates current progress.

> **authenticating(0),**
> **commandmode(1),**
> **connecting(2),**
> **online(3),**
> **dead(4),**
> **kill(5)**

DSP Link (doactDSPIndex) Which DSP chip this call is on (points to DSP table).

WAN Link (doactLinkIndex) Which WAN link this call is on (points to the Link table).

Time Slot Index (doactSlotIndex) Which time slot this call is on (points to the Fractional table).

Session

This is section contains activity time for the current or most recent session.

Time Call Is/Wan Active (doactSessionTime) The number of seconds this call was/is active.

Minutes Until Timeout (doactRemainingIdle) Number of minutes until idle timeout (counts down).

Time Left In Session (doactRemainingSession) Number of seconds left in this session (counts down).

Phone

Number Called (doactNumberDialed) The phone number that was dialed into.

Data

This section contains session octet information.

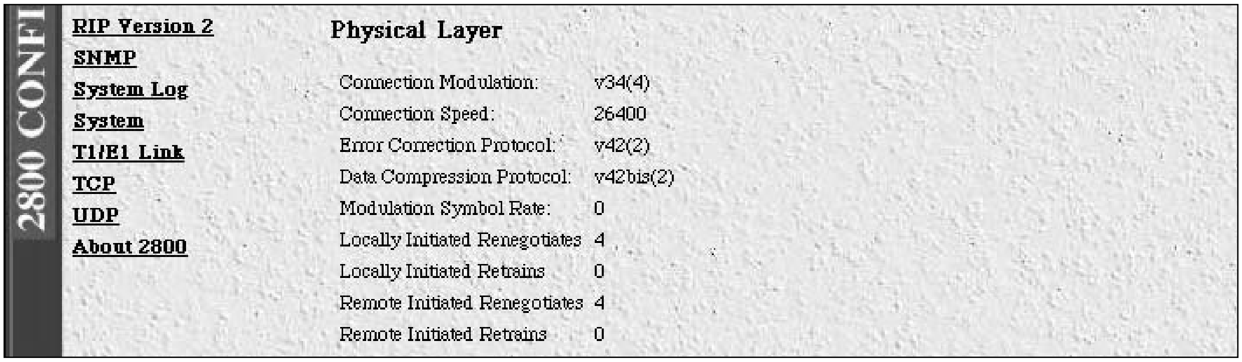
Octets Sent (doactSentOctets) The number of octets sent on this call.

Octets Received (doactReceivedOctets) The number of octets received on this call.

User Statistics (Physical Layer)

Figure A-21, below, shows Physical Layer connection information for a dial out connection. To reach this screen, scroll down from the previous screen.

Figure A-21. Dial Out - Details (Physical Layer)



Physical Layer

Connection Modulation:	v34(4)
Connection Speed:	26400
Error Correction Protocol:	v42(2)
Data Compression Protocol:	v42bis(2)
Modulation Symbol Rate:	0
Locally Initiated Renegotiates	4
Locally Initiated Retrains	0
Remote Initiated Renegotiates	4
Remote Initiated Retrains	0

Physical Layer

Connection Modulation (doactModulation) The modulation of the link.

unknown(0),
v21(1),
v22(2),
v32(3),
v34(4),
k56(5),
x2(6),
vpcm(7),
v110(8),
isdn64(9),
isdn56(10)

Connection Speed (doactSpeed) The connected speed of the link.

Error Correction Protocol (doactErrorCorrection) The error correction scheme used on this call.

unknown(0),
none(1),
v42(2),
mnp(3),
v120(4),
cellular(5),
hdlc(6)

Data Compression Protocol (doactCompression) The compression technique used on this call.

unknown(0),
none(1),
v42bis(2),
mnp5(3),
stac(4)

Modulation Symbol Rate (doactSymbolRate) The symbol rate of the call (modem only).

Locally Initiated Renegotiates (doactLocalRenegotiates) The number of times the local side (this unit) has initiated a modem speed renegotiate.

Locally Initiated Retrains (doactLocalRetrains) The number of times the local side (this unit) has initiated a modem carrier retrain.

Remote Initiated Renegotiates (doactRemoteRenegotiates) The number of times the far modem has initiated a modem speed renegotiate.

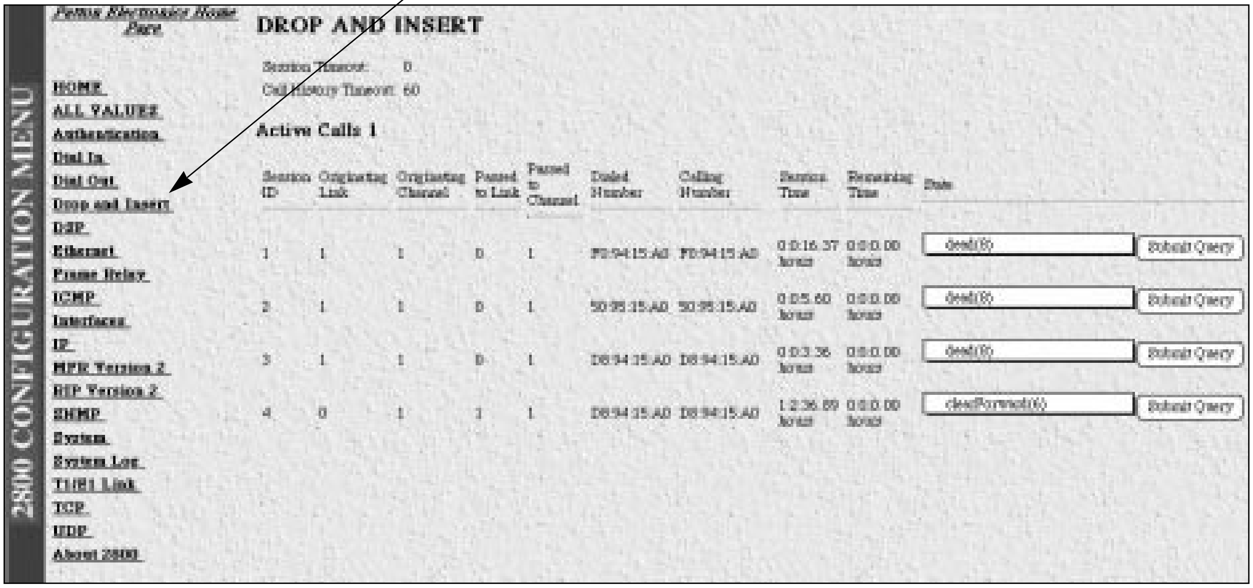
Remote Initiated Retrains (doactRemoteRetrains) The number of times the far modem has initiated a modem carrier retrain.

Drop and Insert

The Drop and Insert contains setup objects associated with using the 2800 as a drop and insert box to an upstream or downstream location. This section contains channel information for each unique session ID. If there are no drop and insert connections to the 2800, this screen will be blank.

To reach the dial out Section, select Drop and Insert. from the 2800 Configuration Menu. (see Figure A-22, below). Following Figure A-22 are descriptions for each object on this page.

Figure A-22. Drop and Insert Main Screen



DROP AND INSERT

Session Timeout: 0
Call History Timeout: 60

Active Calls 1

Session ID	Originating Link	Originating Channel	Passed to Link	Passed to Channel	Dialed Number	Calling Number	Session Time	Remaining Time	State
1	1	1	0	1	F0:94:15:A0	F0:94:15:A0	0:0:16.37 hours	0:0:0.00 hours	dead(8)
2	1	1	0	1	50:95:15:A0	50:95:15:A0	0:0:5.60 hours	0:0:0.00 hours	dead(8)
3	1	1	0	1	D8:94:15:A0	D8:94:15:A0	0:0:3.36 hours	0:0:0.00 hours	dead(8)
4	0	1	1	1	D8:94:15:A0	D8:94:15:A0	1:2:36.89 hours	0:0:0.00 hours	clearForward(6)

Session Timeout (drSessionTimeout) This is the maximum time in minutes which a connection is allowed to be maintained. After this time the connection will be terminated, even if there is active traffic on the connection.

Call History Timeout (drLingerTime) Number of seconds a MIB entry in the Active table will remain after the call is dead.

Active Calls (drActive) The total number of active calls.

Session ID (dractIndex) Unique identification of this active call

Originating Link (dractLinkIndex) Which WAN link this call originated on.

Originating Channel (dractChannel) Which channel this call originated on.

Passed to Link (dractPassLinkIndex) Which link this call was passed to.

Passed to Channel (dractPassChannel) Which channel this call was passed to.

Number Dialed (dractNumberDialed) The phone number that was dialed into.

Calling Number (dractCallingPhone) The phone number that was dialed from.

Session Time (dractSessionTime) The number of seconds this call was/is active.

Remaining Time (dractRemainingSession) Number of seconds left in this session (counts down).

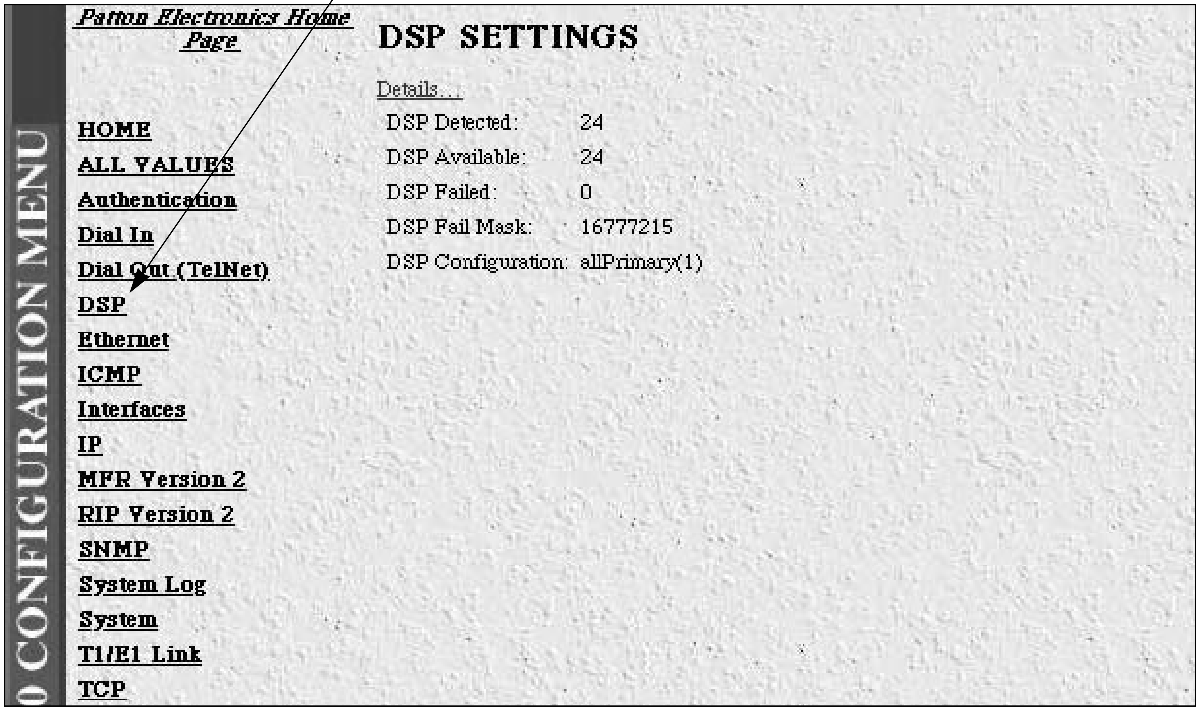
State (dractState) Indicates current progress.

setup(1),
alerting(2),
flash(3),
online(4),
sessiontime(5),
clearForward(6),
clearBackward(7),
dead(8),
kill(9)

DSP (Digital Signal Processing)

The 2800 uses between twelve and thirty DSPs (Digital Signal Processors) to pass digital information without translating that information between analog and digital signals. Digital signal processing makes special performance demands which distinguish DSP architectures from other microprocessor and microcontroller architectures. Select DSP from the Configuration Menu to monitor the five variables which describe the current state of the DSP's (see Figure A-23, below). Following Figure A-23 are descriptions for each variable on this page.

Figure A-23. DSP (Digital Signal Processing) Main Screen



DSP SETTINGS

Details...

```
DSP Detected:       24
DSP Available:      24
DSP Failed:         0
DSP Fail Mask:      16777215
DSP Configuration:  allPrimary(1)
```

DSP Detected (dspDetected) Indicates the number of DSP's the PAR-1 has detected as installed at time of boot up

DSP Available (dspAvailable) Indicates the number of DSP's available for operation

DSP Failed (dspFailed) Indicates the number of DSP's taken out of the DSP resource pool.

DSP Fail Mask (dspFailMask) A bit mask which Identifies which DSP's are working

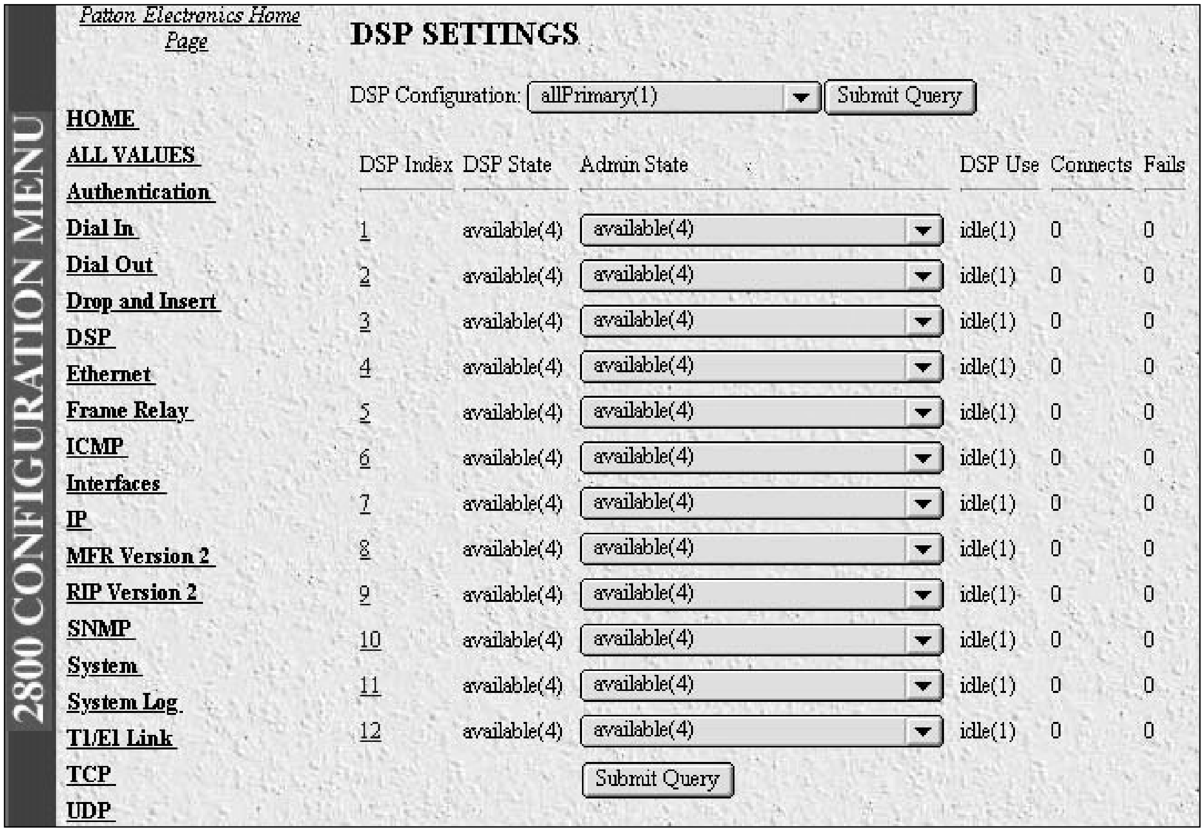
DSP Configuration (dspConfiguration) Tells the PAR-1 how the DSP resource pool is allocated between the two T1/E1/PRI ports.

Select Details to modify the DSP Settings

DSP Settings

When you select Detail, the monitor will display the DSP Settings page. This screen shows the status of all DSP's (See Figure A-24, below). The SNMP variable for this table are referenced through the **DSP Index (dspIndex)** variable.

Figure A-24. DSP Settings



DSP SETTINGS

DSP Configuration: allPrimary(1)

DSP Index	DSP State	Admin State	DSP Use	Connects	Fails
1	available(4)	available(4)	idle(1)	0	0
2	available(4)	available(4)	idle(1)	0	0
3	available(4)	available(4)	idle(1)	0	0
4	available(4)	available(4)	idle(1)	0	0
5	available(4)	available(4)	idle(1)	0	0
6	available(4)	available(4)	idle(1)	0	0
7	available(4)	available(4)	idle(1)	0	0
8	available(4)	available(4)	idle(1)	0	0
9	available(4)	available(4)	idle(1)	0	0
10	available(4)	available(4)	idle(1)	0	0
11	available(4)	available(4)	idle(1)	0	0
12	available(4)	available(4)	idle(1)	0	0

DSP Configuration (dspConfiguration) Tells the PAR-1 how the DSP resource pool is allocated between the two T1/E1/PRI ports. Select from:

allPrimary(1) = All of the DSP's are attached to Line A

split(2) = 1/2 of the DSP's are attached to Line A and 1/2 of the DSP's are attached to Line B

dropAddInsert(3) = Feature not available

NOTE: If you only have one T1/E1/PRI connection, then the DSP configuration should be set to **allPrimary(1)**.

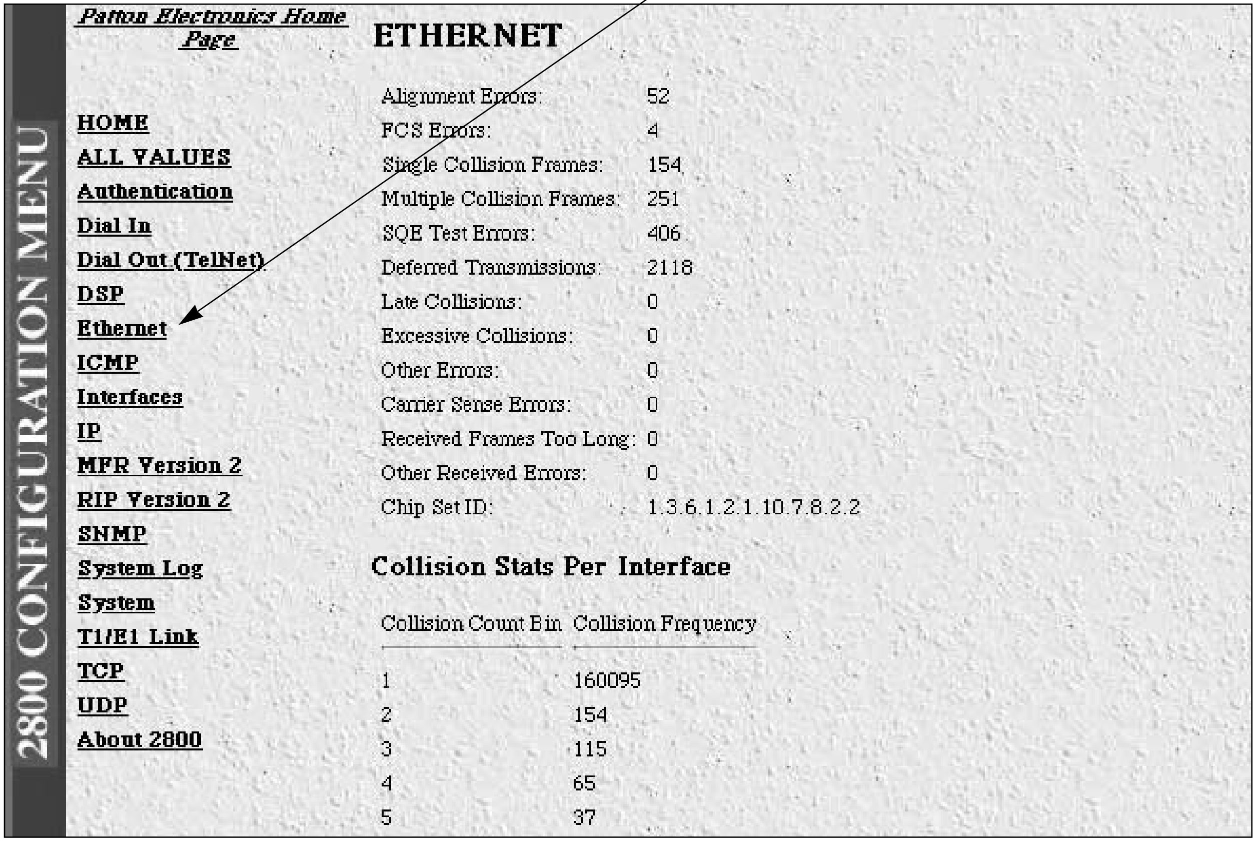
DSP Index (dspIndex)	Identifies the DSP we are reporting on.
DSP State (dspState)	Identifies the state of the DSP. Select from:
usable(1) =	The DSP is available
inuse(2) =	The DSP has been allocated to a process
unusable(3) =	The DSP has been taken out of service
DSP Use (dspUse)	This variable identifies the current stae that the DSP is in. Select from:
idle(1) =	The DSP is idle and awainting allocation
dialin(2) =	The DSP is processing a dial-in call
dialout(3) =	The DSP is processing a dial-out call
framerelay(4) =	The DSP is allocated to frame relay processing (future option)
fracPPP(5) =	The DSP is allocated to PPP procssing on the WAN link
signalling(6) =	The DSP is being used to process WAN link signalling

DSP Call Index(dspCallIndex) This is the pointer to the connection identifer. Every connection has an internal number which identifies the connection throughout the box. This number is identifes that connection.

Ethernet

The 2800 provides management and statistical information on the Ethernet interface. Detailed information regarding the SNMP MIB II variables may be downloaded from **RFC 1643, Definitions of Managed Objects for the Ethernet-like Interface Types**. Select Ethernet from the Configuration Menu to monitor Ethernet statistics. Following Figure A-25 are descriptions for each variable on this page.

Figure A-25. Ethernet Main Screen



ETHERNET

Alignment Errors:	52
FCS Errors:	4
Single Collision Frames:	154
Multiple Collision Frames:	251
SQE Test Errors:	406
Deferred Transmissions:	2118
Late Collisions:	0
Excessive Collisions:	0
Other Errors:	0
Carrier Sense Errors:	0
Received Frames Too Long:	0
Other Received Errors:	0
Chip Set ID:	1.3.6.1.2.1.10.7.8.2.2

Collision Stats Per Interface

Collision Count Bin	Collision Frequency
1	160095
2	154
3	115
4	65
5	37

Alignment Items (dot3StatsAlignmentErrors) The number of frames received that are not an integral number of octets in length and do not pass the FCS check.

FCS Errors (dot3StatsFCSErrors) The number of frames received that are an integral number of octets in length but do not pass the FCS check.

Single Collision Frames (dot3StatsSingleCollision Frames) The number of successfully transmitted frames in which there was exactly one collision.

Multiple Collision Frames (dot3StatsMultipleCollisionFrames) The number of successfully transmitted frames in which there was more than one collision.

SQE Test Errors (dot3StatsSQETestErrors) The number of times that the SQE TEST ERROR message is generated by the PLS sublayer.

Deferred Transmissions (dot3StatsDeferredTransmissions) The number of times in which the first transmission attempt is delayed because the medium is busy. This number does not include frames involved in collisions.

Late Collisions (dot3StatsLateCollisions) The number of times that a collision is detected later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbps system.

Excessive Collisions (dot3StatsExcessiveCollisions) The number of frames in which transmission failed due to excessive collisions.

Other Errors (dot3StatsInternalMacTransmitErrors) The number of frames transmission on a fails due to an internal MAC sublayer transmit error.

Carrier Sense Errors (dot3StatsCarrierSenseErrors) The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.

Received Frames Too Long (dot3StatsFrameTooLongs) The number of frames received that exceed the maximum permitted frame size.

Other Received Errors (dot3StatsInternalMacReceiveErrors) The number of frames in which reception fails due to an internal MAC sublayer receive error.

Chip Set ID (dot3StatsEtherChipSet) Identifies the chipset used to realize the interface by using an OBJECT IDENTIFIER. Ethernet-like interfaces are typically built out of several different chips. This chip set gathers the transmit and receive statistics and error indications.

Collision Stats Per Interface (dot3StatsIndex) An index value that uniquely identifies an interface to an ethernet-like medium. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

Collision Count (dot3CollCount) The number of collisions on reported in the histogram cell.

Collision Frequency (dot3CollFrequencies) The number of individual MAC frames in which the successful or unsuccessful transmission occurs after the frame has experienced the number of collisions in dot3CollCount.

Frame Relay

The Frame Relay Section is:

This Page Intentionally Blank

This Page Intentionally Blank

This Page Intentionally Blank

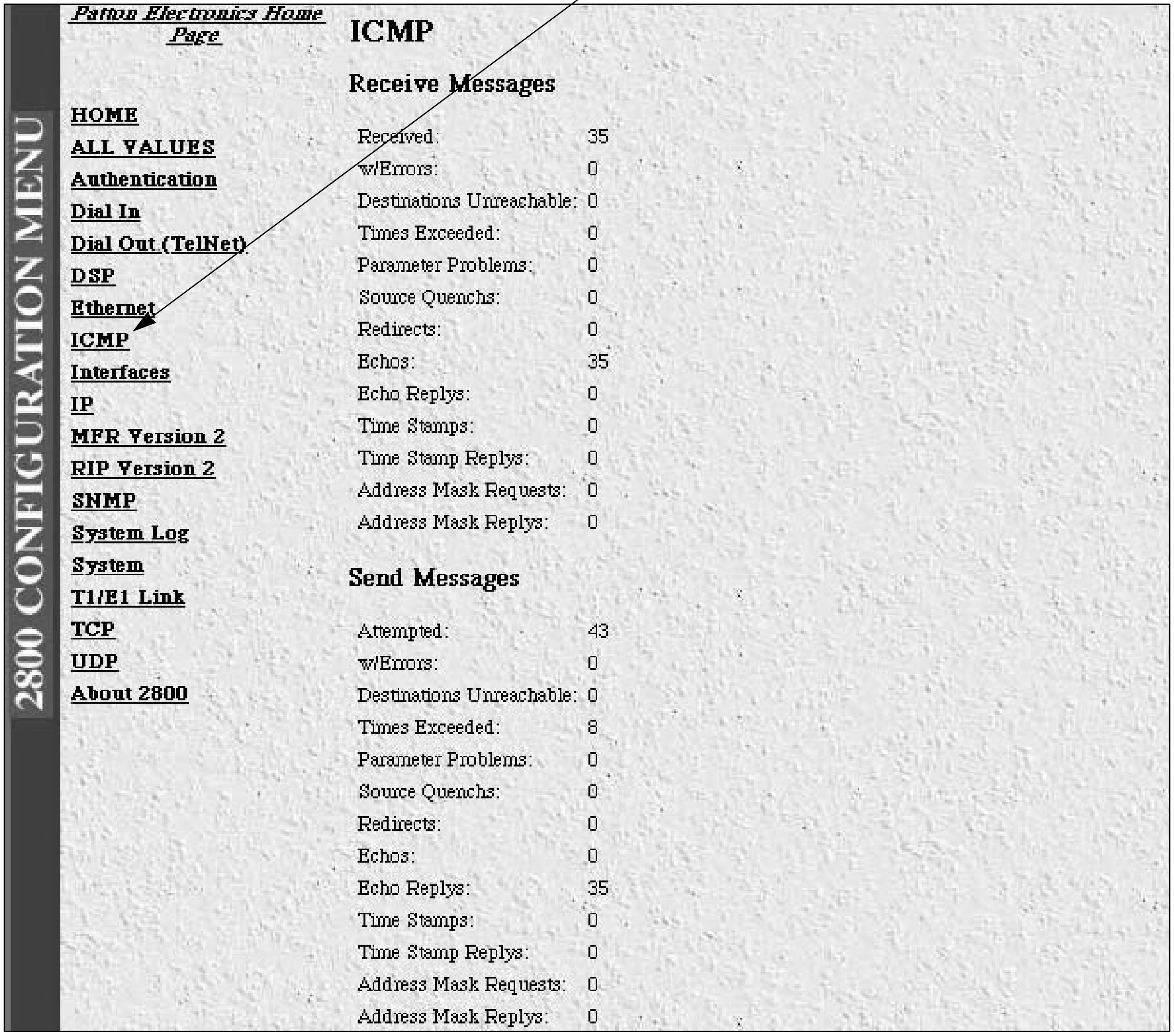
This Page Intentionally Blank

This Page Left Intentionally Blank

ICMP

Under normal circumstances, IP makes very efficient use of system resources. However errors, congestion and system malfunctions occur periodically. ICMP (Internet Control Message Protocol) assists network managers with IP routing by sending control and error reporting messages between IP hosts. The statistics listed on the 2800 ICMP page correspond directly to ICMP statistics listed in *RFC 792 - Internet Control Message Protocol (ICMP)*. Implementation of the ICMP group is mandatory for all TCP/IP networks. To monitor the 2800 ICMP parameters, select ICMP from the 2800 Configuration Menu (see Figure A-30, below). Following Figure A-30 are descriptions for each variable on this page.

Figure A-30. ICMP Main Screen



ICMP

Receive Messages

Received:	35
w/Errors:	0
Destinations Unreachable:	0
Times Exceeded:	0
Parameter Problems:	0
Source Quenchs:	0
Redirects:	0
Echos:	35
Echo Replys:	0
Time Stamps:	0
Time Stamp Replys:	0
Address Mask Requests:	0
Address Mask Replys:	0

Send Messages

Attempted:	43
w/Errors:	0
Destinations Unreachable:	0
Times Exceeded:	8
Parameter Problems:	0
Source Quenchs:	0
Redirects:	0
Echos:	0
Echo Replys:	35
Time Stamps:	0
Time Stamp Replys:	0
Address Mask Requests:	0
Address Mask Replys:	0

The ICMP link on the 2800 displays the ICMP message counters. ICMP messages, as displayed by the 2800, are broken down into two types of messages:

1. Messages received by the 2800 **(InMibVariable)**
2. Messages sent by the 2800 **(OutMibVariable)** .

Example:
Parameter (InMibVariable, OutMibVariable)

The numbers following the parameters can be a good source of what is happening on the network to point out potential problems. Both gateways (routers) and hosts may send ICMP messages.

ICMP Receive/Send Messages

Received (icmpInMsgs) The number of ICMP messages the 2800 has received. This number also includes ICMP messages received/sent which have ICMP specific errors.

Attempted (icmpOutMsgs) The number of ICMP messages the 2800 has attempted to send out. This number also includes any internal ICMP packet errors.

w/Errors (icmpInErrors, icmpOutErrors) The number of ICMP messages which the 2800 has received/sent but are deemed to be faulty (e.g. bad ICMP checksums, bad length, Non-routable, etc...)

Destinations Unreachable (IcmpInDestUnreachs, IcmpOutDestUnreachs) The number of ICMP destination unreachable messages received/sent. For instance, if the information in a gateway’s routing table determine that the network specified in a packet is unreachable, the gateway will send back an ICMP message stating that the network is unreachable. The following five conditions will send back an unreachable message:

1. The network is unreachable;
2. The host is unreachable;
3. The protocol is not available to the network;
4. The port on the host is unavailable. a specified source route failed;
5. A packet must be fragmented (i.e. broken up into two or more packets) but the packet was sent with instructions *NOT* to be fragmented.

Times Exceeded (icmpInTimeExcds, icmpOutTimeExcds) The number of ICMP Time Exceeded messages received/sent. Each time a packet passes through a gateway, that gateway reduces the Time-To-Live (TTL) field by one. The default starting number is defined under the IP section. If the gateway processing a packet finds that the TTL field is zero it will discard the packet and send the ICMP Time Exceeded Message. Time Exceeded will also be incremented when a host which is reassembling a framented packet cannot complete the reassembly due to missing packets within its time limit. In this case, ICMP will discard the packet and send the Time Exceeded message.

Parameter Problems (icmpInParmProbs, icmpOutParmProbs) The number of ICMP Parameter Problem messages received/sent. If while processing a packet, a gateway or host finds a problem with one or more of the IP header parameters which progibits further processing, the gatway or host will discard the packet and return an ICMP Paramenter Problem message. One potential source of this problem may be with incorrect or invalid arguments in an option. ICMP sends the Paramenter Problems message if the gateway or host has discarded the whole packet.

Source Quenchs (icmpInSrcQuenchs, icmpOutSrcQuenchs) The number of ICMP Source Quench messages received/sent. A gateway will discard packets if cannot allocate the resources, such as buffer space, to process the packet. If a gateway discards the packet, it will send an ICMP Source Quench message back to the sending device. A host may send this messages if packets arrive too fast to be processed or if there is network congestion. The Source Quench message is a request to reduce the rate at which it is sending traffic. If the 2800 receives a Source Quench, it will wait for acknowledgment of all outstanding packets before sending more packets to the remote destination. Then it will begin sending out packets at an increasing rate until the connection is restored to standard operating conditions.

Redirects (icmpInRedirects, icmpOutRedirects) The number of ICMP Redirect messages received/sent. A gateway sends a redirect message to a host if the network gateways find a shorter route to the destination through another gateway.

Echos (icmpInEchos, icmpOutEchos) The number of ICMP Echo Request messages received/send. The ICMP Echo is used whenever one uses the diagnostic PING tool. PING is used to test connectivity with a remote host by sending regular ICMP Echo commands and then waiting for a reply. Received **Echos (icmpInEchos)** will increment when the 2800 is PINGed.

Echo Replys (icmpInReps, icmpOutReps) The number of ICMP Echo Reply messages received/sent. An Echo Reply is a response to an Echo Request. Send Echos (icmpOutEchos) will increment when the 2800 is PINGed.

Time Stamps (icmpInTimestamps, icmpInTimestamps) The number of ICMP Timestamp messages received/sent. Time Stamp and Time Stamp Replys were originally designed into the ICMP facility to allow network clock synchronization. Subsequently, a new protocol -- Network Ttime Protocol (NTP) has been designed and implemented to perform this function. In normal conditions, this number will be zero.

Time Stamp Replys (icmpInTimestampsReps) (icmpOutTimestampsReps) The number of ICMP Timestamp Reply messages received/sent. This message is part of a Time Stamp (see above) request. In normal conditions, this number will be zero.

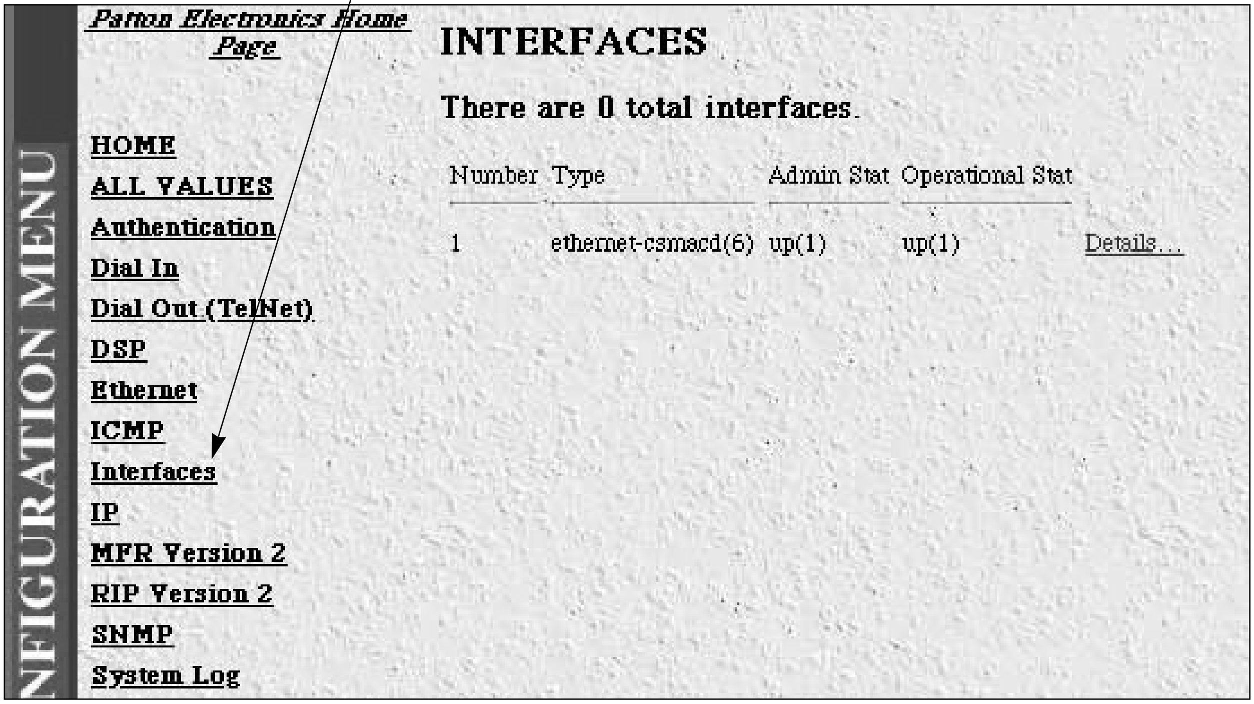
Address Mask Requests (icmpInAddrMasks) (icmpOutAddrMasks) The number of ICMP Address Mask Request messages received/sent. This message is generally used for diskless workstations which use this request at boot time to obtain their subnet mask. This number will increase if there are hosts on the network which broadcast these requests..

Address Mask Replys (icmpInAddrMasksReps) (icmpOutAddrMasksReps) The number of ICMP Address Mask Reply messages received/sent. In normal conditions, this number will be zero.

Interfaces

The Interfaces screen shows the quantity of incoming and outgoing traffic, as well as errors that cause frames to be discarded for each of the local interfaces. The statistics listed on the 2800 Interfaces page correspond directly to statistics listed in RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II. Frames are counted when theU arrive on the network. Some frames are then discarded during error screening. The remaining frames are delivered to the appropriate higher layer or sublayer. Implementation of the Interfaces group is mandatory for all systems. To monitor the Interfaces page, select Interfaces from the 2800 Configuration Menu (see Figure A-31). Following Figure A-31 are descriptions for each variable on this page.

Figure A-31. Interfaces Main Screen



INTERFACES

There are 0 total interfaces.

Number	Type	Admin Stat	Operational Stat	
1	ethernet-csmacd(6)	up(1)	up(1)	Details...

There are **(ifNumber)** total interfaces The number of network interfaces (regardless of their current state) present on this system.

Number (ifIndex) A unique number for each interface that ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one re-initialization of the entity's network management system to the next re-initalization. *Many MIB tables refer back to the interfaces table. For example, there is an Ethernet table that counts error collision statistics. Each of this table's entries starts with the ifIndex value telling us which interface we are talking about. This enables us to look up the other generic information that we need to know about that interface.*

Type (ifType) The type of interface, distinguished according to the physical/link protocol(s) immediatly ‘below’ the network layer in the protocl stack. Valid interface options are:

other(1)
ethernet-csmacd(6),
iso88023-csmacd(7),
ds1(18)
e1(19),
basicISDN(20),
primaryISDN(21),
ppp(23),
softwareLoopback(24),
slip(28)
frame-relay(32)

Admin Stat (ifAdminStatus) The desired state of the interface.

up(1) = The selected interface is ready to pass frames.
down(2) = The selected interface is not ready to pass frames.
testing(3) = The selected interface is being tested. No opera tional frames may be passed in this mode.

Operational Status) The current operational state of the interface.

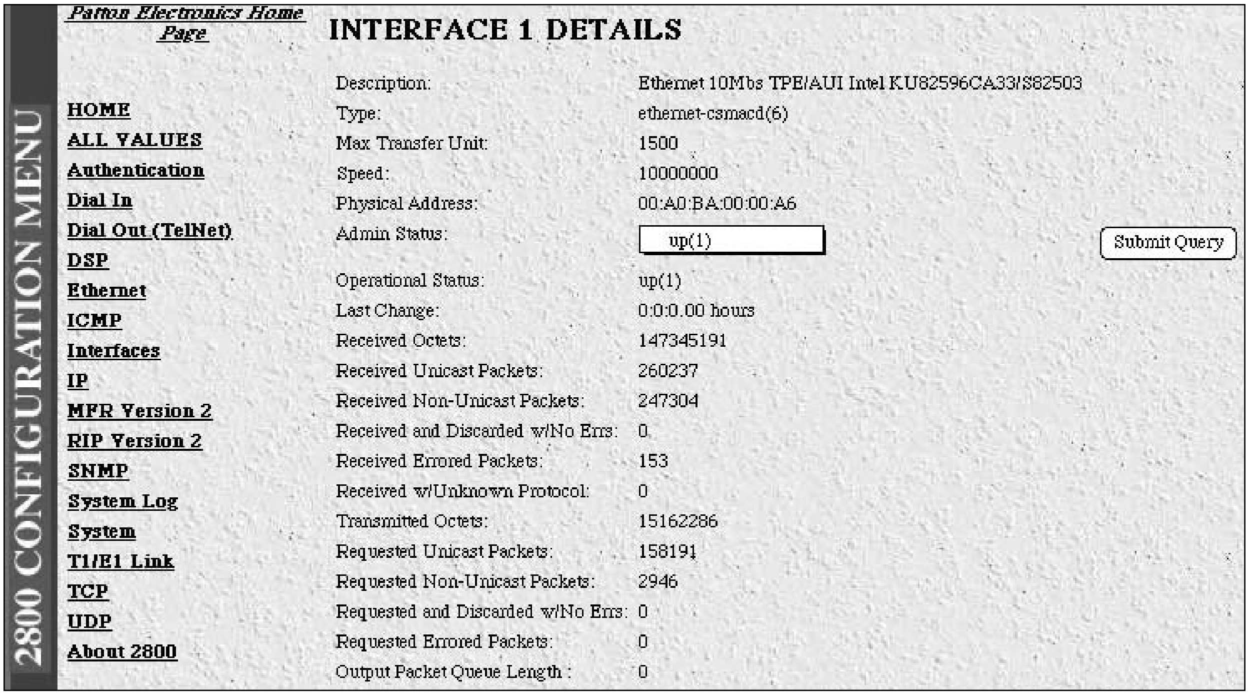
up(1) = The selected interface is ready to pass frames.
down(2) = The selected interface is not ready to pass frames.
testing(3) = The selected interface is being tested. No operational frames may be passed in this mode.

Select Details from the Interfaces Screen to monitor the status of the connected interfaces.

Interface Details

When you select Details from the Interfaces Screen, the monitor will display the type and description of the interface, speed, status, maximum size of Protocol Data Units (PDUs), and physical address as shown in Figure A-32, below. This page shows the status of all DSP's. The SNMP variable for this table are referenced through the SNMP MIB Interfaces Table. Following Figure A-32 are descriptions for each variable on this page.

Figure A-32. Interface Details



INTERFACE 1 DETAILS

Description:	Ethernet 10Mbs TPE/AUI Intel KU82596CA33/S82503
Type:	ethernet-csmacd(6)
Max Transfer Unit:	1500
Speed:	10000000
Physical Address:	00:A0:BA:00:00:A6
Admin Status:	up(1)
Operational Status:	up(1)
Last Change:	0:0:0.00 hours
Received Octets:	147345191
Received Unicast Packets:	260237
Received Non-Unicast Packets:	247304
Received and Discarded w/No Errs:	0
Received Errored Packets:	153
Received w/Unknown Protocol:	0
Transmitted Octets:	15162286
Requested Unicast Packets:	158191
Requested Non-Unicast Packets:	2946
Requested and Discarded w/No Errs:	0
Requested Errored Packets:	0
Output Packet Queue Length :	0

Description (ifDescr) A textual string containin information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface.

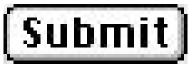
Max Transfer Unit (ifMTU) The size of the largest protocol data unit which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network protocol data units, this is the size of the largest network protocol data unit that can be sent on the interface.

Speed (ifSpeed) An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those in which no accurate estimation can be made, this object should contain the nominal bandwidth.

Admin Stat (ifAdminStatus) The desired state of the interface.

up(1) = The selected interface is ready to pass frames.
down(2) = The selected interface is not ready to pass frames.
testing(3) = The selected interface is being tested. No operational frames may be passed in this mode.

To change the Admin Stat of the 2800:

1) Select the desired Admin Stat mode
2) Select  to store the user information.

Operational Status (ifOperStatus) The current operational state of the interface.

up(1) The selected interface is ready to pass frames.
down(2) The selected interface is not ready to pass frames.
testing(3) The selected interface is being tested. No operational frames may be passed in this mode.

Last Change (ifLastChange) The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object will be zero.

Received Octets (ifInOctets) The number of octets received on the interface, including framing characters.

Received Unicast Packets (ifUcastPkts) The number of subnetwork-unicast packets delivered to a higher layer protocol.

Received Non-Unicast Packets (ifNUcastPkts) The number of non-unicast (i.e.,subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher layer protocol.

Received and Discarded w/No Errs (ifInDiscards) The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Received Errored Packets (ifInErrors) The number of inbound packets that contained errors preventing them from being deliverable to a higher layer protocol.

Received w/Unknown Protocol (ifInUnknownProtos) The number of packets received via the interface which were discared because of an unknown or unsupported protocol.

Transmitted Octets (ifOutOctets) The total number of octets transmitted out of the interface, including framing characters.

Requested Unicast Packets (ifOutUcastPkts) The total number of packets that higher level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Requested Non-Unicast Packets (ifOutNUcastPkts) The total number of packets that higher level protocols requested be transmitted to a non-unicast (i.e. a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.

Requested and Discarded w/No Errs (ifOutDiscards) The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

Requested Errored Packets (ifOutErrors) The number of outbound packets that could not be transmitted because of errors.

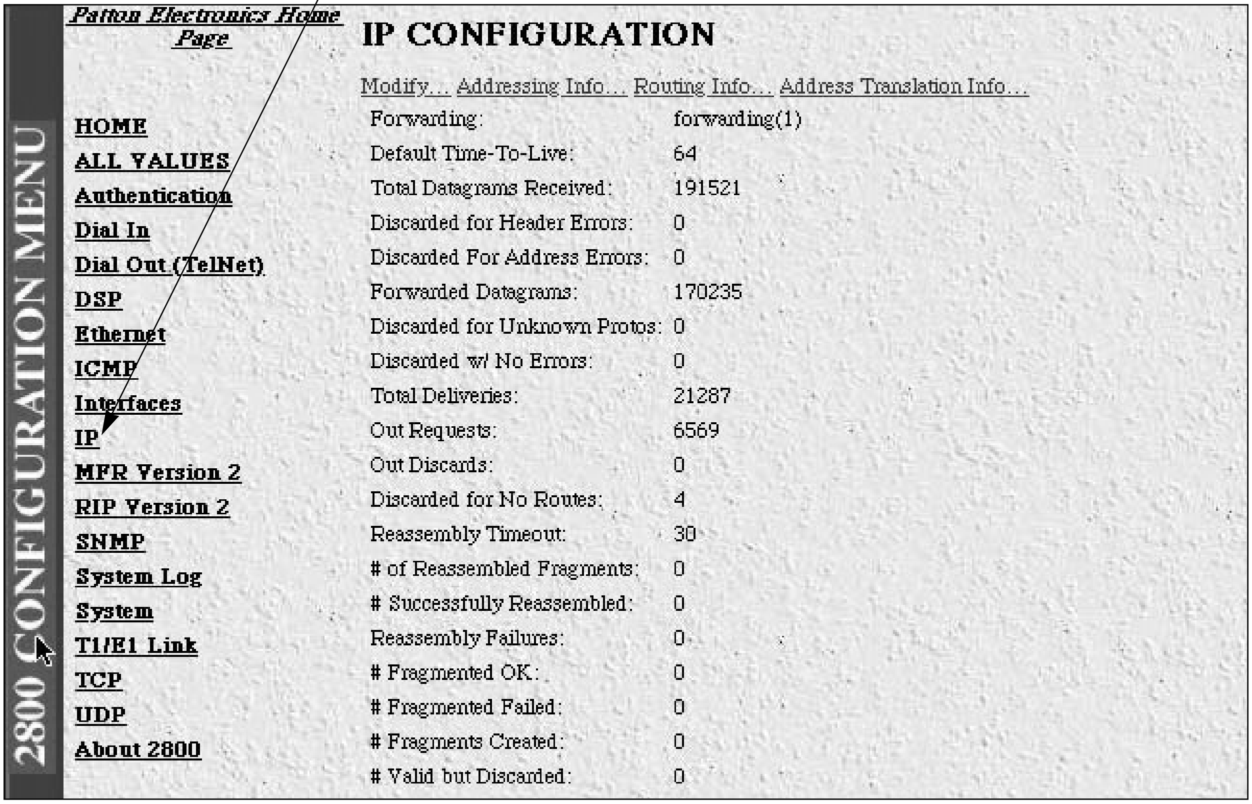
Output Packet Queue Length (ifOutQLen) The length of the output packet queue (in packets)

IP

The IP (Internet Protocol) section describes basic IP configuration parameters and statistics, IP Address Table information, IP Routing Table information, and Address Translation information. All object identifiers described in the section are described in *RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II.*

To reach the IP section, select IP from the 2800 Configuration Menu. (see Figure A-33, below). Following Figure A-33 are descriptions for each variable on this screen.

Figure A-33. IP Configuration Main Screen



IP CONFIGURATION

Forwarding:	forwarding(1)
Default Time-To-Live:	64
Total Datagrams Received:	191521
Discarded for Header Errors:	0
Discarded For Address Errors:	0
Forwarded Datagrams:	170235
Discarded for Unknown Protos:	0
Discarded w/ No Errors:	0
Total Deliveries:	21287
Out Requests:	6569
Out Discards:	0
Discarded for No Routes:	4
Reassembly Timeout:	30
# of Reassembled Fragments:	0
# Successfully Reassembled:	0
Reassembly Failures:	0
# Fragmented OK:	0
# Fragmented Failed:	0
# Fragments Created:	0
# Valid but Discarded:	0

Forwarding (ipForwarding) The indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host).

Note that for some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to change this object to an inappropriate value.

forwarding(1),	acting as a gateway
not-forwarding(2)	NOT acting as a gateway

Default Time-To-Live (ipDefaultTTL) The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol."

Total Datagrams Received (ipInReceives) The total number of input datagrams received from interfaces, including those received in error.

Discarded for Header Errors (ipInHdrErrors) The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc."

Discarded for Address Errors (ipInAddrErrors) The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address."

Forwarded Datagrams (ipForwDatagrams) The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.

Discarded for Unknown Protos (ipInUnknownProtos) The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Discarded w/No Errors (ipInDiscards) The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

Total Deliveries (ipInDelivers) The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

Out Requests (ipOutRequests) The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams."

Out Discards (ipOutDiscards) The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion."

Discarded for No Routes (ipOutNoRoutes) The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagarms which a host cannot route because all of its default gateways are down.

Reassembly Timeout (ipReasmTimeout) The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.

# of Reassembled Fragments (ipReasmReqds) The number of IP fragments received which needed to be reassembled at this entity.

# Successfully Reassembled (ipReasmOKs) The number of IP datagrams successfully reassembled.

Reassembly Failures (ipReasmFails) The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

# Fragmented OK (ipFragOKs) The number of IP datagrams that have been successfully fragmented at this entity.

# Fragmented Failed (ipFragFails) The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.

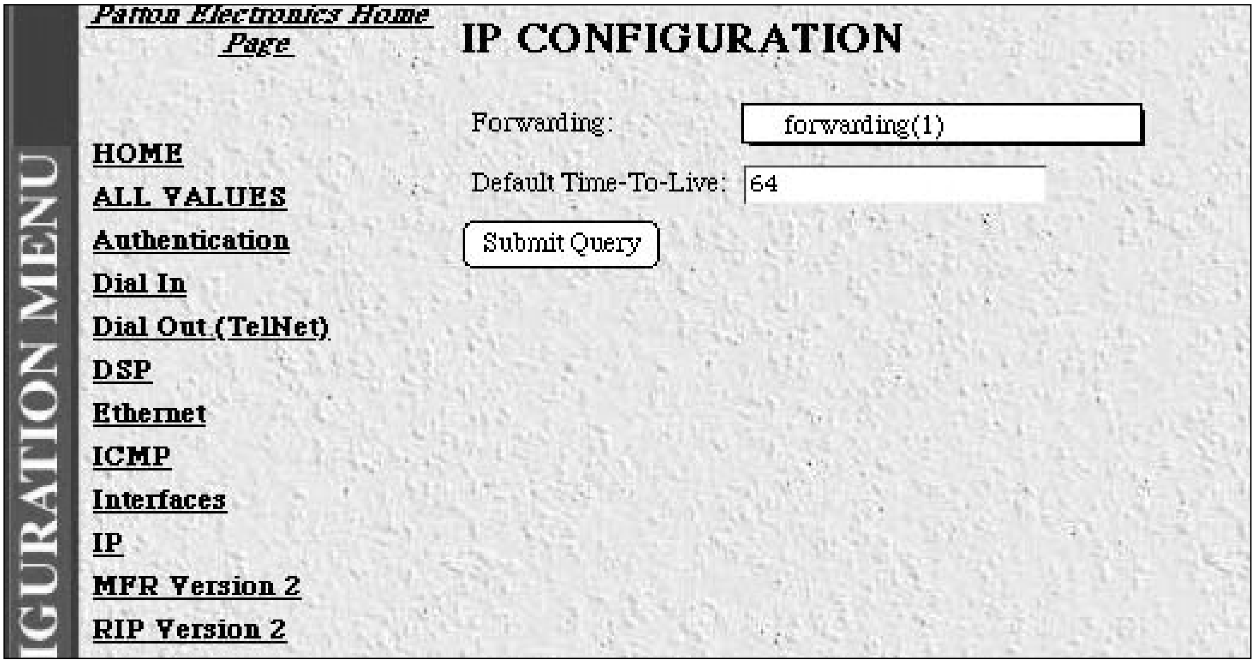
# Fragments Created (ipFragCreates) The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

# Valid but Discarded (ipRoutingDiscards) The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.

IP Configuration (Modify Forwarding and Time-To-Live)

IP Forwarding and Time-To-Live (Figure A-34, below) are basic read-write values that can be set on the HTTP/HTML screen or by a management application. To reach this screen, select Modify from the hypertext entries at the top of the main IP Configuration screen.

Figure A-34. IP Configuration - Modify Forwarding and Time-To-Live



IP CONFIGURATION

Forwarding: forwarding(1)

Default Time-To-Live: 64

Forwarding (ipForwarding) The indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host).

Note that for some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to change this object to an inappropriate value.

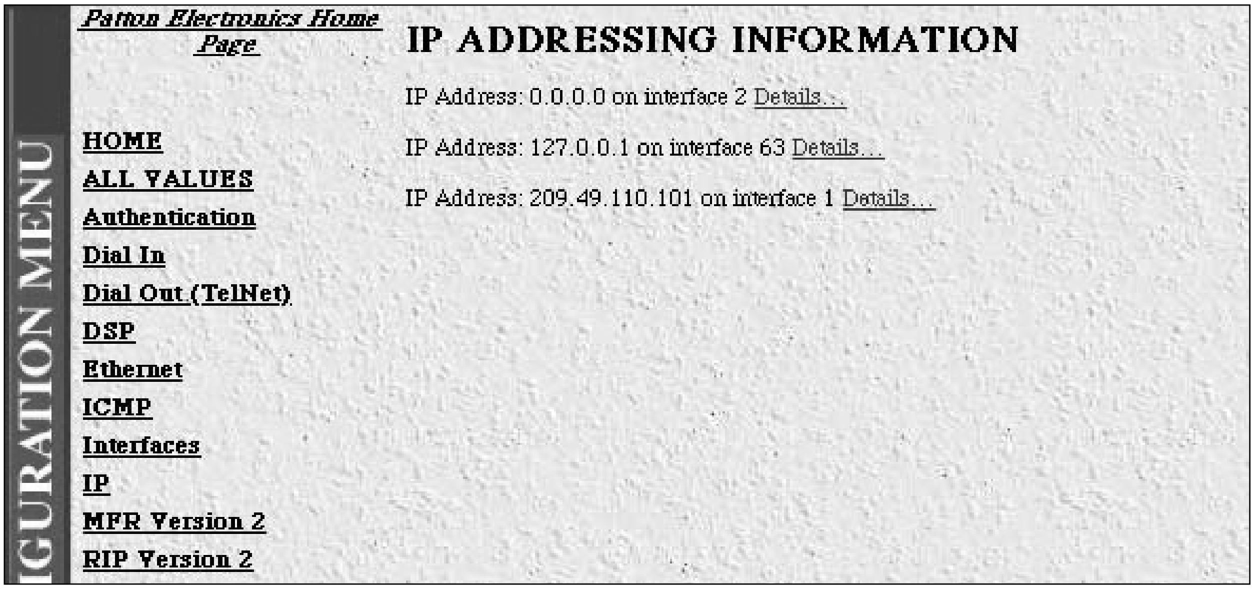
forwarding(1),	acting as a gateway
not-forwarding(2)	NOT acting as a gateway

Default Time-To-Live (ipDefaultTTL) The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.

IP Configuration (Addressing Information)

This section allows you to view IP addressing details for (1) the default address for outgoing IP datagrams; (2) the local or loopback address of the box; and, (3) the IP address of the box as defined in the System section (see Figure A-35, below). To reach this page, select Addressing Info... from the main IP Configuration screen.

Figure A-35. IP Configuration - Addressing Information



IP ADDRESSING INFORMATION

IP Address: 0.0.0.0 on interface 2 Details...

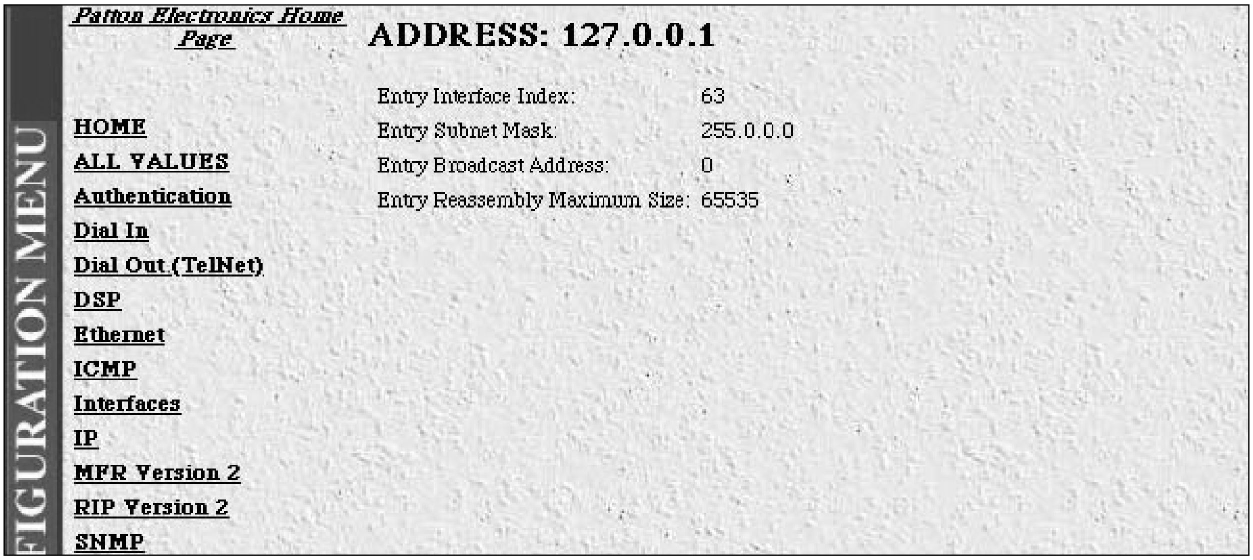
IP Address: 127.0.0.1 on interface 63 Details...

IP Address: 209.49.110.101 on interface 1 Details...

IP Configuration (Addressing Information Details)

This screen shows IP Address Table entries for each defined network interface (See Figure 3-36). The objects shown on this screen are described following Figure A-36. To reach this screen, select Details for one of the IP Addresses shown on the Addressing Information screen.

Figure A-36. IP Configuration - Addressing Information Details



ADDRESS: 127.0.0.1

Entry Interface Index:	63
Entry Subnet Mask:	255.0.0.0
Entry Broadcast Address:	0
Entry Reassembly Maximum Size:	65535

Entry Interface Index (ipAdEntIfIndex) The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

Entry Subnet Mask (ipAdEntNetMask) The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.

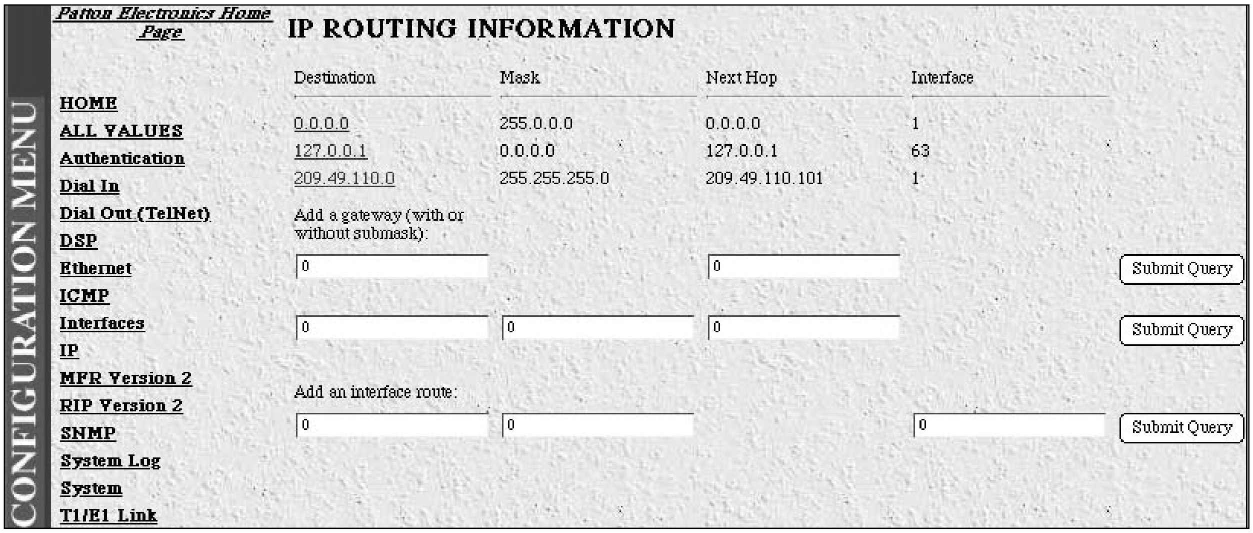
Entry Broadcast Address (ipAdEntBcastAddr) The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.

Entry Reassembly Maximum Size (ipAdEntReasmMaxSize) The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

IP Configuration (Routing Information)

The IP Routing Information screen shows routing information required to route IP datagrams. Specifically, the IP address, subnet mask, next hop router, and interface for each network interface defined in the box. To reach this screen, select IP Routing Info... from the main IP Configuration screen.

Figure A-37. IP Configuration - Routing Information



IP ROUTING INFORMATION

Destination	Mask	Next Hop	Interface
0.0.0.0	255.0.0.0	0.0.0.0	1
127.0.0.1	0.0.0.0	127.0.0.1	63
209.49.110.0	255.255.255.0	209.49.110.101	1

Add a gateway (with or without submask):

Add an interface route:

Destination (ipRouteDest) The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

Mask (ipRouteMask) Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belong to a class-A, B, or C network, and then using one of:

mask	network
255.0.0.0	class-A
255.255.0.0	class-B
255.255.255.0	class-C

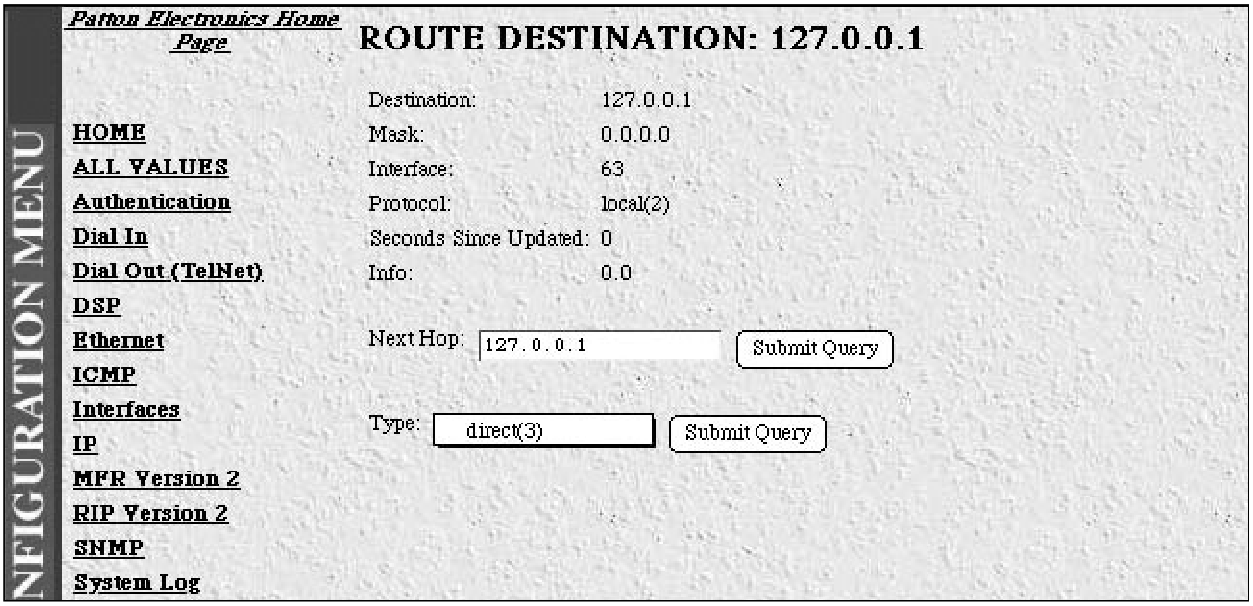
Next Hop (ipRouteNextHop) The IP address of the next hop of this route. (In the case of a route bound to an interface which is realized via a broadcast media, the value of this field is the agent's IP address on that interface.)

Interface (ipRouteIfIndex) The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

IP Configuration (Routing Information - Destination)

The IP Routing Information screen shows next hop routing information. To reach this screen, select one of the IP addresses under the hyperlink Destination column in the previous routing information screen.

Figure A-38. IP Configuration - Routing Information - Destination



ROUTE DESTINATION: 127.0.0.1

Destination:	127.0.0.1
Mask:	0.0.0.0
Interface:	63
Protocol:	local(2)
Seconds Since Updated:	0
Info:	0.0

Next Hop: 127.0.0.1

Type: direct(3)

Destination (ipRouteDest) The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

Mask (ipRouteMask) Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belong to a class-A, B, or C network, and then using one of:

mask	network
255.0.0.0	class-A
255.255.0.0	class-B
255.255.255.0	class-C

Interface (ipRouteIfIndex) The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

Protocol (ipRouteProto) The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts should support those protocols.

other(1)	none of the following
local(2),	non-protocol information,-- e.g., manually configured entries
netmgmt(3),	set via a network management protocol
icmp(4)	obtained via ICMP, -- e.g., Redirect
	the remaining values are all gateway routing protocols

egp(5),
ggp(6),
hello(7),
rip(8),
is-is(9),
es-is(10),
ciscoIgrp(11),
bbnSpfIgp(12),
ospf(13),
bgp(14)

Seconds Since Updated (ipRouteAge) The number of seconds since this route was last updated or otherwise determined to be correct. Note that no semantics of `too old' can be implied except through knowledge of the routing protocol by which the route was learned.

Info (ipRouteInfo) A reference to MIB definitions specific to the particular routing protocol which is responsible for this route, as determined by the value specified in the route's ipRouteProto value. If this information is not present, its value should be set to the OBJECT IDENTIFIER { 0 0 }, which is a syntatically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.

Next Hop (ipRouteNextHop) The IP address of the next hop of this route. (In the case of a route bound to an interface which is realized via a broadcast media, the value of this field is the agent's IP address on that interface.)

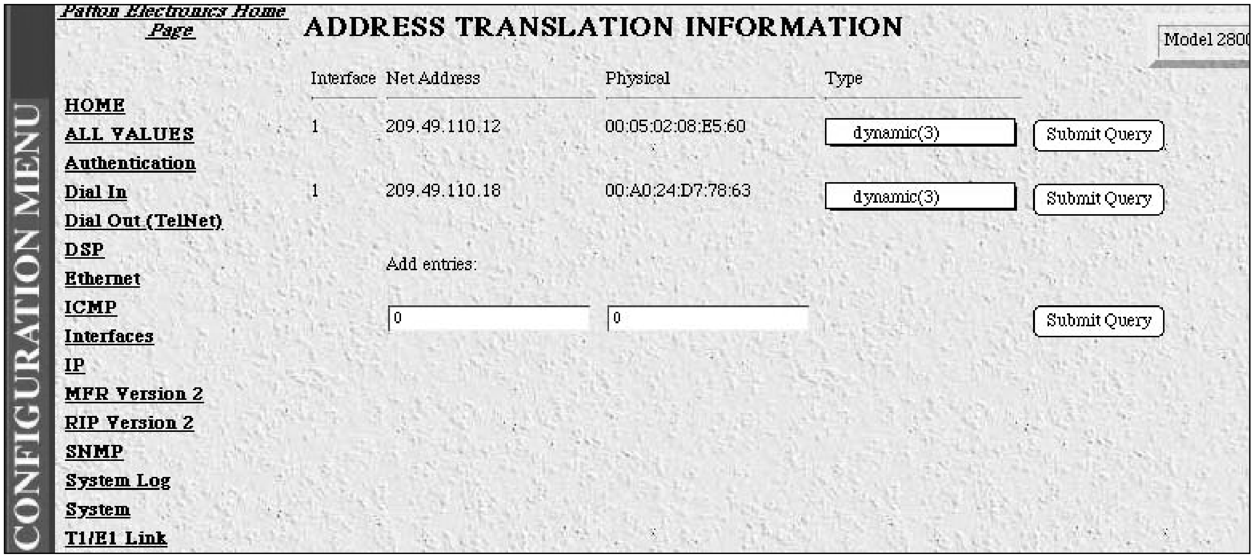
Type (ipRouteType) The type of route. Note that the values direct(3) and indirect(4) refer to the notion of direct and indirect routing in the IP architecture. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipRouteTable object. That is, it effectively dissasociates the destination identified with said entry from the route identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipRouteType object.

other(1),	none of the following
invalid(2),	an invalidated route
direct(3),	route to directly connected (sub-)network
indirect(4)	route to a non-local host/network/sub-network

IP Configuration - Address Translation Information

The IP address translation table contain the IpAddress to physical' address equivalences. Some interfaces do not use translation tables for determining address equivalences (e.g., DDN-X.25 has an algorithmic method); -- if all interfaces are of this type, then the Address Translation table is empty, i.e., has zero entries (See Figure A-39, below).

Figure A-39. IP Configuration - Address Translation Information



ADDRESS TRANSLATION INFORMATION

Interface	Net Address	Physical	Type
1	209.49.110.12	00:05:02:08:E5:60	dynamic(3)
1	209.49.110.18	00:A0:24:D7:78:63	dynamic(3)

Add entries:

0	0	

Interface (ipNetToMediaEntry) Each entry contains one IpAddress to `physical' address equivalence.

Net Address (ipNetToMediaNetAddress) The IpAddress corresponding to the media-dependent `physical' address.

Physical (ipNetToMediaPhysAddress) The media-dependent `physical' address.

Type (ipNetToMediaType) The type of mapping. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively dissasociates the interface identified with said entry from the mapping identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object.

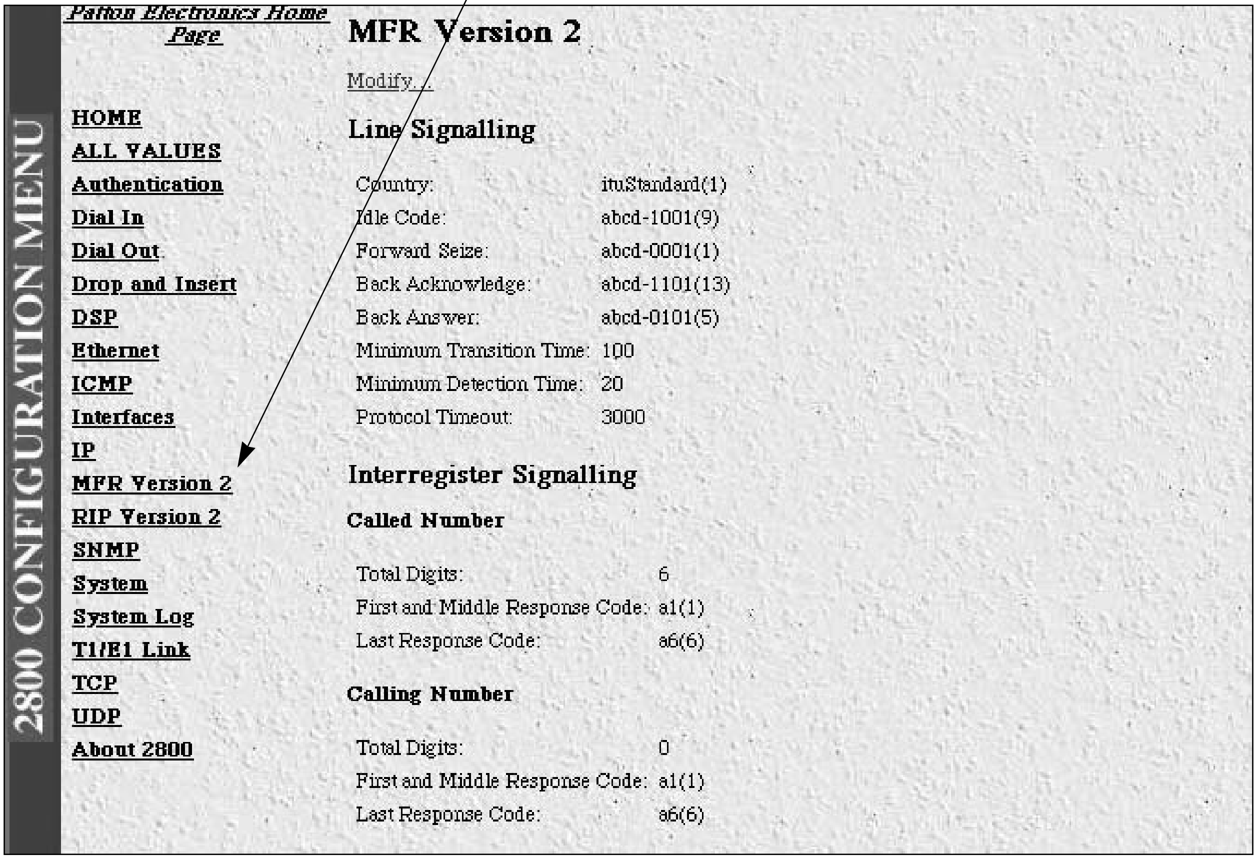
other(1),	none of the following
invalid(2),	an invalidated mapping
dynamic(3),	
static(4)	

MFR Version 2

The MFR Version 2 section contains objects that networks that use Signalling System R2. (In order to set up R2 Signalling in the 2800, refer to Recommendations Q.400 - Q.490 AND to the host country's PTT for national signalling specifications). This section contains read only and read/write Line Signalling, and Interregister Signalling information.

To reach the dial out Section, select MFR Version 2 from the 2800 Configuration Menu. (see Figure A-40, below). Following Figure A-40 are descriptions for each object on this page.

Figure A-40. MFR Version 2



MFR Version 2

Modify...

Line Signalling

Country:	ituStandard(1)
Idle Code:	abcd-1001(9)
Forward Seize:	abcd-0001(1)
Back Acknowledge:	abcd-1101(13)
Back Answer:	abcd-0101(5)
Minimum Transition Time:	100
Minimum Detection Time:	20
Protocol Timeout:	3000

Interregister Signalling

Called Number

Total Digits:	6
First and Middle Response Code:	a1(1)
Last Response Code:	a6(6)

Calling Number

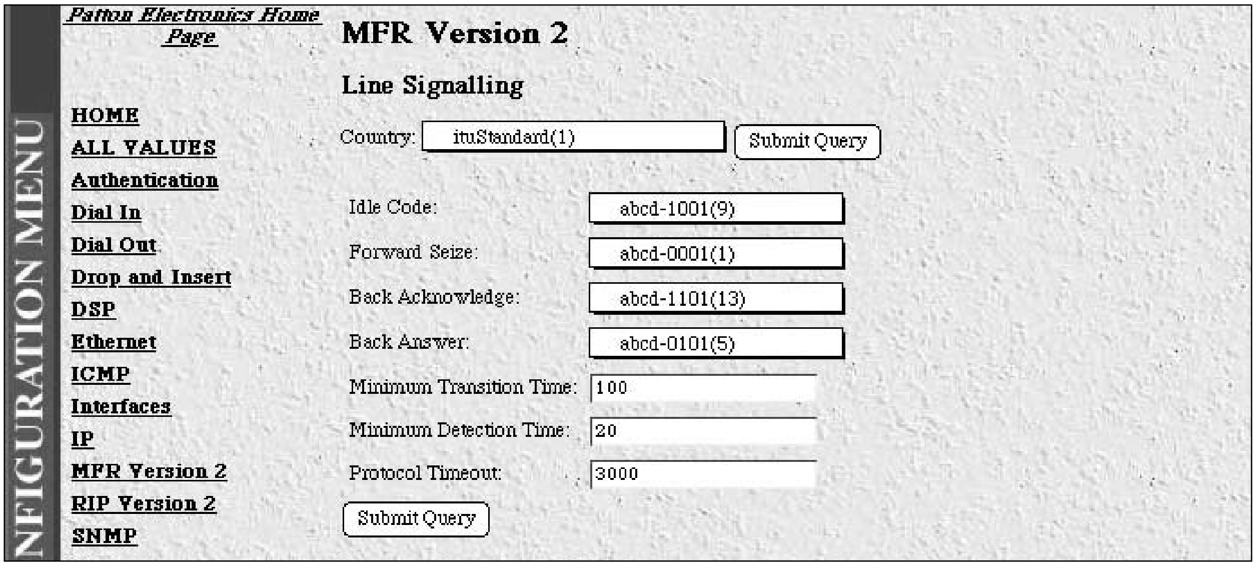
Total Digits:	0
First and Middle Response Code:	a1(1)
Last Response Code:	a6(6)

The objects on this screen will be discussed in the next section.

MFR Version 2 (Modify Line Signalling)

From this screen you can modify Line Signalling parameters (see Figure A-41, below). The Line Signalling parameters are link-by-link digital signals that use two signalling channels in each direction per circuit. To reach this screen, select Modify from the main Drop and Insert screen.

Figure A-41. MFR Version 2 - Modify Line Signalling



MFR Version 2

Line Signalling

Country: ituStandard(1)

Idle Code: abcd-1001(9)

Forward Seize: abcd-0001(1)

Back Acknowledge: abcd-1101(13)

Back Answer: abcd-0101(5)

Minimum Transition Time: 100

Minimum Detection Time: 20

Protocol Timeout: 3000

Line Signalling

The Line Signalling parameters are link-by-link digital signals that use two signalling channels in each direction per circuit. Set the 2800 objects based upon codes that pertain to Idle, Seized, Answered, Clear-back, Release, and Blocked conditions.

> **NOTE:** Line Signalling setup codes are country-specific. Please refer to Recommendation Q.400 - Q.490 and to the host country's PTT for national signalling specifications.

Country (lineSigCountry) Specifying a particular country or itu Standard defines the values of the remaining fields based on the specs. Custom allows for any values in the following fields (Line Signalling objects are country-specific. Please refer to the host country's PTT for national signalling specifications).

ituStandard(1),
custom(2)

Idle Code (lineSigIdleCode) Code to indicate that a line is not used.

abcd-0000(0),
abcd-0001(1),
abcd-0010(2),
abcd-0011(3),
abcd-0100(4),
abcd-0101(5),
abcd-0110(6), 1111(15)
abcd-0111(7),
abcd-1000(8),
abcd-1001(9),
abcd-1010(10),
abcd-1011(11),
abcd-1100(12),
abcd-1101(13),
abcd-1110(14),
abcd-

Forward Seize (lineSigForwardSeize) Code to indicate there is a desire to use a line.

abcd-0000(0),
abcd-0001(1),
abcd-0010(2),
abcd-0011(3),
abcd-0100(4),
abcd-0101(5),
abcd-0110(6), 1111(15)
abcd-0111(7),
abcd-1000(8),
abcd-1001(9),
abcd-1010(10),
abcd-1011(11),
abcd-1100(12),
abcd-1101(13),
abcd-1110(14),
abcd-

Back Acknowledge (lineSigBackAck) Code to indicate there is an agreement to use a line.

abcd-0000(0),
abcd-0001(1),
abcd-0010(2),
abcd-0011(3),
abcd-0100(4),
abcd-0101(5), 1111(15)
abcd-0110(6),
abcd-0111(7),
abcd-1000(8),
abcd-1001(9),
abcd-1010(10),
abcd-1011(11),
abcd-1100(12),
abcd-1101(13),
abcd-1110(14),
abcd-

Back Answer (lineSigBackAnswer) Code to indicate a call has been completed.

abcd-0000(0),
abcd-0000(0),
abcd-0001(1),
abcd-0010(2),
abcd-0011(3),
abcd-0100(4),
abcd-0101(5),
abcd-0110(6), 1111(15)
abcd-0111(7),
abcd-1000(8),
abcd-1001(9),
abcd-1010(10),
abcd-1011(11),
abcd-1100(12),
abcd-1101(13),
abcd-1110(14),
abcd-

Minimum Transition Time (lineSigMinTransTime) The minimum transition time in milliseconds.

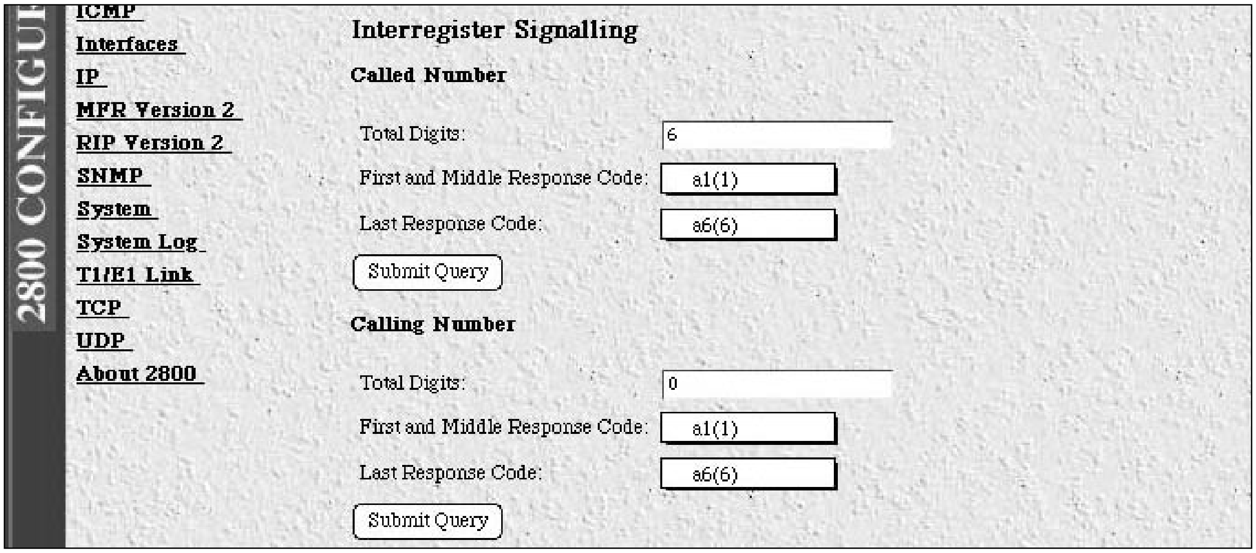
Minimum Detection Time (lineSigMinDetectTime) The minmum detect time in milliseconds.

Protocol Timeout (lineSigProtoTimeout) The time for a protocol timeout in milliseconds.

MFR Version 2 (Modify Interregister Signalling)

From this screen you can modify Line Signalling parameters (see Figure A-42, below). The Line Signalling parameters are link-by-link digital signals that use two signalling channels in each direction per circuit. To reach this screen, select Modify from the main Drop and Insert screen.

Figure A-42. MFR Version 2 - Modify Line Signalling



Interregister Signalling

Called Number

Total Digits: 6

First and Middle Response Code: a1(1)

Last Response Code: a6(6)

Submit Query

Calling Number

Total Digits: 0

First and Middle Response Code: a1(1)

Last Response Code: a6(6)

Submit Query

Interregister Signalling

The Interregister Signalling parameters are end-to-end 2-out-of-6 in-band code signals that use backward and forward-compelled signalling. Set the 2800 objects based upon codes that pertain to Forward Line Signals, Forward Register Signals, Backward Line, and Backward Register Signals.

> **NOTE:** Interregister Signalling setup codes are country-specific. Please refer to Recommendation Q.400 -Q.490 and to the host country's PTT for national signalling specifications.

Called Number

Total Digits (interRegCalledNumDig) The number of digits expected for the called number.

First and Middle Response Code (interRegCalledNumFirst) The code specifying what is done after every digit is sent except the last for the called number.

a1(1),
a2(2),
a3(3),
a4(4),
a5(5),
a6(6),
a7(7),
a8(8),
a9(9),
a10(10),
a11(11),
a12(12),
a13(13),
a14(14),
a15(15)

Last Response Code (interRegCalledNumLast) The code specifying what is done after the last digit is sent for the called number.

a1(1),
a2(2),
a3(3),
a4(4),
a5(5),
a6(6),
a7(7),
a8(8),
a9(9),
a10(10),
a11(11),
a12(12),
a13(13),
a14(14),
a15(15)

Calling Number

Total Digits (interRegCallingNumDig) The number of digits expected for the calling number.

First and Middle Response Code (interRegCallingNumFirst) The code specifying what is done after every digit is sent except the last for the calling number.

a1(1),
a2(2),
a3(3),
a4(4),
a5(5),
a6(6),
a7(7),
a8(8),
a9(9),
a10(10),
a11(11),
a12(12),
a13(13),
a14(14),
a15(15)

Last Response Code (interRegCallingNumLast) The code specifying what is done after the last digit is sent for the calling number.

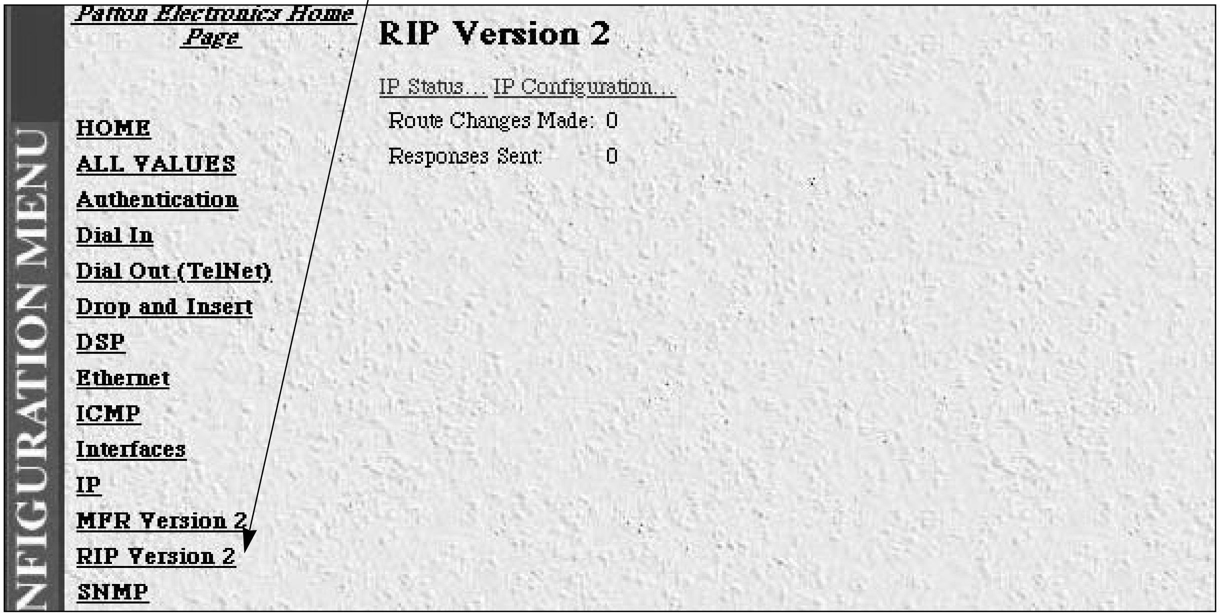
a1(1),
a2(2),
a3(3),
a4(4),
a5(5),
a6(6),
a7(7),
a8(8),
a9(9),
a10(10),
a11(11),
a12(12),
a13(13),
a14(14),
a15(15)

RIP Version 2

This section describes routing information as defined by the Routing Information Protocol (RIP). IP Status objects are read-only values, while IP Configuration objects are read-write values. In the IP All object identifiers described in the section are described in *RFC 1724: RIP Version 2 MIB Extension*.

To reach this section, select RIP Version 2 from the 2800 Configuration Menu. (see Figure 3-43, below). Following Figure A-43 are descriptions for each variable on this screen.

Figure A-43. RIP Version 2 Main Screen



RIP Version 2

Route Changes Made: 0
Responses Sent: 0

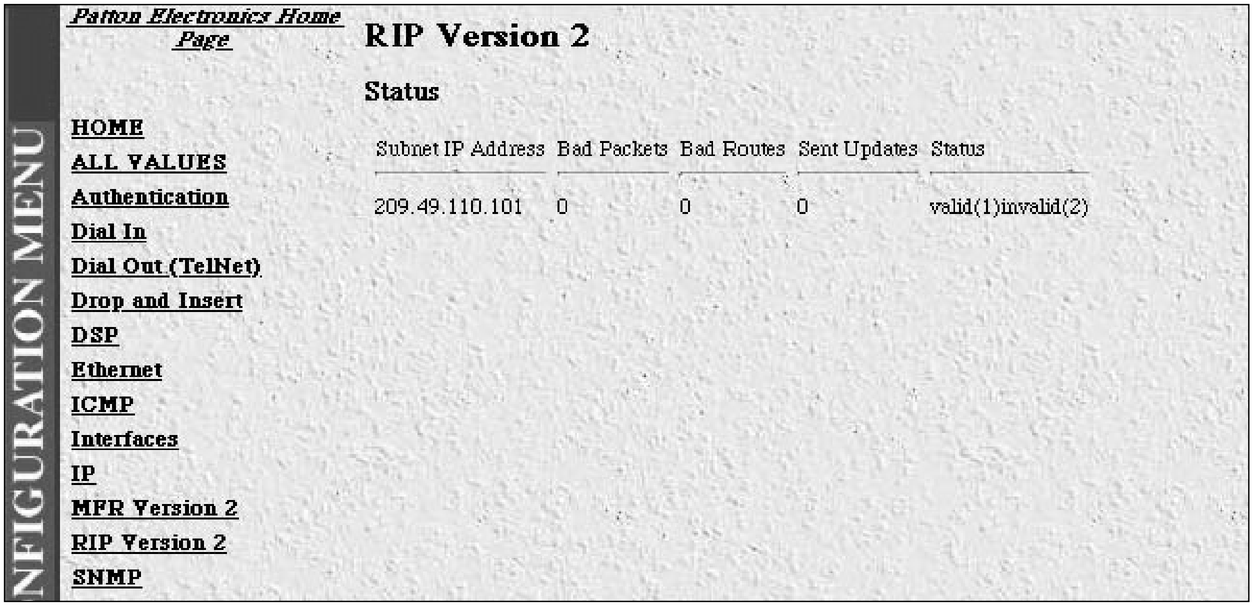
Route Changes Made (rip2GlobalRouteChanges) The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.

Responses Sent (rip2GlobalQueries) The number of responses sent to RIP queries from other systems.

RIP Version 2 (IP Status)

The RIP Version 2 Status screen read-only values that reflect routing and update information for each subnet address. To reach this screen, select IP Status from the hypertext entries at the top of the main RIP Version 2 screen (See Figure A-44, below).

Figure A-44. RIP Version 2 - IP Status



RIP Version 2

Status

Subnet IP Address	Bad Packets	Bad Routes	Sent Updates	Status
209.49.110.101	0	0	0	valid(1)invalid(2)

Subnet IP Address (rip2IfStatAddress) The IP Address of this system on the indicated subnet. For unnumbered interfaces, the value 0.0.0.N, where the least significant 24 bits (N) is the ifIndex for the IP Interface in network byte order.

Bad Packets (rip2IfStatRcvBadPackets) The number of RIP response packets received by the RIP process which were subsequently discarded for any reason (e.g. a version 0 packet, or an unknown command type).

Bad Routes (rip2IfStatRcvBadRoutes) The number of routes, in valid RIP packets, which were ignored for any reason (e.g. unknown address family, or invalid metric).

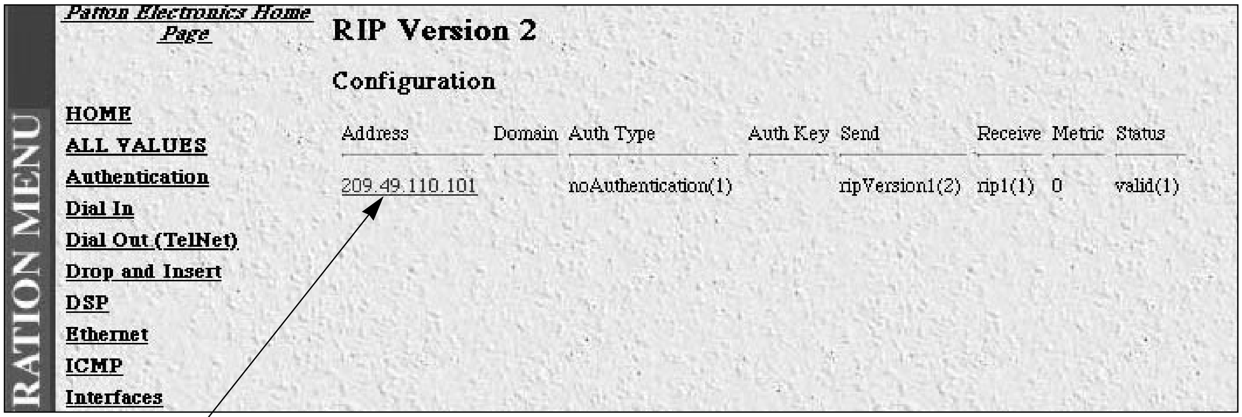
Sent Updates (rip2IfStatSentUpdates) The number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.

Status (rip2IfStatStatus) Writing invalid has the effect of deleting this interface.

RIP Version 2 (IP Configuration)

The RIP Version 2 Configuration screen shows objects for each subnet address including authentication method, RIP Version 1 or Version 2 compatibility, and metric value. To reach this screen, select IP Configuration from the main RIP Version 2 screen (See Figure A-45, below).

Figure A-45. RIP Version 2 - IP Configuration



RIP Version 2

Configuration

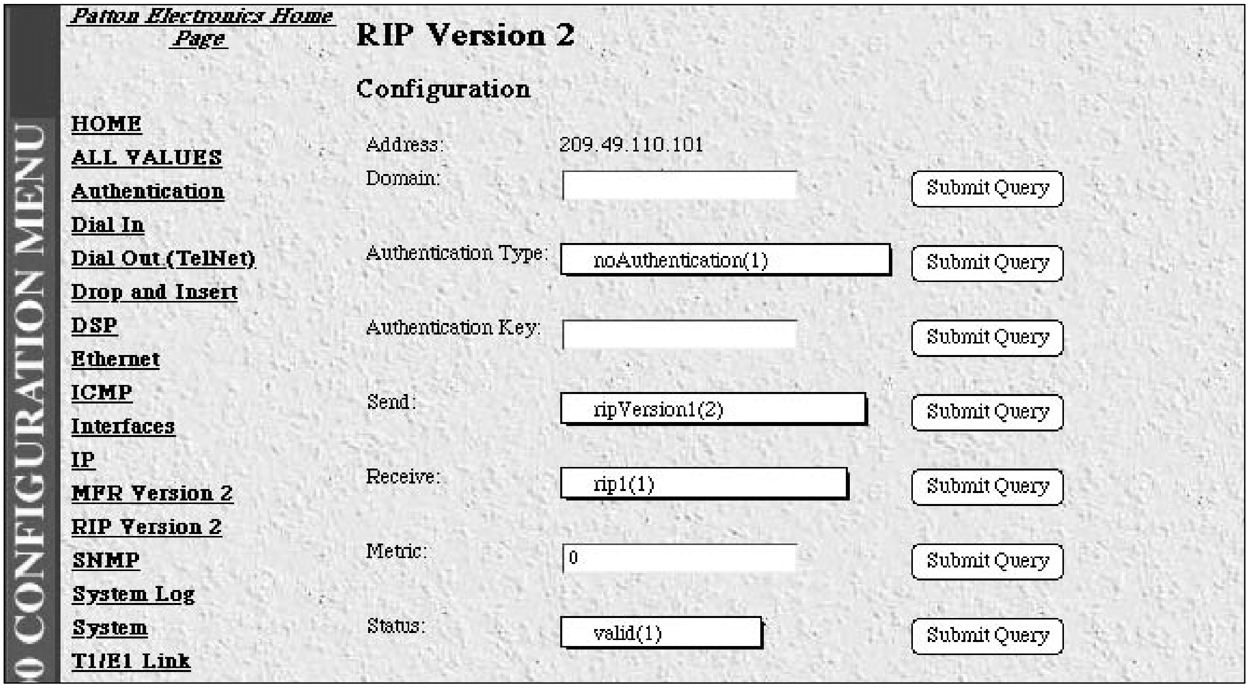
Address	Domain	Auth Type	Auth Key	Send	Receive	Metric	Status
209.49.110.101		noAuthentication(1)		ripVersion1(2)	rip1(1)	0	valid(1)

Each object except the subnet address is a read-write value that may be changed by selecting the hypertext subnet value shown above. The objects on shown on this this screen are reserved for the following section, RIP Version 2 - Configuration Details**.**

RIP Version 2 (IP Configuration Details)

The RIP Version 2 Configuration Details screen shows read-write objects for each subnet address including authentication method, RIP Version 1 or Version 2 compatibility, and metric value (See Figure A-46, below). The section below describes each of the following objects.

Figure A-46. RIP Version 2 - Configuration Details



RIP Version 2

Configuration

Address: 209.49.110.101
Domain:
Authentication Type: noAuthentication(1)
Authentication Key:
Send: ripVersion1(2)
Receive: rip1(1)
Metric: 0
Status: valid(1)

Address (rip2IfConfAddress) The IP Address of this system on the indicated subnet. For unnumbered interfaces, the value 0.0.0.N, where the least significant 24 bits (N) is the ifIndex for the IP Interface in network byte order.

Domain (rip2IfConfDomain) Value inserted into the Routing Domain field of all RIP packets sent on this interface.

Auth Type (rip2IfConfAuthType) The type of Authentication used on this interface.

noAuthentication (1),
simplePassword (2),

Auth Key (rip2IfConfAuthKey) The value to be used as the Authentication Key whenever the corresponding instance of rip2IfConfAuthType has a value other than authentication. A modification of the corresponding instance of rip2IfConfAuthType does not modify the rip2IfConfAuthKey value. If a string shorter than 16 octets is supplied, it will be left-justified and padded to 16 octets, on the right, with nulls (0x00).

Reading this object always results in an OCTET STRING of length zero; authentication may not be bypassed by reading the MIB object."

Send (rip2IfConfSend) What the router sends on this interface. ripVersion 1 implies sending RIP updates compliant with RFC 1058. rip1Compatible implies broadcasting RIP-2 updates using RFC 1058 route subsumption rules. ripVersion2 implies multicasting RIP-2 updates. ripV1Demand indicates the use of Demand RIP on a WAN interface under RIP Version 1 rules. ripV2Demand indicates the use of Demand RIP on a WAN interface under Version 2 rules.

doNotSend (1),
ripVersion1 (2),
rip1Compatible (3),
ripVersion2 (4)

Receive (rip2IfConfReceive) This indicates which version of RIP updates are to be accepted. Note that rip2 and rip1OrRip2 implies reception of multicast packets.

rip1 (1),
rip2 (2),
rip1OrRip2 (3),
doNotRecieve (4)

Metric (rip2IfConfDefaultMetric) This variable indicates the metric that is to be used for the default route entry in RIP updates originated on this interface. A value of zero indicates that no default route should be originated; in this case, a default route via another router may be propagated.

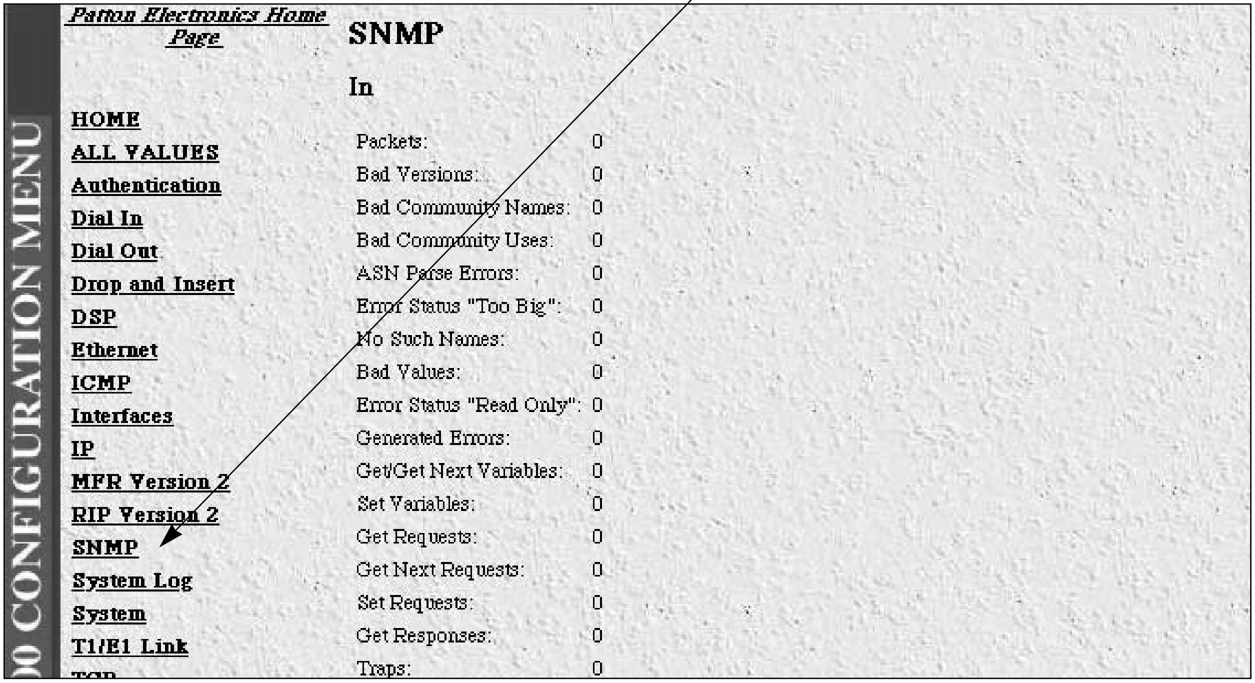
Status (rip2IfConfStatus) Writing invalid has the effect of deleting this interface.

valid (1),
invalid (2),

SNMP

The 2800 provides management and statistical information on SNMP. Detailed information on the SNMP MIB variables may be downloaded from the RFC. Select SNMP from the 2800 Configuration Menu to monitor SNMP statistics. Following Figure A-47 and A-48 are descriptions for each variable on this page.

Figure A-47 SNMP Out

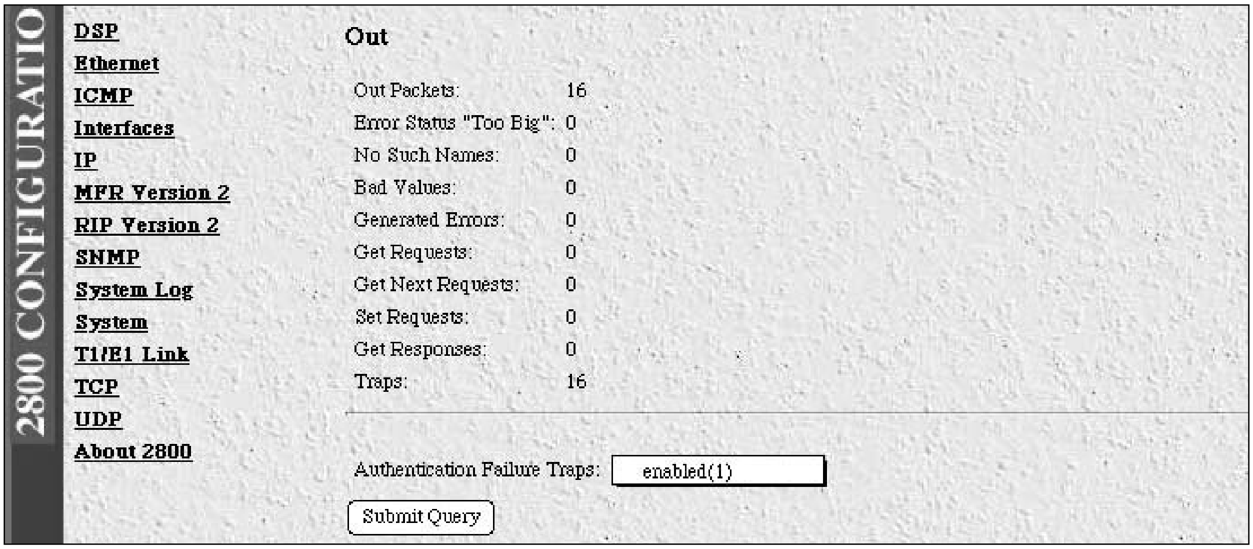


SNMP

In

Packets:	0
Bad Versions:	0
Bad Community Names:	0
Bad Community Uses:	0
ASN Parse Errors:	0
Error Status "Too Big":	0
No Such Names:	0
Bad Values:	0
Error Status "Read Only":	0
Generated Errors:	0
Get/Get Next Variables:	0
Set Variables:	0
Get Requests:	0
Get Next Requests:	0
Set Requests:	0
Get Responses:	0
Traps:	0

Figure A-48 SNMP Out



Out

Out Packets:	16
Error Status "Too Big":	0
No Such Names:	0
Bad Values:	0
Generated Errors:	0
Get Requests:	0
Get Next Requests:	0
Set Requests:	0
Get Responses:	0
Traps:	16

Authentication Failure Traps: enabled(1)

In

Packets (snmpInPkts) The total number of Messages delivered to the SNMP entity from the transport service.

Bad Version (snmpInBadVersions) The total number of SNMP Messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version."

Bad Community Names (snmpInBadCommunityNames) The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity."

Bad Community Uses (snmpInBadCommunity) The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message."

ASN ParseErrors (snmpInASNParseErrs) The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP Messages."

Error Status "Too Big" (snmpInTooBigs) The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'tooBig'."

No Such Names (snmpInNoSuchNames) The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName'."

Bad Values (snmpInBadValues) The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue'."

Error Status "Read Only" (snmpInReadOnlys) The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `readOnly'. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value `readOnly' in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.

Generated Errors (snmpInGenErrs) The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr'."

Get/Get Next Variables (snmpInTotalReqVars) The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs."

Set Variables (snmpInTotalSetVars) The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs."

Get Requests (snmpInGetRequests) The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity."

Get Next Requests (snmpInGetNexts) The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.

Set Requests (snmpInSetRequests) The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity."

Get Responses (snmpInGetResponses) The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity."

Traps (snmpInTraps) The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.

Out

Out Packets (snmpOutPkts) The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.

Error Status "Too Big" (snmpOutTooBigs) The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is "tooBig.'

No Such Names (snmpOutNoSuchNames) The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status is `noSuchName'.

Bad Values (snmpOutBadValues) The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is `badValue'.

Generated Errors (snmpOutGenErrs) The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is `genErr'.

Get Requests (snmpOutGetRequests) The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.

Get Next Requests (snmpOutGetNexts) The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity.

Set Requests (snmpOutSetRequests) The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.

Get Responses (snmpOutGetResponses) The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.

Traps (snmpOutTraps) The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.

Authentication Failure Traps (snmpEnableAuthenTraps) Indicates whether the SNMP agent process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authentication-failure traps may be disabled. Note that it is strongly recommended that this object be stored in non-volatile memory so that it remains constant between re-initializations of the network management system.

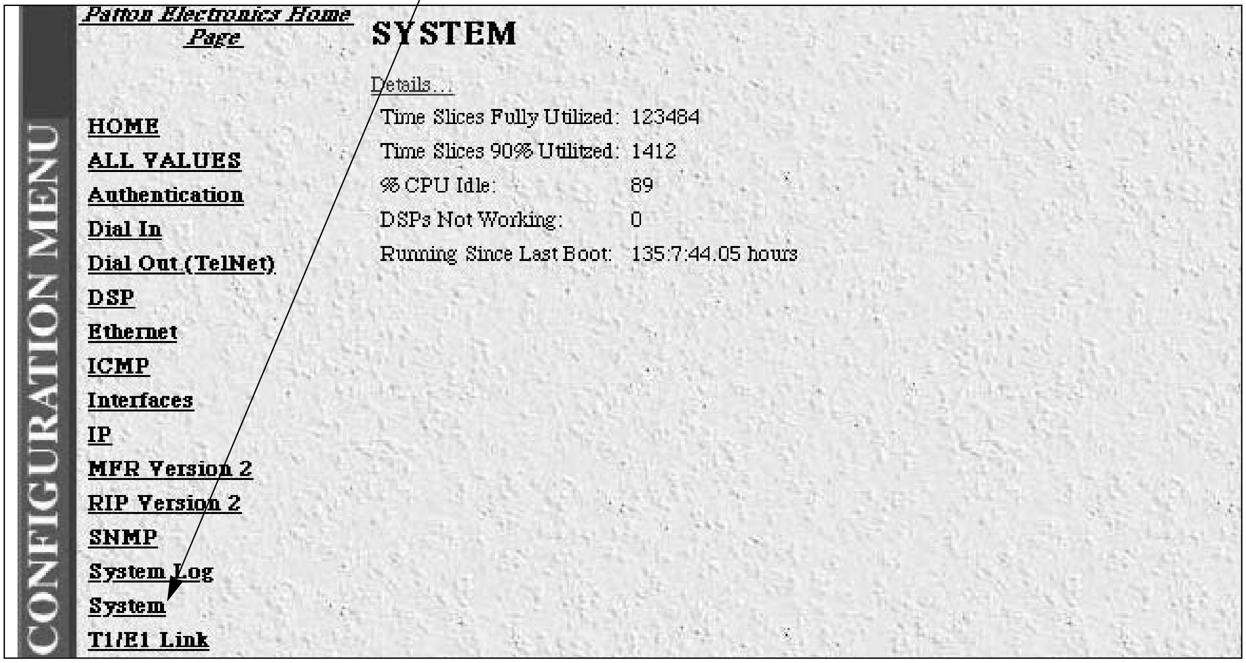
enable (1);
disable (2)

System

The System Section contains general setup information about the 2800. System parameters may be read only and read write parameters. These parameters are Patton Enterprise MIB object identifiers, though some are contained in RFC 1213, “Management Information Base for Network Management of TCP/IP-based internets: MIB-II”.

To reach the System Section, select System from the 2800 Configuration Menu. (see Figure A-49, below). Following Figure A-49 are descriptions for each variable on this screen.

Figure A-49. System Main Screen



SYSTEM

Details...

```
Time Slices Fully Utilized:  123484
Time Slices 90% Utilitzed:   1412
% CPU Idle:                  89
DSPs Not Working:            0
Running Since Last Boot:     135:7:44.05 hours
```

Total Active Calls (diActive) This number, ranging from 0 to 60 (this number can be no more than forty-six (46) for two T1/PRIs running PRI, and sixty (60) for a E1/PRI) displays the total number of calls being processed (connecting, dead, authenticating,etc...) in a 2800 at the time the HOME page was brought up.

Time Slices Fully Utilized (boxCPUCritical) Each second is divided into 100 time slices. If a time slice passes in which all the CPU power was used to handle the system, then this count is incremented by one.

Time Slices 90% Utilized (boxCPUWarning) Each second is divided into 100 time slices. If a time slice passs in which only 10 percent of the CPU power was accessed, then this count is impletement by one.

Percentage CPU Idle (boxIdleTime) This is an indication of the amount of system CPU power which is not being utilized by the 2800. The return value is a percentage of free CPU cycles since the last time the variable was read.

DSPs Not Working (dspFailed) This number should always be zero. The DSP's in the 2800 are arranged as a resource pool and called upon at ring-time. Therefore, if a DSP does not work, chances are you'll never know, as the 2800 will automatically remove the defiant DSP from the resource pool. One symptom of a DSP failures is the 2800 isn't handling as many calls as it should. A DSP may be taken out of service if it fails to respond to the 2800 CPU. If a DSP isn’t available when a call comes in, the call will simply ring and not be answered.

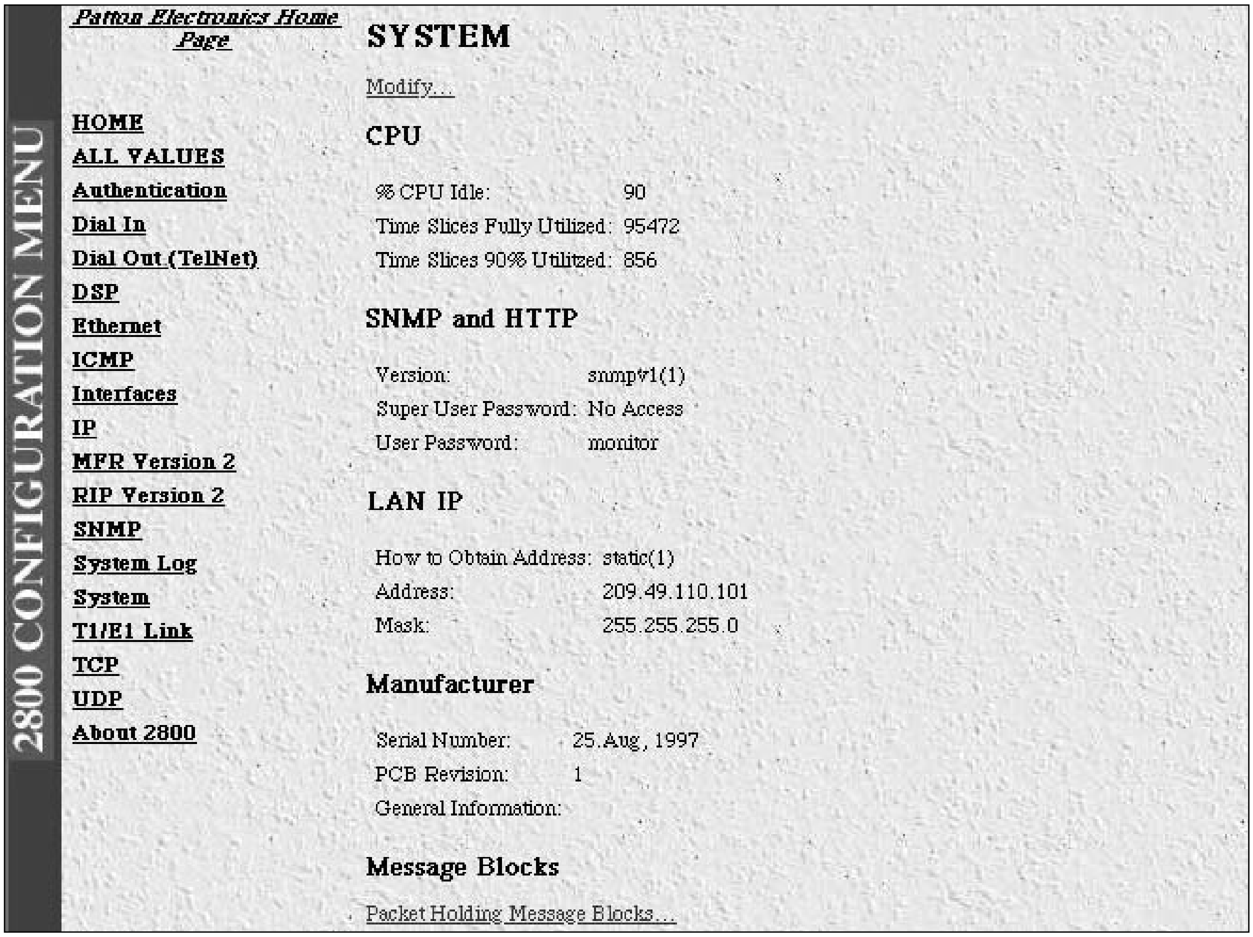
Total DRAM Detected (boxDetectedMemory) This number shows the total number of bits of installed and available DRAM.

Running Since Last Boot (sysUpTime) This tells you how long the 2800 has been running since the it was last reset. It displays the number of hours and rolls over after 1,193 hours (497 days).

System Details (CPU, SNMP and HTTP, LAN IP, Manufacturer, Message Blocks)

From this screen you can view CPU, SNMP and HTTP, LAN IP, Manufacturer, and Message Block information (see Figure A-50, below). To reach this screen, select Details from the main System Details screen. (**NOTE:** You may modify SNMP and HTTP, and LAN IP parameters by selecting Modify from the top of this screen).

Figure A-50. System Details (CPU, SNMP and HTTP, LAN IP, Manufacturer, Message Blocks)



SYSTEM

CPU

% CPU Idle: 90
Time Slices Fully Utilized: 95472
Time Slices 90% Utilized: 856

SNMP and HTTP

Version: snmpv1(1)
Super User Password: No Access
User Password: monitor

LAN IP

How to Obtain Address: static(1)
Address: 209.49.110.101
Mask: 255.255.255.0

Manufacturer

Serial Number: 25.Aug, 1997
PCB Revision: 1
General Information:

Message Blocks

Packet Holding Message Blocks...

CPU

This section describes certain CPU utilization parameters.

Percentage CPU Idle(boxidletime) This indicates what percentage of the I960 CPU processing power is not being utilized.

Time Slices Fully Utilized(boxCPUcritical) This value represents a count of how many times the CPU was fully utilized expressed in 1/100th seconds.

Time Slices 90% Utilized(boxCPUWarning) This value represents a count of how many times the CPU approached full utilization expressed in 1/100th seconds.

SNMP and HTTP

This section describes the login and password parameters.

Version(boxSnmpVersion) This parameter indicates the SNMP version number supported by this unit. snmpv (ver #) A revision of Simple Network Management Protocol (not just a new MIB) which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

Super User Password(boxSnmpMasterPassword) This accesses the super user password stored in Flash memory.

User Password(boxSnmpMonitorPassword) This accesses the user monitoring password for SNMP and HTTP.

LAN IP

This section describes the IP access parameters used in the 2800 (**NOTE:** This software release of the 2800, Rev. 1.3) uses only **disable(0) , static(1), rarp (2)** IP access methods**.**

How to Obtain Address(boxIPAddressTechnique) This indicates how to obtain the LAN IP address.

Options:

disable(0)	Ethernet port is disabled (e.g. 2800 T1 to T1 usage only)
static(1)	LAN IP address is obtained from EIA-232 port and stored in Flash memory
rarp (2)	Reverse Address Resolution Protocol - A protocol defined in RFC 903 which provides the reverse function of ARP. RARP maps a hardware address (MAC address) to an Internetaddress. It is used primarily by diskless nodes, when they first initialize, to find their Internet address.
bootp(3)	The Bootstrap Protocol. A protocol described in RFCs 951 and 1084 and

used for booting diskless workstations.

dhcp(4) Dynamic Host Configuration Protocol A protocol introduced by Microsoft on their NT server with version 3.5 in late 1994. This protocol provides a means to dynamically allocate IP addresses to IBM PCs running on a Microsoft Windows local area network. The system administrator assigns a range of IP addresses to DHCP and each client PC on the LAN has its TCP/IP software configured to request an IP address from the DHCP server. The request and grant process uses a lease concept with a controllable time period. More information can be found in the Microsoft documentation on NT Server.

Address(boxIPAddress) If the address technique above is static then this represents the LAN IP address.

Mask(boxIPMask) If the address technique above is static then the represents the LAN IP mask.

Manufacturer

This section describes 2800-specific manufacturer information.

Serial Number(boxManufactureDatecode) The datecode of manufacture and serial number.

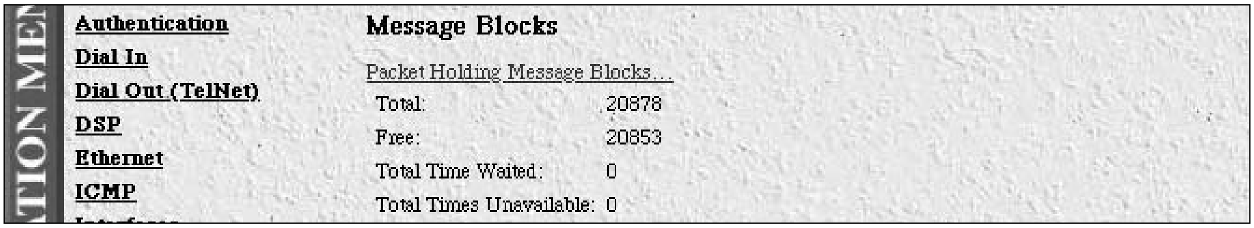
PCB Revision(boxManufacturePcbRevision) The revision of the printed circuit board.

General Information(boxManufactureGeneralInfo) A manufacturing notes area for additional information.

Message Blocks

The 2800 system manages the I960 processor utilization by allocating message blocks for incoming data. Message block sizes are 0, 128, 1536, and 2560 bytes. This section shows total values of 2800 message block usage (see Figure A-51, below).

Figure A-51. Message Blocks



Message Blocks

Packet Holding Message Blocks...

Total:	20878
Free:	20853
Total Time Waited:	0
Total Times Unavailable:	0

Packet Holding Message Blocks... buffer usage of 2800 message blocks based upon message block sizes (see below).

Total(boxMsgBlksConfigured) The total number of message blocks on the system.

Free(boxMsgBlksFree) The number of free message blocks available.

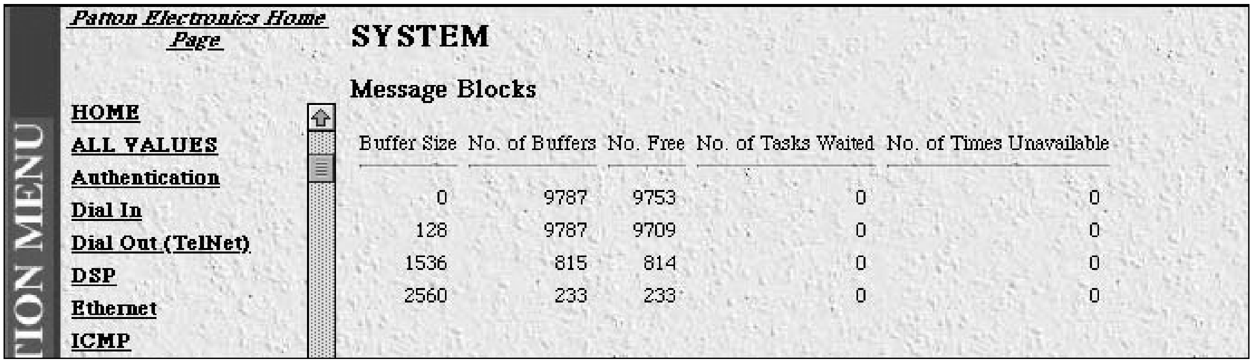
Total Time Waited(boxCountMsgBlkTaskWait) The number of times a CPU task had to wait for a message block.

Total Times Unavailable(boxCountMsgBlkUnavailable) The number of times a message block was unavailable.

Packet Holding Message Blocks...

The 2800 system manages the I960 processor utilization by allocating message blocks for data transfers. This section shows buffer usage of 2800 message blocks based upon message block sizes (See Figure A-52, below).

Figure A-52. Packet Holding Message Blocks



SYSTEM

Message Blocks

Buffer Size	No. of Buffers	No. Free	No. of Tasks Waited	No. of Times Unavailable
0	9787	9753	0	0
128	9787	9709	0	0
1536	815	814	0	0
2560	233	233	0	0

Buffer Size(boxbuffersize) The size in bytes of the buffer.

No. of Buffers (boxbuffercount) The number of buffers this size which are currently free for use

No. Free (boxbuffersfree) The number of buffers this size which are currently free for use

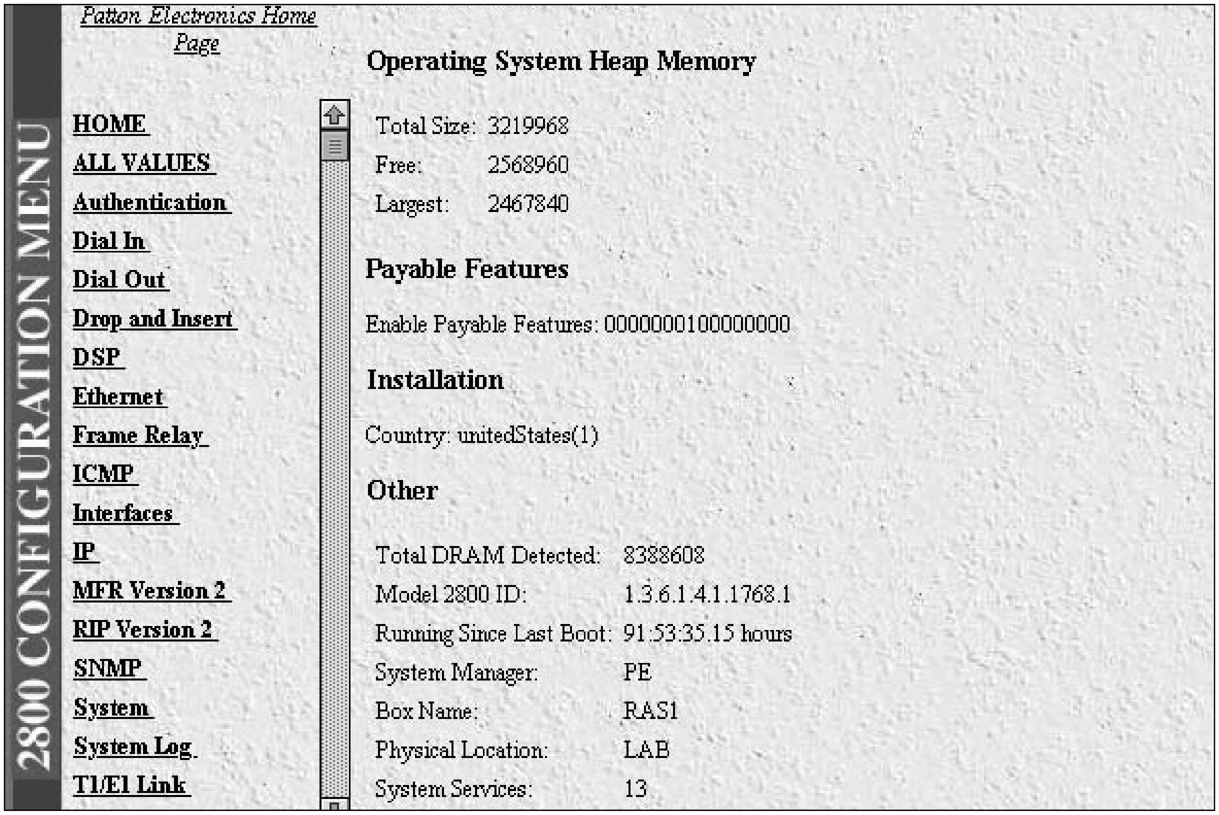
No. of Tasks Waited (boxCountBufferTaskWait) The number of times a task has waited for this buffer size.

No. of Times Unavailable(boxCountBufferUnavailable) The number of times one of these buffers was unavailable.

System Details (Operating System Heap Memory, Payable Features, Installation, Other)

From this screen you can view Operating System Heap Memory, Payable Features, Installation, and Other system parameters for dial in users (see Figure A-53, below). To reach this screen, scroll down from the previous screen. (**NOTE:** You may modify Payable Features, Installation, and Other parameters by selecting <u>Modify</u> from the top of this screen).

Figure A-53. System Details (Operating System Heap Memory, Payable Features, Installation, Other)



Operating System Heap Memory

Total Size: 3219968
Free: 2568960
Largest: 2467840

Payable Features

Enable Payable Features: 0000000100000000

Installation

Country: unitedStates(1)

Other

Total DRAM Detected:	8388608
Model 2800 ID:	1.3.6.1.4.1.1768.1
Running Since Last Boot:	91:53:35.15 hours
System Manager:	PE
Box Name:	RAS1
Physical Location:	LAB
System Services:	13

<u>Operating System Heap Memory</u>

Operating System Heap memory is used to efficiently manage the memory and address space of a process for an application. Applications typically need to allocate a specific number of bytes to fulfill a parameter request or to act as a temporary buffer.

Total Size (boxHeapSize) The size of the operating system heap memory.

Free (boxHeapFreeSpace) The amount of operating system heap memory currently available.

Payable Features

Enable Payable Features(boxFeatureEnableKey) This encoded string is used to enable payable features.

Installation

Country (installCountry) This object allows the user to specify the country that the box lives in so we can change the way the box operates based on local laws.

other(0),
unitedStates(1),
australia(2),
canada(3),
europeanUnion(4),
france(5),
germany(6)

Other

Total DRAM Detected(boxDetectedMemory) The total number of bytes of DRAM detected by the CPU.

Model 2800 ID(sysObjectID) This SNMP variable represents the “kind of box” is being managed as defined by specification RFC1213.MIB.

Running Since Last Boot(sysUpTime) This SNMP variable represents the time (in hundreds of seconds) since the network management portion of the system was last re-initialized as specified in RFC1213.MIB.

System Manager(sysContact) This SNMP variable represents the textual identification of the contact person for this managed node,together with information on how to contact this person as defined by specification RFC1213.MIB.

Box Name(sysName) This is “An administratively assigned name for this managed node. By convention, this is the node’s fully-qualified domain name. “(RFC1213.MIB)

Physical Location(sysLocation) “The physical location of this node (e.g., ‘ telephone closet, 3rd floor’).” (RFC1213.MIB)

System Services(sysServices) “A value which indicates the set of services that this entity primarily offers” (RFC1213.MIB)

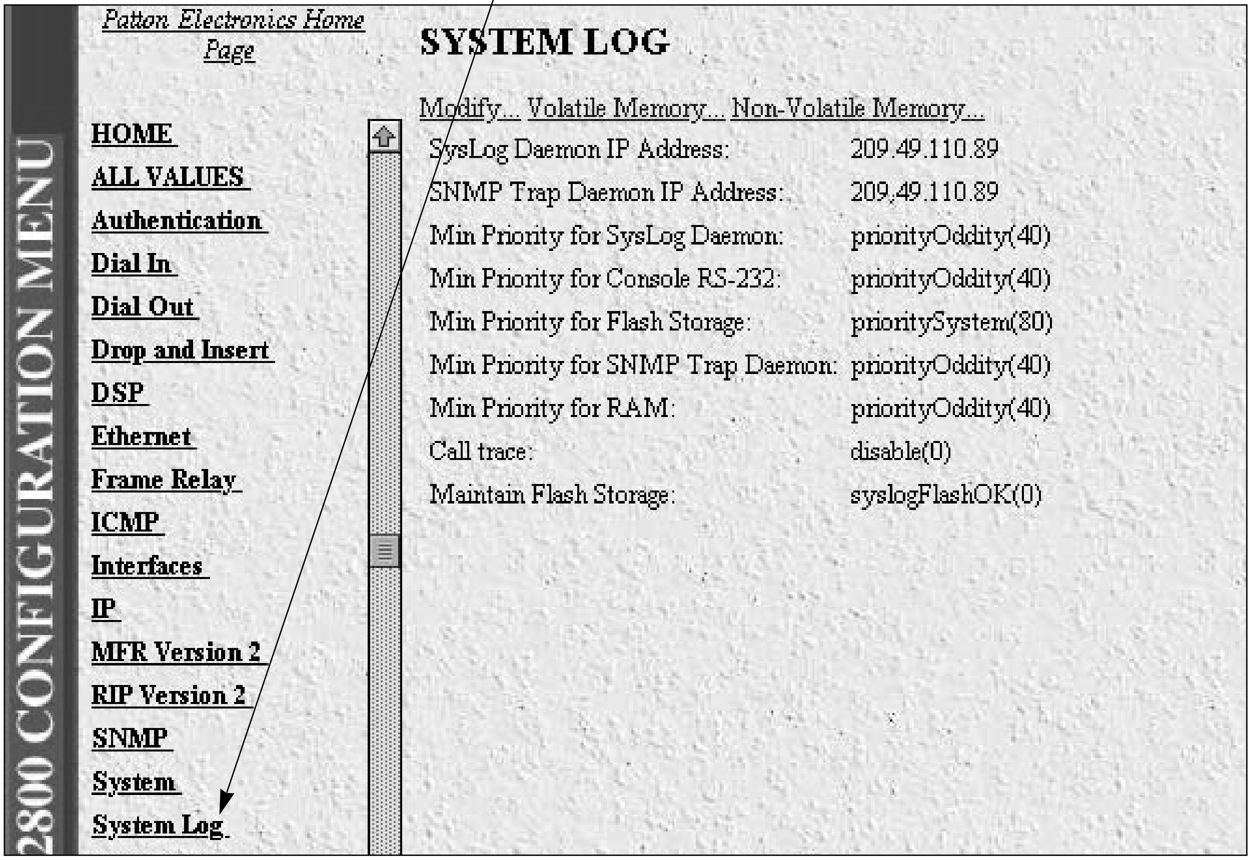
You may modify SNMP and HTTP, LAN IP, Payable Features, Installation, and Other parameters of the 2800 simply by selecting Modify at the top of the System Details Screen..

System Log

The System Log is a system-wide error reporting utility. The objects in the System Log are read only and read-write parameters. These parameters are all Patton Enterprise MIB object identifiers.

To reach the System Log Section, select System Log from the 2800 Configuration Menu. (see Figure A-54, below). Following Figure A-54 are descriptions for each variable on this screen.

Figure A-54 System Log Main Screen



SYSTEM LOG

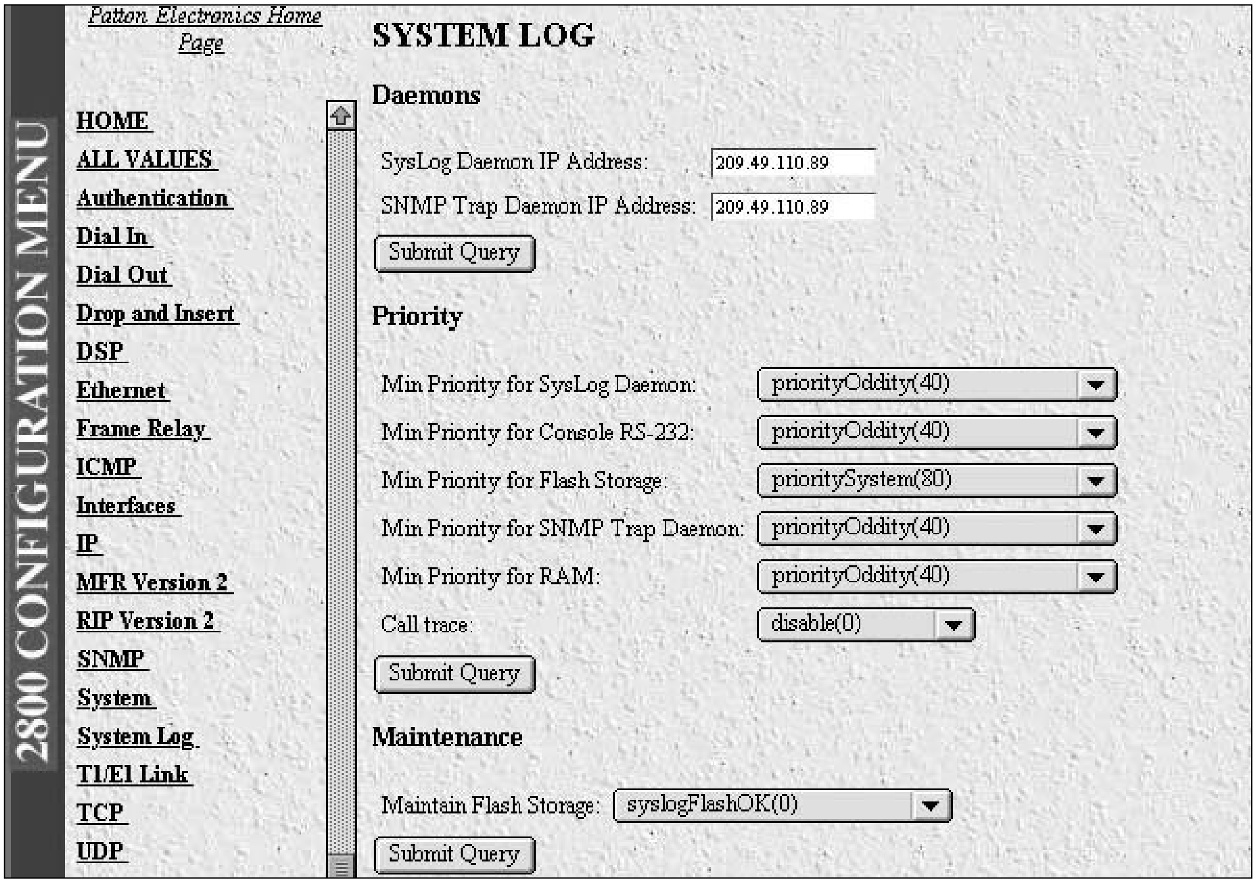
SysLog Daemon IP Address:	209.49.110.89
SNMP Trap Daemon IP Address:	209.49.110.89
Min Priority for SysLog Daemon:	priorityOddity(40)
Min Priority for Console RS-232:	priorityOddity(40)
Min Priority for Flash Storage:	prioritySystem(80)
Min Priority for SNMP Trap Daemon:	priorityOddity(40)
Min Priority for RAM:	priorityOddity(40)
Call trace:	disable(0)
Maintain Flash Storage:	syslogFlashOK(0)

The objects contained on this screen are read-write values. They are described in the next section.

System Log (Modify Daemon, Priority, Maintenance)

The System Log -Modify screen shows syslog and SNMP trap daemon locations, priority and maintenance. To reach this screen, select Modify from the main System Log screen (See Figure A-55, below).

Figure A-55 System Log (Modify Daemon, Priority, Maintenance)



SYSTEM LOG

Daemons

SysLog Daemon IP Address: 209.49.110.89
SNMP Trap Daemon IP Address: 209.49.110.89

Priority

Min Priority for SysLog Daemon: priorityOddity(40)
Min Priority for Console RS-232: priorityOddity(40)
Min Priority for Flash Storage: prioritySystem(80)
Min Priority for SNMP Trap Daemon: priorityOddity(40)
Min Priority for RAM: priorityOddity(40)
Call trace: disable(0)

Maintenance

Maintain Flash Storage: syslogFlashOK(0)

Daemons

SysLog Daemon IP Address(syslogDaemonIP) The IP address of a host system which is running a syslog daemon. System messages with a priority greater than or equal to syslogDaemonPriority will be sent to this IP address.

SNMP Trap Daemon IP Address (syslogTrapIP) The IP address of a host system which is running a SNMP trap daemon. System messages with a priority greater than or equal to syslogTrapPriority will be sent to this IP address.

Priority

Min Priority for SysLog Daemon (syslogDaemonPriority) System messages which have a priority equal to or greater than this setting will be sent to the syslog daemon defined by syslogDaemonIP

priorityVerbose(5)
priorityDebug(10)
priorityInfo(20)
priorityOddity(40)
priorityService(60)
prioritySystem(80)
priorityDisable(1000)

Min Priority for Console RS-232 (syslogConsolePriority) System messages which have a priority equal to or greater than this setting will be printed directly to the RS-232 configuration port. Messages will be printed regardless of the current operating state of the RS-232 configuration port. If a manager is logged into the RS-232 port using PPP then syslog messages are not packed into PPP packets.

priorityVerbose(5)
priorityDebug(10)
priorityInfo(20)
priorityOddity(40)
priorityService(60)
prioritySystem(80)
priorityDisable(1000)

Min Priority for Flash Storage (syslogFlashPriority) System messages which have a priority equal to or greater than this setting will be permenantly stored in the Flash PROM. Some maximum number of messages may be stored in the Flash PROM before this storage area must be cleared.

priorityVerbose(5)
priorityDebug(10)
priorityInfo(20)
priorityOddity(40)
priorityService(60)
prioritySystem(80)
priorityDisable(1000)

Min Priority for SNMP Trap Daemon (syslogTrapPriority) System messages which have a priority equal to or greater than this setting will be sent to the SNMP trap daemon defined by syslogTrapIP.

priorityVerbose(5)
priorityDebug(10)
priorityInfo(20)
priorityOddity(40)
priorityService(60)
prioritySystem(80)
priorityDisable(1000)

Cll Trace (syslogCallTrace) Enabling this will activate the call tracing utility. This is a powerful debugging utility which will log every single function call and return. At the death of a box the call trace will be printed out and can be sent to tech support. This utility will take a large amount of CPU power.

disable(0),
enable(1),
dump(2)

Min Priority for RAM (syslogTablePriority) System messages which have a priority equal to or greater than this setting will be temporarily stored in the RAM of the unit. A maximum number of messages is kept in the RAM and old messages are aged out. All messages are lost during a reboot.

priorityVerbose(5)
priorityDebug(10)
priorityInfo(20)
priorityOddity(40)
priorityService(60)
prioritySystem(80)
priorityDisable(1000)

Maintenance

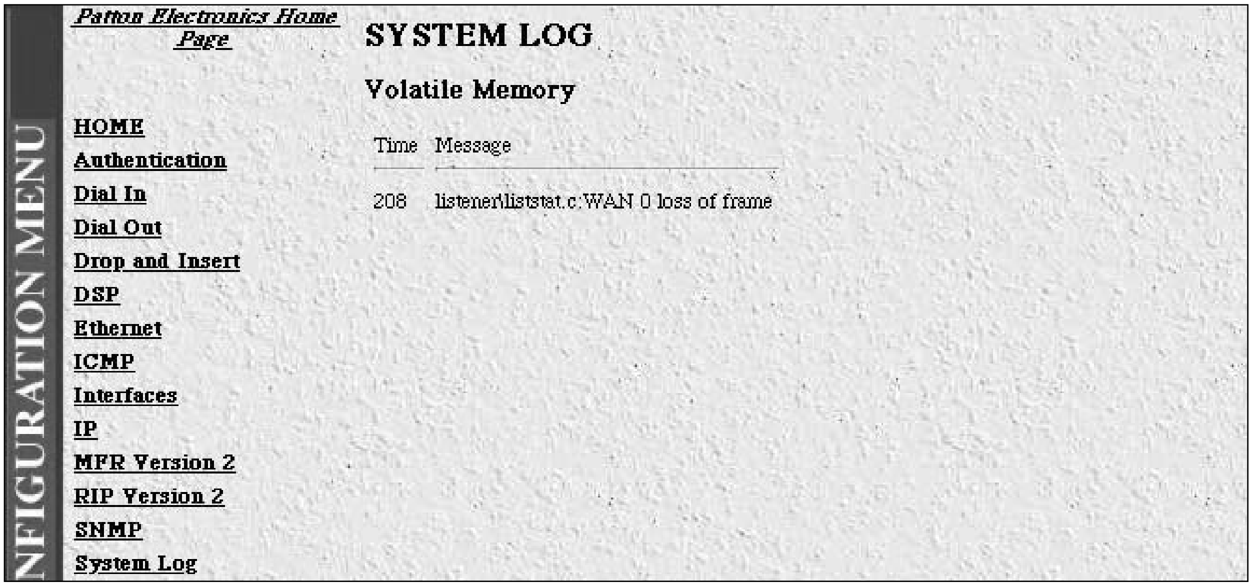
Maintain Flash Storage (syslogFlashClear) Setting this variable to syslogFlashClear will cause the erasing of any system messages which have been saved in the Flash. On reading this variable will indicate if the syslog Flash is rejecting messages because it is full.

syslogFlashOK(0),
syslogFlashFull(1),
syslogFlashClear(2)

System Log (Volatile Memory)

The System Log - Volatile Memory screen shows timestamp and stored system log message information. To reach this screen, select Volatile Memory from the main System Log screen (See Figure A-56, below).

Figure A-56 System Log - Volatile Memory



SYSTEM LOG

Volatile Memory

```
Time  Message
208   listener\liststat.c:WAN 0 loss of frame
```

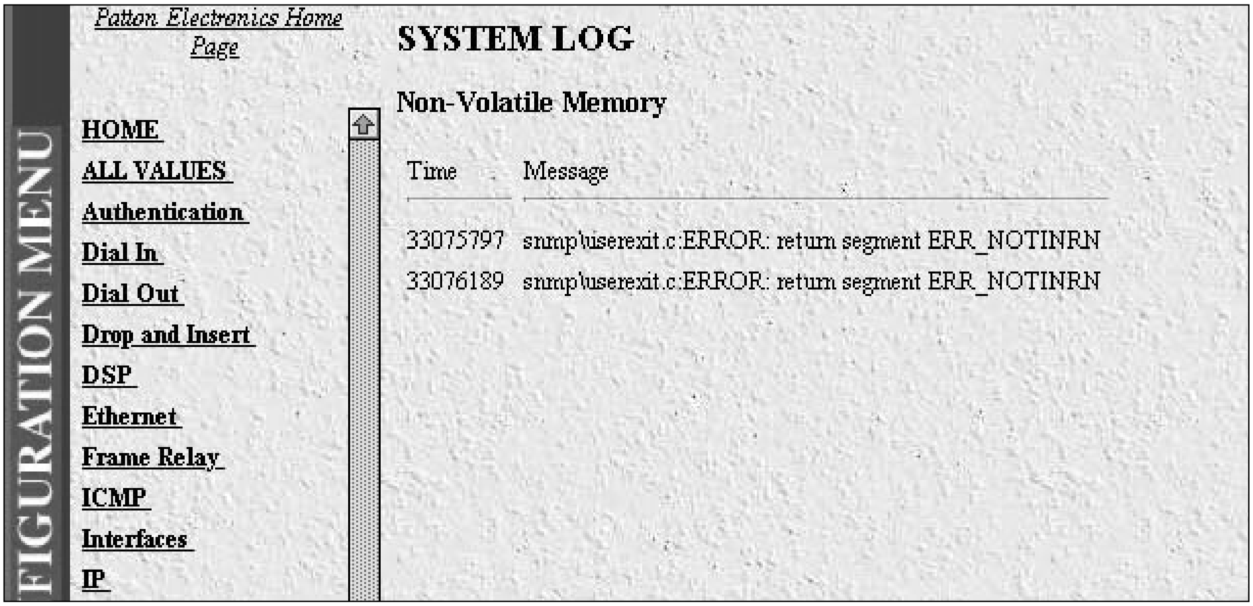
Time (slTick) The time stamp in 100ms intervals of the stored message.

Message (slMessage) Stored system log message.

System Log (Non-Volatile Memory)

The System Log - Non-Volatile screen shows non-volatile RAM messages for each 100ms time stamp. To reach this screen, select Non-Volatile Memory from the main System Log screen (See Figure A-57, below).

Figure A-57 System Log - Non-Volatile Memory



SYSTEM LOG

Non-Volatile Memory

```
Time       Message
33075797   snmp\userexit.c:ERROR: return segment ERR_NOTINRN
33076189   snmp\userexit.c:ERROR: return segment ERR_NOTINRN
```

Time (slfTick) The time stamp in 100ms intervals of the stored message.

Message (slfMessage) Stored system log message.

T1/E1 Link

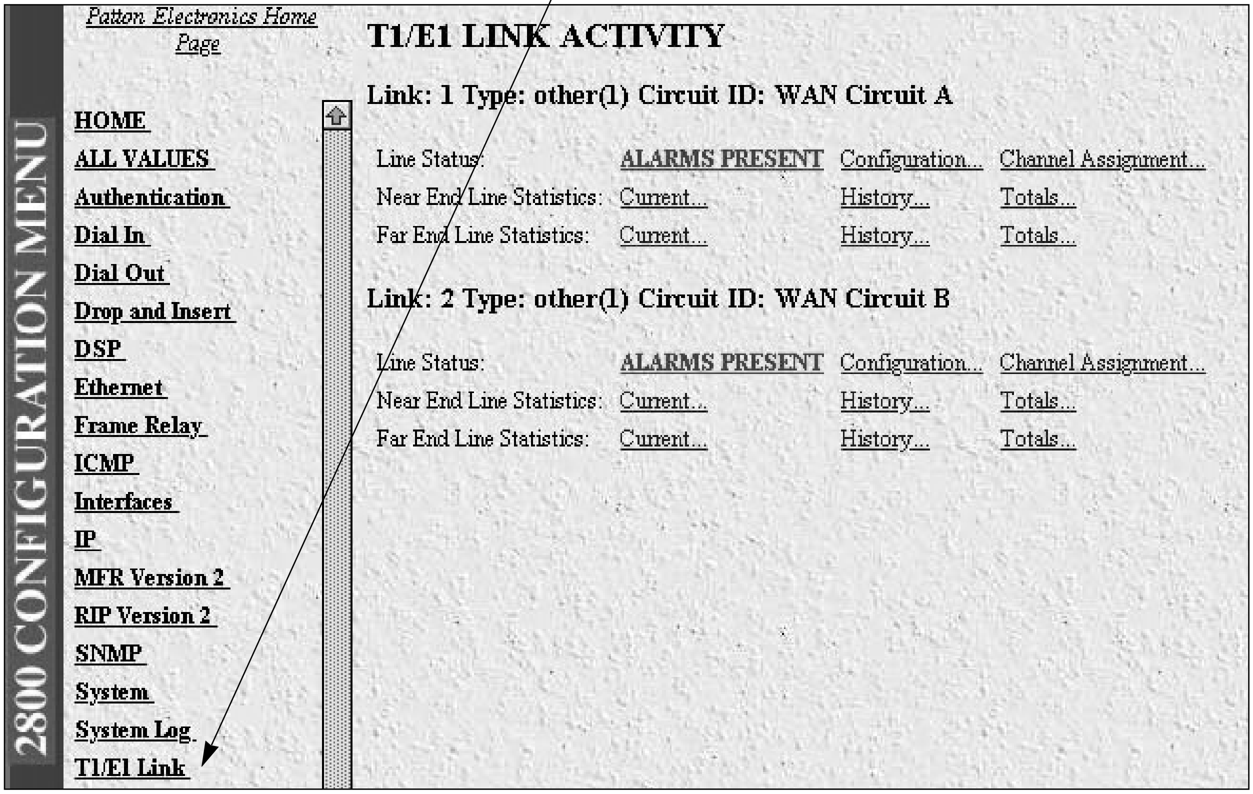
The T1/E1 Link Section shows the configuration of the T1/E1 Interface, and reports statistics on the quality of the T1/E1 connection. The statistics listed in this section correspond directly to statistics listed in RFC 1406 - Definitions of Managed Objects for the DS1 and E1 Interface Types. The T1/E1 Link Activity Page has three main sections that display the following T1/E1 parameters:

1. **Line Status:** shows the configuration of the T1/E1 Interface ands service provided on each user time slot.
2. **Near End Line Statistics:** show error statistics collected from the near end of the T1/E1 line.
3. **Far End Line Statistics:** show statistics collected from the far end T1/E1 line. Far End Line Statistics may be used by devices which use of the Facility Data Link (FDL)

These sections are described below.

To reach the T1/E1 Link Activity page, select T1/E1 Link from the 2800 Configuration Menu. (see Figure A-58, below)). Following Figure A-58 are descriptions for each variable on this page.

Figure A-58. T1/E1 Link Activity Main Screen



T1/E1 LINK ACTIVITY

Link: 1 Type: other(1) Circuit ID: WAN Circuit A

Line Status:	ALARMS PRESENT	Configuration...	Channel Assignment...
Near End Line Statistics:	Current...	History...	Totals...
Far End Line Statistics:	Current...	History...	Totals...

Link: 2 Type: other(1) Circuit ID: WAN Circuit B

Line Status:	ALARMS PRESENT	Configuration...	Channel Assignment...
Near End Line Statistics:	Current...	History...	Totals...
Far End Line Statistics:	Current...	History...	Totals...

The following variables are also shown on the main T1/E1 Link screen:

Link (dsx1LineIndex) This object is the identifier of a DS1 Interface on a managed device. If there is an **ifEntry** that is directly associated with this and only this DS1 interface, it should have the same value as **ifIndex**. Otherwise, the value exceeds **ifNumber**, and is a unique identifier following this rule: inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g.), network side with odd numbers.

Type (dsx1LineType) This variable indicates the variety of DS1 Line implenting this circuit. The type of circuit affects the number of bits per second that the circuit can reasonably carry, as well as the interpretation of the usage and error statistics. The values, in sequence, describe:

dsx1ESF	Extended Superframe DS1
dsx1D4	AT&T D4 format DS1
dsx1E1	Based on CCITT/ITU G.704 without CRC
dsx1E1-CRC	Based on CCITT/ITU G.704 with CRC
dsx1E1-MF	Based on CCITT/ITU G.704 with TS16 multiframing, w/o CRC
dsx1E1-CRC-MF	Based on CCITT/ITU G.704 with TS16 multiframing, w/ CRC

Circuit ID (dsx1CircuitIdentifier) This variable contains the transmission vendor's circuit identifier, for the purpose of facilitating troubleshooting.

Line Status (dsx1LineStatus) This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarm' information.

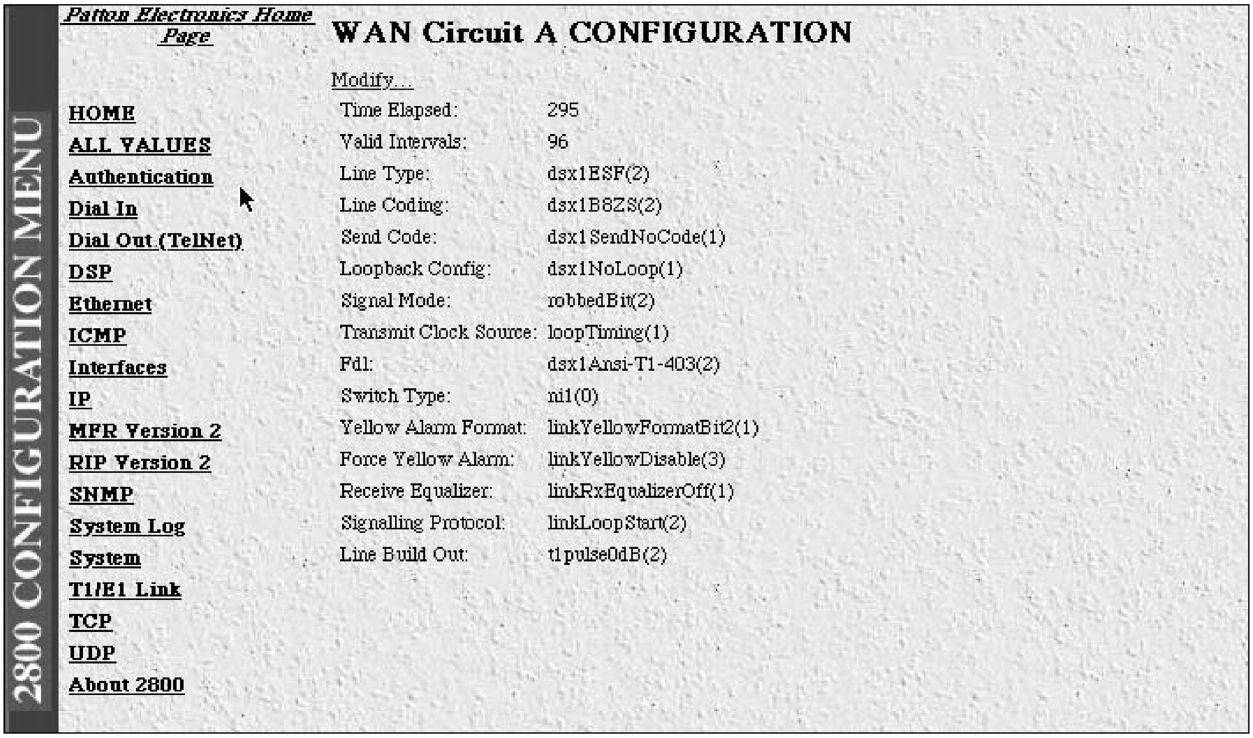
The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm should be set if and only if no other flag is set. If the dsx1LoopbackState bit is set, the loopback in effect can be determined from the dsx1LoopbackConfig object.

1	A**dsx1NoAlarm**	No Alarm Present
2	**dsx1RcvFarEndLOF**	Far end LOF (a.k.a., Yellow Alarm)
4	**dsx1XmtFarEndLOF**	Near end sending LOF Indication
8	**dsx1RcvAIS**	Far end sending AIS
16	**dsx1XmtAIS**	Near end sending AIS
32	**dsx1LossOfFrame**	Near end LOF (a.k.a., Red Alarm)
64	**dsx1LossOfSignal**	Near end Loss Of Signal
128	**dsx1LoopbackState**	Near end is looped
256	**dsx1T16AIS**	E1 TS16 AIS
512	**dsx1RcvFarEndLOMF**	Far End Sending TS16 LOMF
1024	**dsx1XmtFarEndLOMF**	Near End Sending TS16 LOMF
2048	**dsx1RcvTestCode**	Near End detects a test code
4096	**dsx1OtherFailure**	any line status not defined here"

Line Status (Configuration)

Select **Line Status-Configuration** from the main T1/E1 Link Activity screen to display general information about the DS1 interface. This general information includes the type of line (i.e. D4 Superframe or Extended Superframe), amount of time intervals passed, and kind of line coding (i.e. B8ZS or AMI). Figure A-59 shows the Circuit Configuration Screen for a typical ESF connection. Following Figure A-59 are descriptions for each variable on this page.

Figure A-59. Circuit Activity



WAN Circuit A CONFIGURATION

```
Time Elapsed:            295
Valid Intervals:         96
Line Type:               dsx1ESF(2)
Line Coding:             dsx1B8ZS(2)
Send Code:               dsx1SendNoCode(1)
Loopback Config:         dsx1NoLoop(1)
Signal Mode:             robbedBit(2)
Transmit Clock Source:   loopTiming(1)
Fdl:                     dsx1Ansi-T1-403(2)
Switch Type:             ni1(0)
Yellow Alarm Format:     linkYellowFormatBit2(1)
Force Yellow Alarm:      linkYellowDisable(3)
Receive Equalizer:       linkRxEqualizerOff(1)
Signalling Protocol:     linkLoopStart(2)
Line Build Out:          t1pulse0dB(2)
```

Time Elapsed (dsx1TimeElapsed) The number of seconds that have elapsed since the beginning of the current error-measurement period.

Valid Intervals (dsx1ValidIntervals) The number of previous intervals for which valid data was collected. The value will be 96 unless the interface was brought on-line within the last 24 hours, in which case the value will be the number of complete 15 minute intervals the since interface has been online.

Line Type (dsx1LineType) Type (dsx1LineType) This variable indicates the variety of DS1 Line implenting this circuit. The type of circuit affects the number of bits per second that the circuit can reasonably carry, as well as the interpretation of the usage and error statistics. The values, in sequence, describe:

other(1)	
dsx1ESF(2)	Extended Superframe DS1
dsx1D4(3)	AT&T D4 format DS1
dsx1E1(4)	Based on CCITT/ITU G.704 without CRC
dsx1E1-CRC(5)	Based on CCITT/ITU G.704 with CRC
dsx1E1-MF(6)	Based on CCITT/ITU G.704 with TS16 multiframing, w/o CRC
dsx1E1-CRC-MF(7)	Based on CCITT/ITU G.704 with TS16 multiframing, w/ CRC

Line Coding (dsx1LineCoding) This variable describes the variety of Zero Code Suppression used on the link, which in turn affects a number of its characteristics.

dsx1JBZS(1) Jammed Bit Zero Suppression, in which the AT&T specification of at least one pulse every 8 bit periods is literally implemented by forc ing a pulse in bit 8 of each channel. Thus, only seven bits per channel, or 1.344 Mbps, is available for data.

dsx1B8ZS (2) The use of a specified pattern of normal bits and bipolar violations which are used to replace a sequence of eight zero bits.

dsx1HDB3(3)

dsx1ZBTSI(4) May use dsx1ZBTSI, or Zero Byte Time Slot Interchange.

dsx1AMI(5) refers to a mode wherein no zero code suppression is present and the line encoding does not solve the problem directly. In this application, the higher layer must provide data which meets or exceeds the pulse density requirements, such as inverting HDLC data.

other(6)

Send Code (dsx1SendCode) This variable indicates what type of code is being sent across the DS1 interface by the device. The values mean:

dsx1SendNoCode(1)	Sending looped or normal data
dsx1SendLineCode(2)	Sending a request for a line loopback
dsx1SendPayloadCode(3)	Sending a request for a payload loopback
dsx1SendResetCode(4)	Sending a loopback termination request
dsx1SendQRS(5)	Sending a Quasi-Random Signal (QRS) test pattern
dsx1Send511Pattern(6)	Sending a 511 bit fixed test pattern
dsx1Send3in24Pattern(7)	Sending a fixed test pattern of 3 bits set in 24
dsx1SendOtherTestPattern(8)	Sending a test pattern other than those described by this object.

Loopback Config (dsx1LoopbackConfig) This variable represents the loopback configuration of the DS1 interface. Agents supporting read/write access should return badValue in response to a requested loopback state that the interface does not support. The values mean:

dsx1NoLoop(1)	Not in the loopback state. A device that is not capable of performing a loopback on the interface shall always return this as it's value.
dsx1PayloadLoop(2)	The received signal at this interface is looped through the device. Typically the received signal is looped back for re-transmission after it has passed through the device's framing function.
dsx1LineLoop(3)	The received signal at this interface does not go through the device (minimum penetration) but is looped back out.
dsx1OtherLoop(4)	Loopbacks that are not defined here."

Signal Mode (dsx1SignalMode)

none(1)	indicates that no bits are reserved for signaling on this channel.
robbedBit(2)	indicates that T1 Robbed Bit Signaling is in use.
bitOriented(3)	indicates that E1 Channel Associated Signaling is in use.
messageOriented(4)	indicates that Common Channel Signaling is in use either on channel 16 of an E1 link or channel 24 of a T1.

Transmit Clock Source (dsx1TransmitClockSource) The source of Tranmit Clock.

loopTiming(1) indicates that the recovered receive clock is used as the transmit clock.
localTiming(2) indicates that a local clock source is used.
throughTiming(3) indicates that recovered receive clock from another interface is used as the transmit clock.

Fdl (dsx1Fdl) This bitmap describes the use of the facilities data link, and is the sum of the capabili ties:

other(1) indicates that a protocol other than one following is used.
dsx1Ansi-T1-403(2) refers to the FDL exchange recommended by ANSI.
dsx1Att-54016(3) refers to ESF FDL exchanges.
dsx1Fdl-none(4) indicates that the device does not use the FDL.

Switch Type (linkIsdnSwitchType) This object allows the selection of the ISDN variations on the ISDN protocol depending on the switch manufacturer which we are connected to.

ni1(0),
dms(1),
att(2),
net5(3),
ts014(4),
ins1500(5)

Yellow Alarm Format (linkYellowFormat) This variable identifies which standard will be used to transmit and identify the Yellow Alarm.

link YellowFormatBit2(1) Bit-2 equal zero in every channel
YellowFormatDL(2) FF00 pattern in the Data Link
YellowFormatFrame12FS(3) FS bit of frame 12"

Force Yellow Alarm (linkYellowForce) This variable identifies which standard will be used to transmit and identify the Yellow Alarm.

linkYellowAuto Do NOT force the transmission of a yellow alarm. But, yellow alarm may be automatically transmitted.
linkYellowOn Force the transmission of a yellow alarm even if the received signal is in frame.
linkYellowDisable Do NOT transmit a yellow alarm even if the received signal is out of frame.

Receive Equalizer (linkRxEqualizer) This variable determines the equalization used on the received signal. Long haul signals should have the equalization set for more. Short haul signals require less equalization.

linkRxEqualizer6dB(1)
linkRxEqualizer18dB(2)

Signalling Protocol (linkSignalling) This variable determines which robbed bit signalling technique is used. The techniques designated OFFICE are used to simulate the central office site. These allow back to back connection of Model 2800s.

linkGroundStart(1),
linkLoopStart(2),
linkOfficeGroundStart(3),
linkOfficeLoopStart(4),
linkMFR2(5)

Line Build Out (linkLineBuildOut) This variable is used in T1 applications to adjust the T1 pulse shape at the cross connect point. The user should select the enumeration which best represents the amount of cable between the unit and the cross connect point

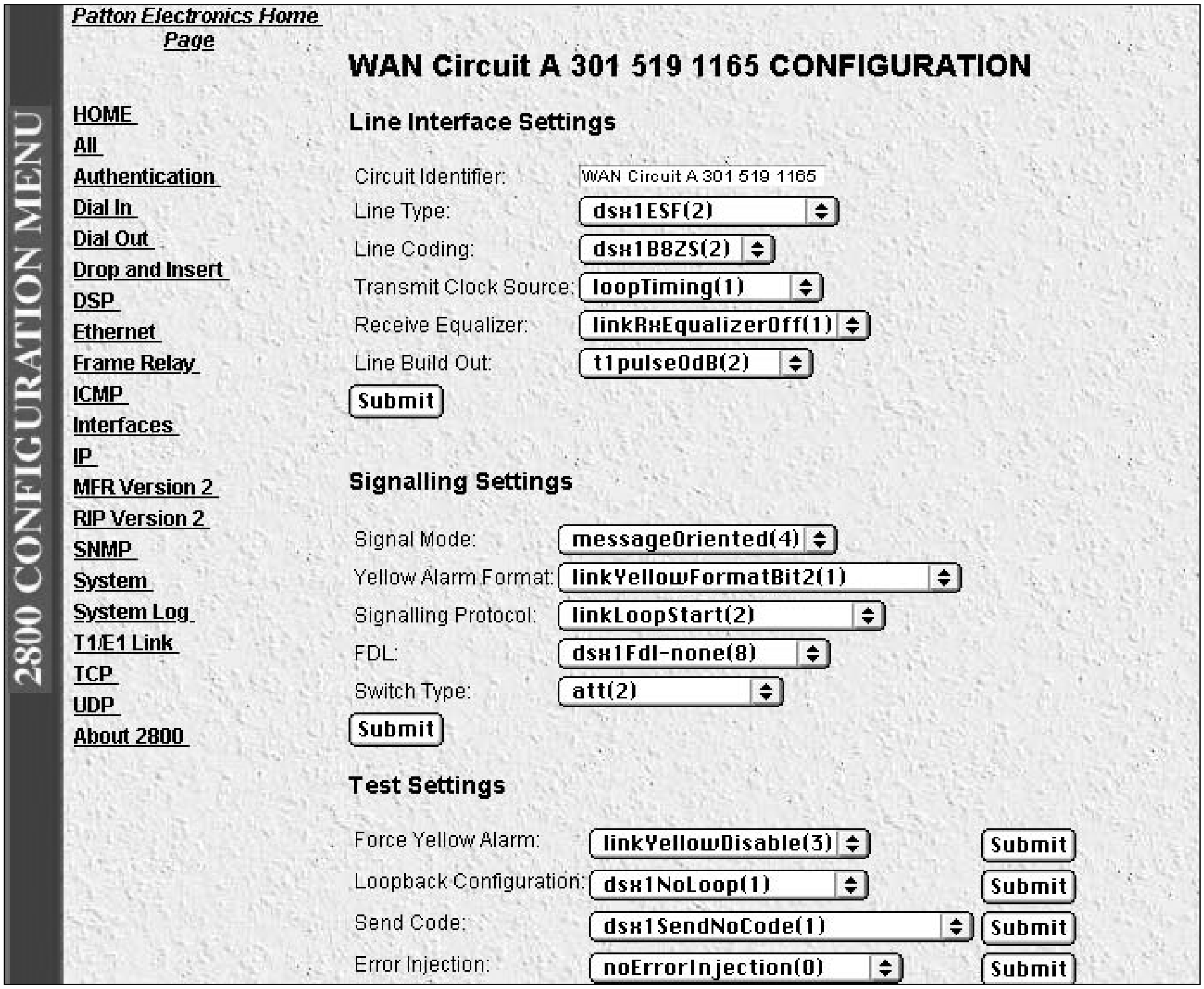
cable0meters(1)
cable25meters(2)
cable55meters(3)
cable85meters(4)
cable115meters(5)
cable145meters(6)
cable175meters(7)
cable18db(8)
e1pulse(9)

To change any of the above parameters, select Modify.

Line Status (Modify Line Interface, Signalling, and Test Settings)

To configure the T1/E1 Link, select Modify from the **Line Status - Configuration** screen. You may modify Line Interface Settings, Signalling Settings, Test Settings, and change the T1/E1 Pulse shapes. Figure A-60, below, shows Line Interface Settings and Signalling Settings.

Figure A-60. Line Status (Modify Line Interface, Signalling, and Test Settings)



WAN Circuit A 301 519 1165 CONFIGURATION

Line Interface Settings

Circuit Identifier: WAN Circuit A 301 519 1165
Line Type: dsx1ESF(2)
Line Coding: dsx1B8ZS(2)
Transmit Clock Source: loopTiming(1)
Receive Equalizer: linkRxEqualizerOff(1)
Line Build Out: t1pulse0dB(2)

Signalling Settings

Signal Mode: messageOriented(4)
Yellow Alarm Format: linkYellowFormatBit2(1)
Signalling Protocol: linkLoopStart(2)
FDL: dsx1Fdl-none(8)
Switch Type: att(2)

Test Settings

Force Yellow Alarm: linkYellowDisable(3)
Loopback Configuration: dsx1NoLoop(1)
Send Code: dsx1SendNoCode(1)
Error Injection: noErrorInjection(0)

Line Interface Settings

Circuit ID (dsx1CircuitIdentifier) This variable contains the transmission vendor's circuit identifier, for the purpose of facilitating troubleshooting.

Line Type (dsx1LineType) Type (dsx1LineType) This variable indicates the variety of DS1 Line implenting this circuit. The type of circuit affects the number of bits per second that the circuit can reasonably carry, as well as the interpretation of the usage and error statistics. The values, in sequence, describe:

other(1)	
dsx1ESF(2)	Extended Superframe DS1
dsx1D4(3)	AT&T D4 format DS1
dsx1E1(4)	Based on CCITT/ITU G.704 without CRC
dsx1E1-CRC(5)	Based on CCITT/ITU G.704 with CRC
dsx1E1-MF(6)	Based on CCITT/ITU G.704 with TS16 multiframing, w/o CRC
dsx1E1-CRC-MF(7)	Based on CCITT/ITU G.704 with TS16 multiframing, w/ CRC

Line Coding (dsx1LineCoding) This variable describes the variety of Zero Code Suppression used on the link, which in turn affects a number of its characteristics.

dsx1JBZS(1) Jammed Bit Zero Suppression, in which the AT&T specification of at least one pulse every 8 bit periods is literally implemented by forc ing a pulse in bit 8 of each channel. Thus, only seven bits per channel, or 1.344 Mbps, is available for data.

dsx1B8ZS (2) The use of a specified pattern of normal bits and bipolar violations which are used to replace a sequence of eight zero bits.

dsx1HDB3(3)

dsx1ZBTSI(4) May use dsx1ZBTSI, or Zero Byte Time Slot Interchange.

dsx1AMI(5) refers to a mode wherein no zero code suppression is present and the line encoding does not solve the problem directly. In this application, the higher layer must provide data which meets or exceeds the pulse density requirements, such as inverting HDLC data.

other(6)

Transmit Clock Source (dsx1TransmitClockSource) The source of Tranmit Clock.

loopTiming(1) indicates that the recovered receive clock is used as the transmit clock.

localTiming(2) indicates that a local clock source is used.

throughTiming(3) indicates that recovered receive clock from another interface is used as the transmit clock.

Receive Equalizer (linkRxEqualizer) This variable determines the equalization used on the received signal. Long haul signals should have the equalization set for more. Short haul signals require less equalization.

linkRxEqualizerOff(1)
linkRxEqualizerOn(2)

Line Build Out (linkLineBuildOut) This variable is used in T1 applications to adjust the T1 pulse shape at the cross connect point. The user should select the enumeration which best represents the amount of cable between the unit and the cross connect point

triState (0)
e1pulse(1),
t1pulse0dB(2)
t1pulse-7dB(3)
t1pulse-15dB(4)

Signalling Settings

Signal Mode (dsx1SignalMode)

none(1)	indicates that no bits are reserved for signaling on this channel.
robbedBit(2)	indicates that T1 Robbed Bit Signaling is in use.
bitOriented(3)	indicates that E1 Channel Associated Signaling is in use.
messageOriented(4)	indicates that Common Channel Signaling is in use either on channel 16 of an E1 link or channel 24 of a T1.

Yellow Alarm Format (linkYellowFormat) This variable identifies which standard will be used to transmit and identify the Yellow Alarm.

link YellowFormatBit2(1)	Bit-2 equal zero in every channel
YellowFormatDL(2)	FF00 pattern in the Data Link
YellowFormatFrame12FS(3)	FS bit of frame 12"

Signalling Protocol (linkSignalling) This variable determines which robbed bit signalling technique is used. The techniques designated OFFICE are used to simulate the central office site. These allow back to back connection of Model 2800s.

linkGroundStart(1),
linkLoopStart(2),
linkOfficeGroundStart(3),
linkOfficeLoopStart(4),
linkMFR2(5)

FDL (dsx1FDL) This bitmap describes the use of the facilities data link, and is the sum of the capabilities:

other(1) indicates that a protocol other than one following is used.
dsx1Ansi-T1-403(2) refers to the FDL exchange recommended by ANSI.
dsx1Att-54016(3) refers to ESF FDL exchanges.
dsx1Fdl-none(4) indicates that the device does not use the FDL.

Switch Type (linkIsdnSwitchType) This object allows the selection of the ISDN variations on the ISDN protocol depending on the switch manufacturer which we are connected to.

ni1(0),
dms(1),
att(2),
net5(3),
ts014(4),
ins1500(5)

Test Settings

Force Yellow Alarm (linkYellowForce) This variable identifies which standard will be used to transmit and identify the Yellow Alarm.

linkYellowAuto Do NOT force the transmission of a yellow alarm. But, yellow alarm may be automatically transmitted.
linkYellowOn Force the transmission of a yellow alarm even if the received signal is in frame.
linkYellowDisable Do NOT transmit a yellow alarm even if the received signal is out of frame.

Loopback Config (dsx1LoopbackConfig) This variable represents the loopback configuration of the DS1 interface. Agents supporting read/write access should return badValue in response to a requested loopback state that the interface does not support. The values mean:

dsx1NoLoop Not in the loopback state. A device that is not capable of performing a loopback on the interface shall always return this as it's value.
dsx1PayloadLoop The received signal at this interface is looped through the device. Typically the received signal is looped back for retransmission after it has passed through the device's framing function.
dsx1LineLoop The received signal at this interface does not go through the device (minimum penetration) but is looped back out.
dsx1OtherLoop Loopbacks that are not defined here."

Send Code (dsx1SendCode) This variable indicates what type of code is being sent across the DS1 interface by the device. The values mean:

dsx1SendNoCode	Sending looped or normal data
dsx1SendLineCode	Sending a request for a line loopback
dsx1SendPayloadCode	Sending a request for a payload loopback
dsx1SendResetCode	Sending a loopback termination request
dsx1SendQRS	Sending a Quasi-Random Signal (QRS) test pattern
dsx1Send511Pattern	Sending a 511 bit fixed test pattern
dsx1Send3in24Pattern	Sending a fixed test pattern of 3 bits set in 24
dsx1SendOtherTestPattern	Sending a test pattern other than those described by this object.

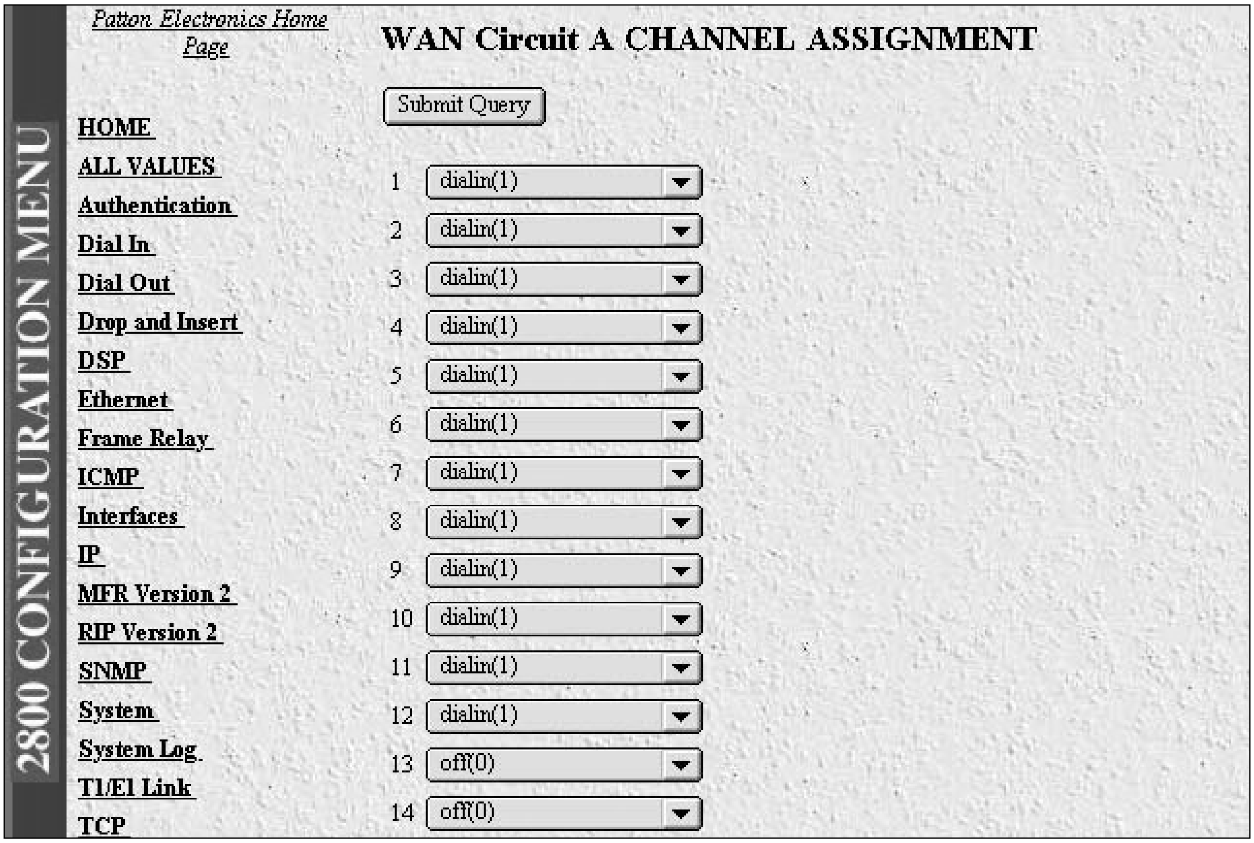
Error Injection (linkInjectError) Force an output error to see if other end detects it

noErrorInjection(0)
injectCRCerrorBurst(1)
injectLineErrorBurst(2)

Line Status (Slot/Channel Assignment0

T1/E1 lines are segmented into twenty-four (T1) or thirty (E1) individual channels or time slots. Select Line Status - Slot Assignment from the Main T1/E1 Link screen to display or modify how each of the T1/E1 time slots is defined (see Figure A-61, below).

Figure A-61. Slot/Channel Assignments



WAN Circuit A CHANNEL ASSIGNMENT

1 dialin(1)
2 dialin(1)
3 dialin(1)
4 dialin(1)
5 dialin(1)
6 dialin(1)
7 dialin(1)
8 dialin(1)
9 dialin(1)
10 dialin(1)
11 dialin(1)
12 dialin(1)
13 off(0)
14 off(0)

1 through 30(slotIndex) This object is the identifier of an entry in the slot table.

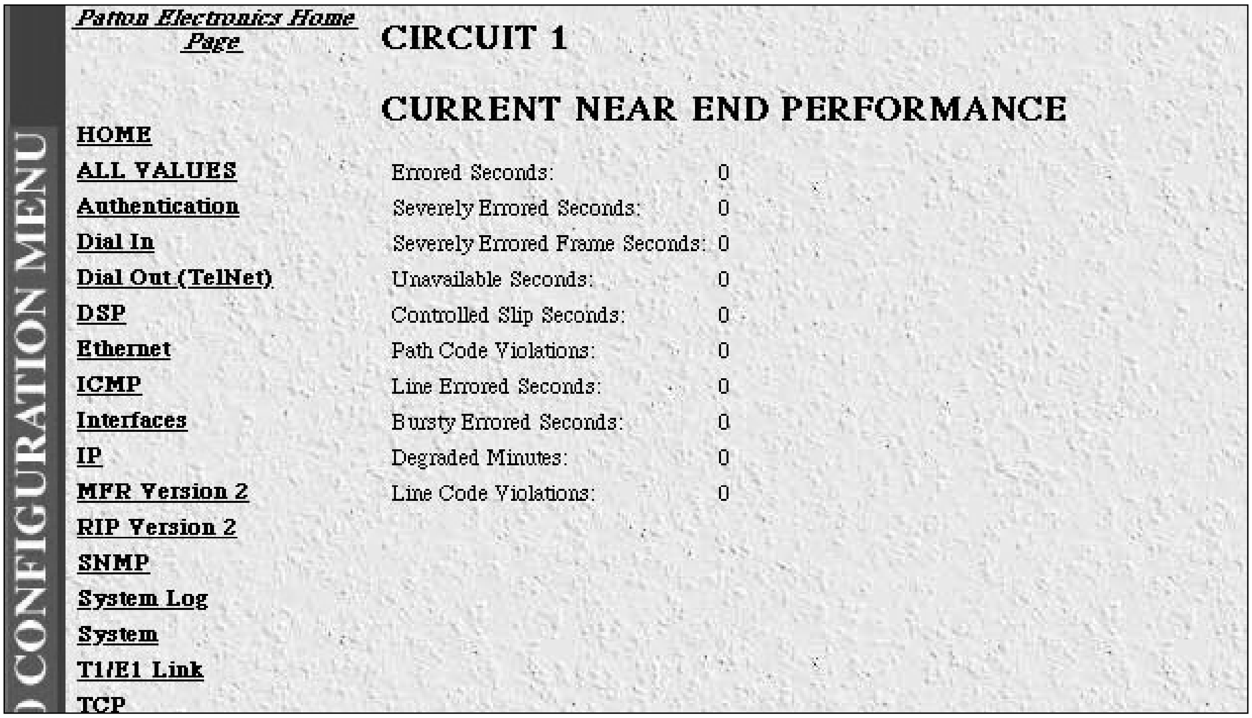
(slotFunction) This variable defines how the connection is made to each of the 24 or 30 T1/E1 time slots.

off(0)
dialin(1)
ppp(2)
frameRelay(3)
phoneBook(4)
fax(5)
IP(6)

Near End Line Statistics (Current)

Select Near End Line Statistics - Current to show line statistics for the current 15 minute interval (see Figure A-62, below).

Figure A-62. Near End Performance - Current Activity



CIRCUIT 1

CURRENT NEAR END PERFORMANCE

Errored Seconds:	0
Severely Errored Seconds:	0
Severely Errored Frame Seconds:	0
Unavailable Seconds:	0
Controlled Slip Seconds:	0
Path Code Violations:	0
Line Errored Seconds:	0
Bursty Errored Seconds:	0
Degraded Minutes:	0
Line Code Violations:	0

Errored Seconds (dsx1CurrentESs) The number of Errored Seconds, encountered by a DS1 interface in the current 15 minute interval.

Severely Errored Seconds (dsx1CurrentSESs) The number of Severely Errored Seconds encountered by a DS1 interface in the current 15 minute interval.

Severely Errored Frame Seconds (dsx1CurrentSEFSs) The number of Severely Errored Framing Seconds encountered by a DS1 interface in the current 15 minute interval.

Unavailable Seconds (dsx1CurrentUASs) The number of Unavailable Seconds encountered by a DS1 interface in the current 15 minute interval.

Controlled Slip Seconds (dsx1CurrentCSSs) The number of Controlled Slip Seconds encountered by a DS1 interface in the current 15 minute interval.

Path Code Violations (dsx1CurrentPCVs) The number of Path Coding Violations encountered by a DS1 interface in the current 15 minute interval.

Line Errored Seconds (dsx1CurrentLESs) The number of Line Errored Seconds encountered by a DS1 interface in the current 15 minute interval.

Bursty ErroredSeconds (dsx1CurrentBESs) The number of Bursty Errored Seconds (BESs) encountered by a DS1 interface in the current 15 minute interval.

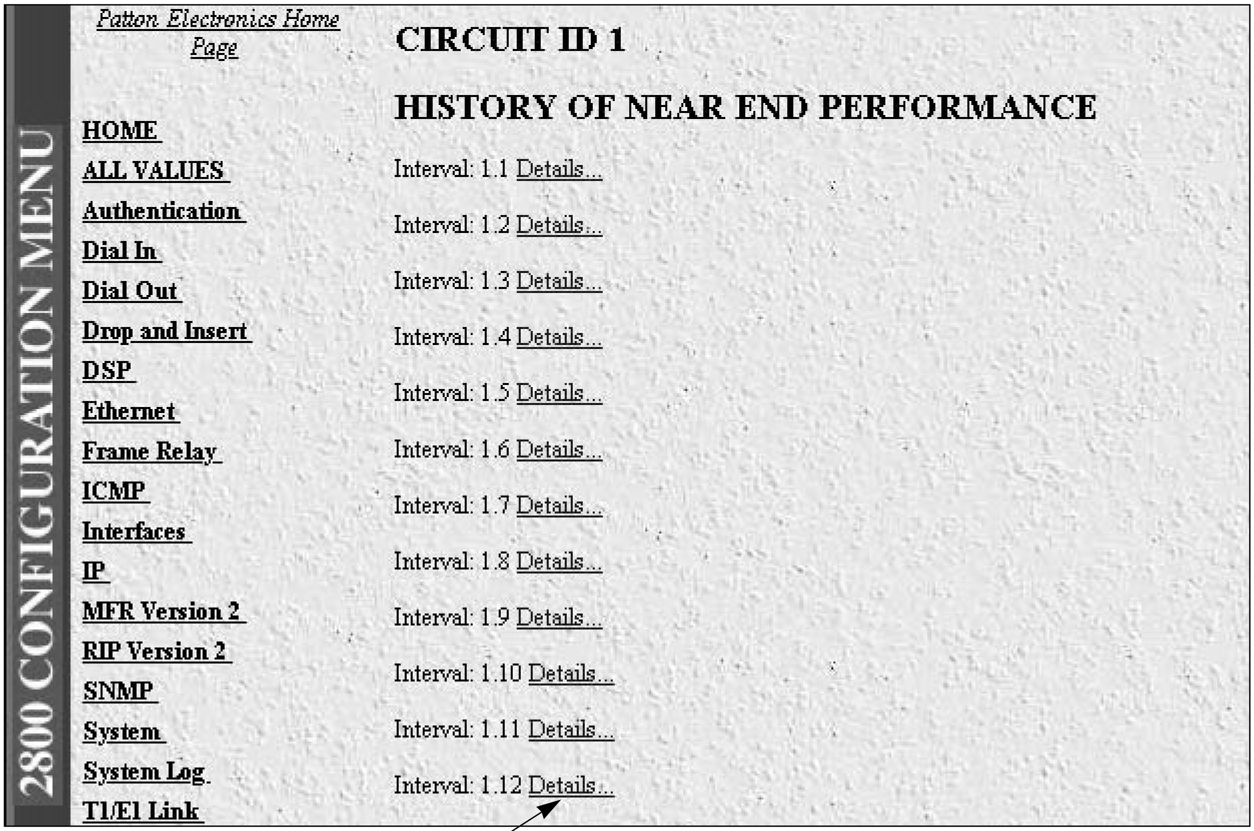
Degraded Minutes (dsx1CurrentDMs) The number of Degraded Minutes (DMs) encountered by a DS1 interface in the current 15 minute interval.

Line Code Violations (dsx1CurrentLCVs) The number of Line Code Violations (LCVs) encountered by a DS1 interface in the current 15 minute interval.

Near End Line Statistics (History)

Select **Near End Line Statistics - History** to show line statistics for earlier, completed 15 minute intervals (see Figure A-63, below).

Figure A-63. Near End Performance - Historical Activity



CIRCUIT ID 1

HISTORY OF NEAR END PERFORMANCE

Interval: 1.1 Details...

Interval: 1.2 Details...

Interval: 1.3 Details...

Interval: 1.4 Details...

Interval: 1.5 Details...

Interval: 1.6 Details...

Interval: 1.7 Details...

Interval: 1.8 Details...

Interval: 1.9 Details...

Interval: 1.10 Details...

Interval: 1.11 Details...

Interval: 1.12 Details...

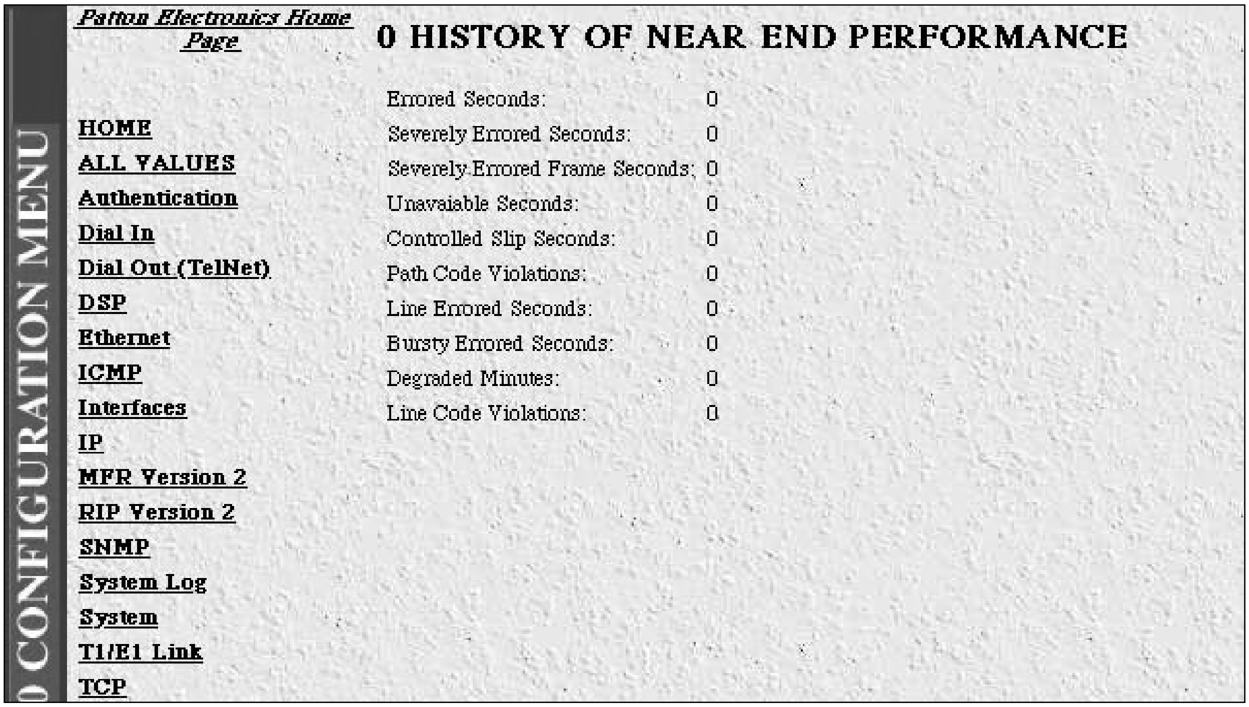
Interval (dsx1IntervalNumber) A number between 1 and 96, where 1 is the most recently completed 15 minute interval and 96 is the least recently completed 15 minutes interval (assuming that all 96 intervals are valid).

Choose Details to view historical information for any previous 15 minute interval T1/E1 link.

Near End Line Statistics (History Details)

Selecting Details on any of the intervals shown in Figure A-64 will display error statistics for that interval. The statistics shown have been collected for one of the previous 96, individual 15 minute intervals (see Figure A-64, below).

Figure A-64. Near End Performance - History - Details



0 HISTORY OF NEAR END PERFORMANCE

Errored Seconds:	0
Severely Errored Seconds:	0
Severely Errored Frame Seconds:	0
Unavaiable Seconds:	0
Controlled Slip Seconds:	0
Path Code Violations:	0
Line Errored Seconds:	0
Bursty Errored Seconds:	0
Degraded Minutes:	0
Line Code Violations:	0

Errored Seconds (dsx1IntervalESs) The number of Errored Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Severely Errored Seconds (dsx1IntervalSESs) The number of Severely Errored Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Severely Errored Frame Seconds (dsx1IntervalSEFSs) The number of Severely Errored Framing Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Unavailable Seconds (dsx1IntervalUASs) The number of Unavailable Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Controlled Slip Seconds (dsx1IntervalCSSs) The number of Controlled Slip Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Path Code Violations (dsx1IntervalPCVs) The number of Path Coding Violations encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Line Errored Seconds (dsx1IntervalLESs) The number of Line Errored Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Bursty ErroredSeconds (dsx1IntervalBESs) The number of Bursty Errored Seconds (BESs) encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

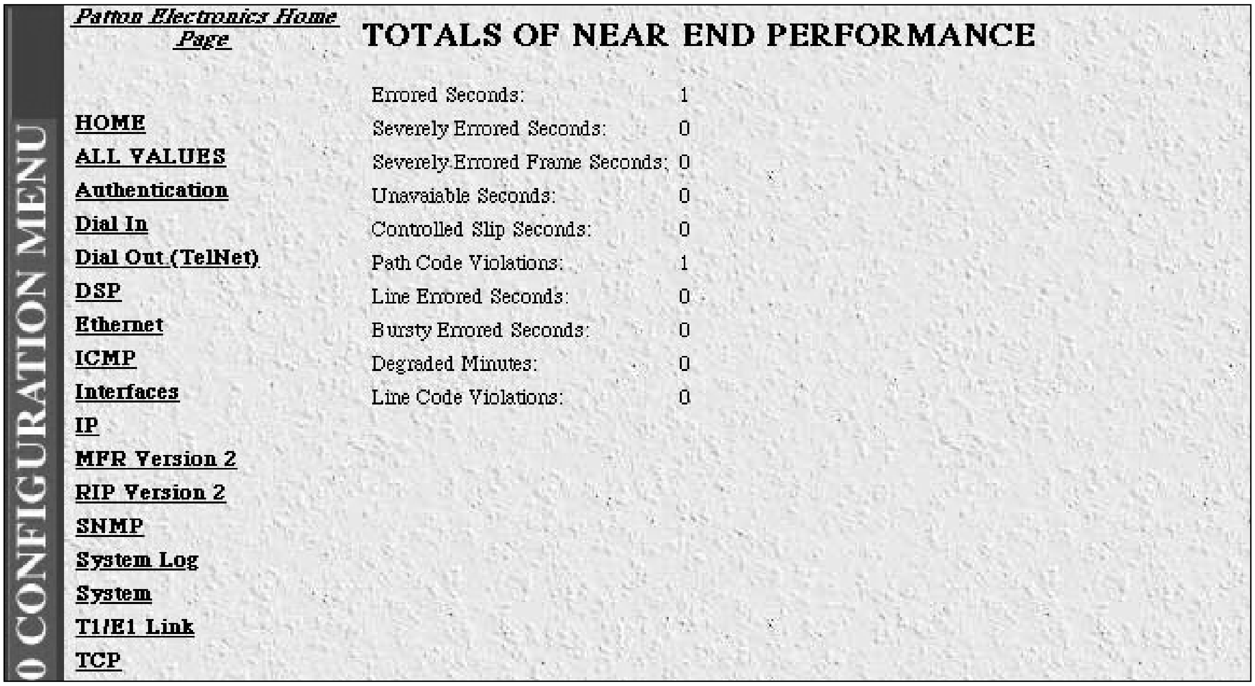
Degraded Minutes (dsx1IntervalDMs) The number of Degraded Minutes (DMs) encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Line Code Violations (dsx1IntervalLCVs) The number of Line Code Violations (LCVs) encountered by a DS1 interface in the current 15 minute interval.

Near End Line Statistics (Totals)

Select **Near End Line Statistics - Totals** to show sums of error statistics collected over the previous 24 hour interval (see Figure A-65, below).

Figure A-65. Near End Performance - Totals



TOTALS OF NEAR END PERFORMANCE

Errored Seconds:	1
Severely Errored Seconds:	0
Severely Errored Frame Seconds:	0
Unavaiable Seconds:	0
Controlled Slip Seconds:	0
Path Code Violations:	1
Line Errored Seconds:	0
Bursty Errored Seconds:	0
Degraded Minutes:	0
Line Code Violations:	0

Errored Seconds (dsx1TotalESs) The number of Errored Seconds encountered by a DS1 interface in the previous 24 hour interval.

Severely Errored Seconds (dsx1TotalSESs) The number of Severely Errored Seconds encountered by a DS1 interface in the previous 24 hour interval.

Severely Errored Frame Seconds (dsx1TotalSEFSs) The number of Severely Errored Framing Seconds encountered by a DS1 interface in the previous 24 hour interval.

Unavailable Seconds (dsx1TotalUASs) The number of Unavailable Seconds encountered by a DS1 interface in the previous 24 hour interval.

Controlled Slip Seconds (dsx1TotalCSSs) The number of Controlled Slip Seconds encountered by a DS1 interface in the previous 24 hour interval.

Path Code Violations (dsx1TotalPCVs) The number of Path Coding Violations encountered by a DS1 interface in the previous 24 hour interval.

Line Errored Seconds (dsx1TotalLESs) The number of Line Errored Seconds encountered by a DS1 interface in the previous 24 hour interval.

Bursty ErroredSeconds (dsx1TotalBESs) The number of Bursty Errored Seconds (BESs) encountered by a DS1 interface in the previous 24 hour interval.

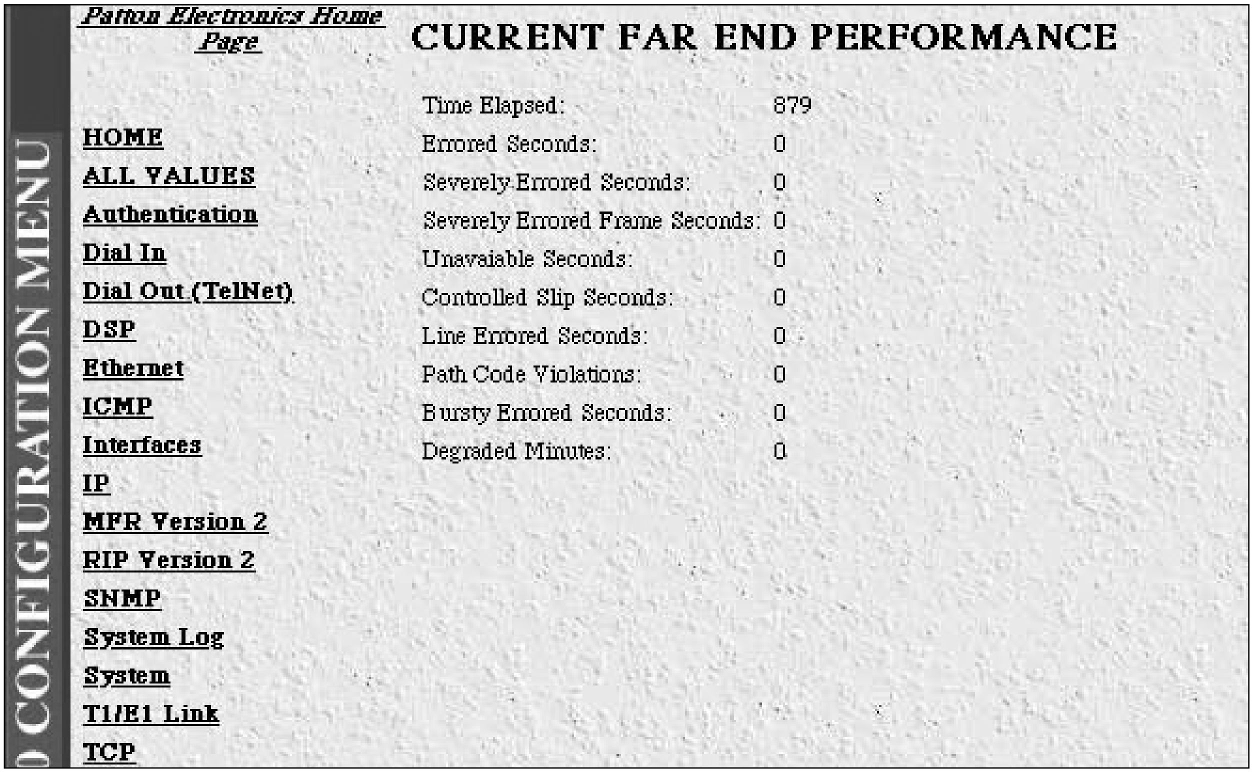
Degraded Minutes (dsx1TotalDMs) The number of Degraded Minutes (DMs) encountered by a DS1 interface in the previous 24 hour interval.

Line Code Violations (dsx1TotalLCVs) The number of Line Code Violations (LCVs) encountered by a DS1 interface in the current 15 minute interval.

Far End Line Statistics (Current)

Select Far End Line Statistics - Current to show far end statistics for the current 15 minute interval (see Figure A-66, below).

Figure A-66. Far End Performance - Current



CURRENT FAR END PERFORMANCE

Time Elapsed:	879
Errored Seconds:	0
Severely Errored Seconds:	0
Severely Errored Frame Seconds:	0
Unavaiable Seconds:	0
Controlled Slip Seconds:	0
Line Errored Seconds:	0
Path Code Violations:	0
Bursty Errored Seconds:	0
Degraded Minutes:	0

Time Elapsed (dsx1FarEndTimeElapsed) The number of seconds that have elapsed since the beginning of the far end current error-measurement period.

Errored Seconds (dsx1FarEndCurrentESs) The number of Far Far End Errored Seconds encountered by a DS1 interface in the current 15 minute interval.

Severely Errored Seconds (dsx1FarEnd CurrentSESs) The number of Far End Severely Errored Seconds encountered by a DS1 interface in the current 15 minute interval."

Severely Errored Frame Seconds (dsx1FarEndCurrentSEFSs) The number of Far End Severely Errored Framing Seconds encountered by a DS1 interface in the current 15 minute interval.

Unavailable Seconds (dsx1FarEndCurrentUASs) The number of Unavailable Seconds encountered by a DS1 interface in the current 15 minute interval.

Controlled Slip Seconds (dsx1FarEndCurrentCSSs) The number of Far End Controlled Slip Seconds encountered by a DS1 interface in the current 15 minute interval."

Line Errored Seconds (dsx1FarEndCurrentLESs) The number of Far End Line Errored Seconds encountered by a DS1 interface in the current 15 minute interval

Path Code Violations (dsx1FarEndCurrentPCVs) The number of Far End Path Coding Violations reported via the far end block error count encountered by a DS1 interface in the current 15 minute interval.

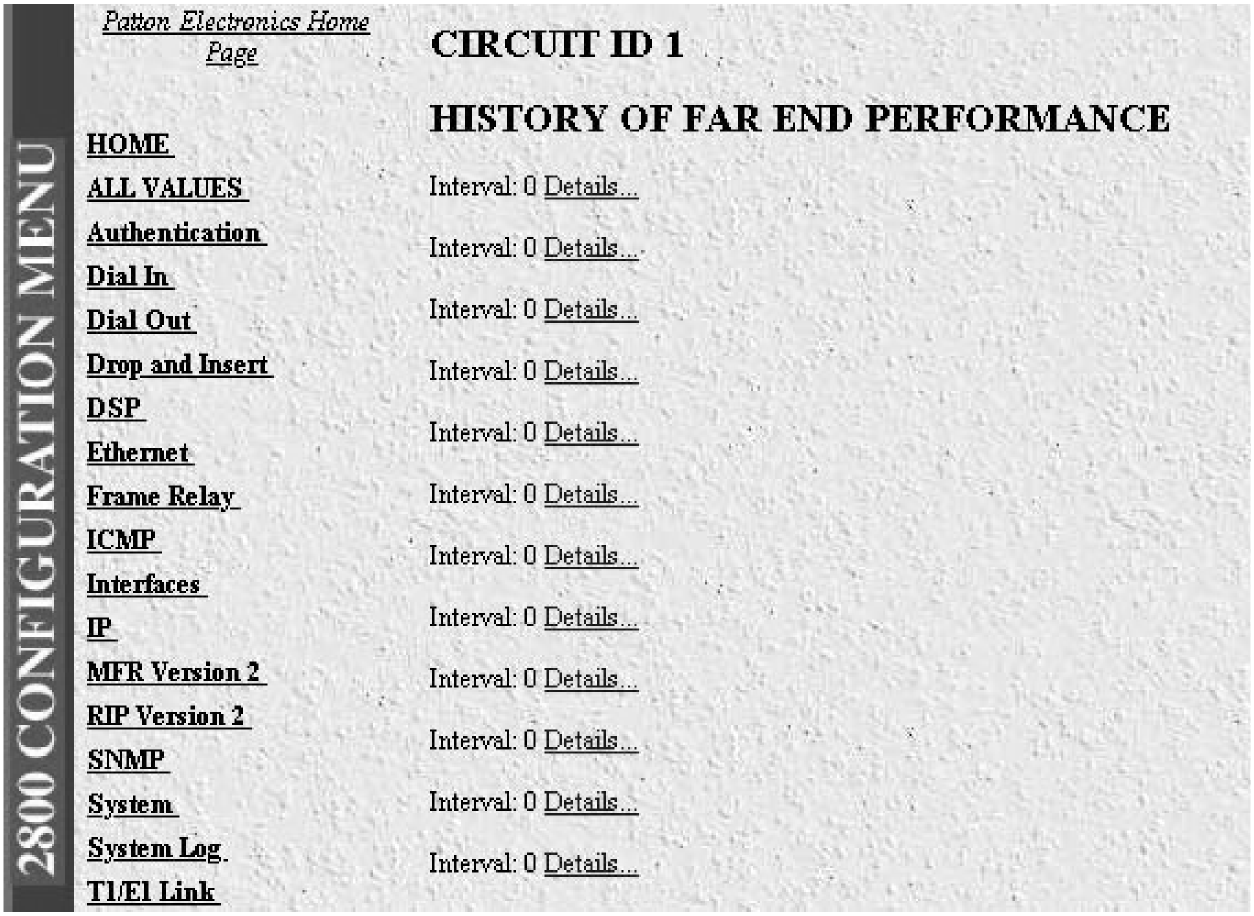
Bursty Errored Seconds (dsx1FarEndCurrentBESs) The number of Bursty Errored Seconds (BESs) encountered by a DS1 interface in the current 15 minute interval.

Degraded Minutes (dsx1FarEndCurrentDMs) The number of Degraded Minutes (DMs) encountered by a DS1 interface in the current 15 minute interval.

Far End Line Statistics (History)

Select **Far End Line Statistics - History** to show far end statistics for earlier, completed 15 minute intervals (see Figure A-67, below).

Figure A-67. Far End Performance - History



CIRCUIT ID 1

HISTORY OF FAR END PERFORMANCE

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

Interval: 0 Details...

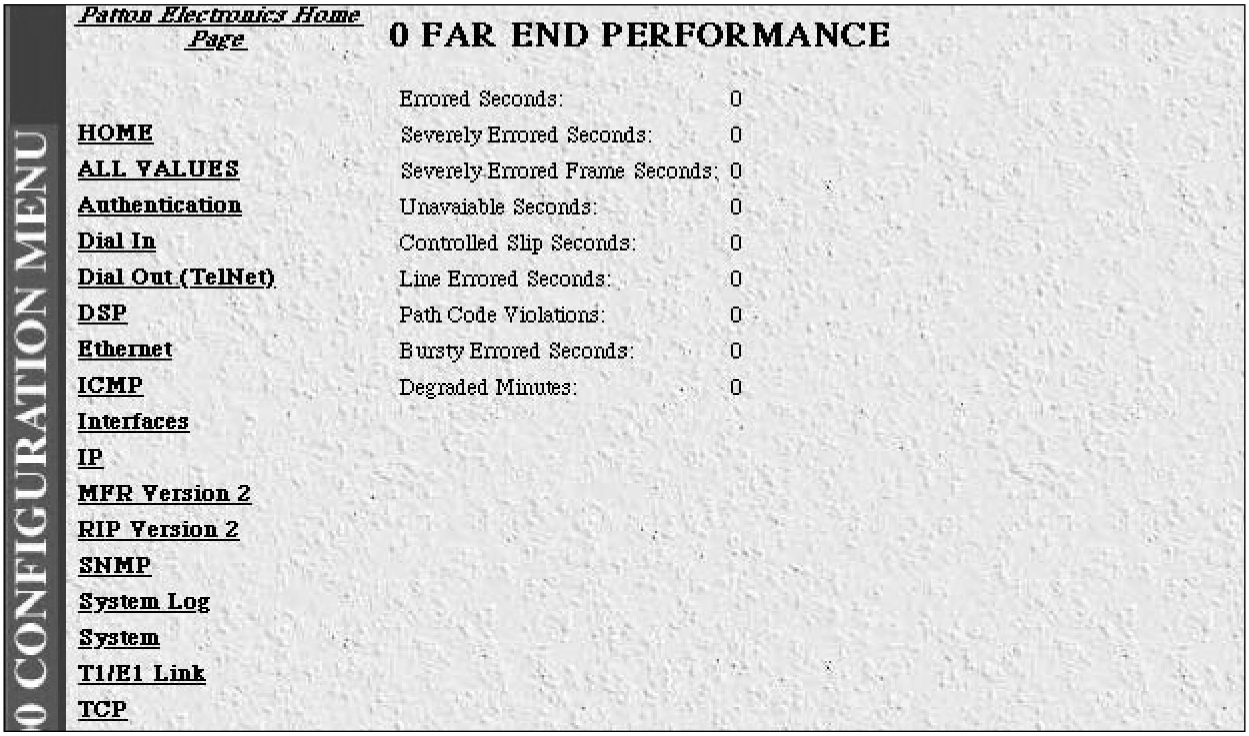
Far End Interval (dsx1FarEndIntervalNumber) A number between 1 and 96, where 1 is the most recently completed 15 minute interval and 96 is the least recently completed 15 minutes interval (assuming that all 96 intervals are valid).

Choose Details to view historical information for any previous 15 minute interval T1/E1 link.

Far End Line Statistics (History Details)

Selecting Details on any of the intervals shown in Figure A-22 will display error statistics for that interval. The far end statistics shown have been collected for one of the previous 96, individual 15 minute intervals (see Figure A-68, below).

Figure A-68. Far End Performance - History Details



0 FAR END PERFORMANCE

```
Errored Seconds:                   0
Severely Errored Seconds:          0
Severely Errored Frame Seconds:    0
Unavaiable Seconds:                0
Controlled Slip Seconds:           0
Line Errored Seconds:              0
Path Code Violations:              0
Bursty Errored Seconds:            0
Degraded Minutes:                  0
```

Errored Seconds (dsx1FarEndIntervalESs) The number of Far End Errored Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Severely Errored Seconds (dsx1FarEndIntervalSESs) The number of Far End Severely Errored Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Severely Errored Frame Seconds (dsx1FarEndIntervalSEFSs) The number of Far End Severely Errored Framing Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Unavailable Seconds (dsx1FarEndIntervalUASs) The number of Unavailable Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Controlled Slip Seconds (dsx1FarEndIntervalCSSs) The number of Far End Controlled Slip Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Path Code Violations (dsx1FarEndIntervalPCVs) The number of Far End Path Coding Violations encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Line Errored Seconds (dsx1FarEndIntervalLESs) The number of Far End Line Errored Seconds encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Bursty ErroredSeconds (dsx1FarEndIntervalBESs) The number of Far End Bursty ErroredSeconds (BESs) encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

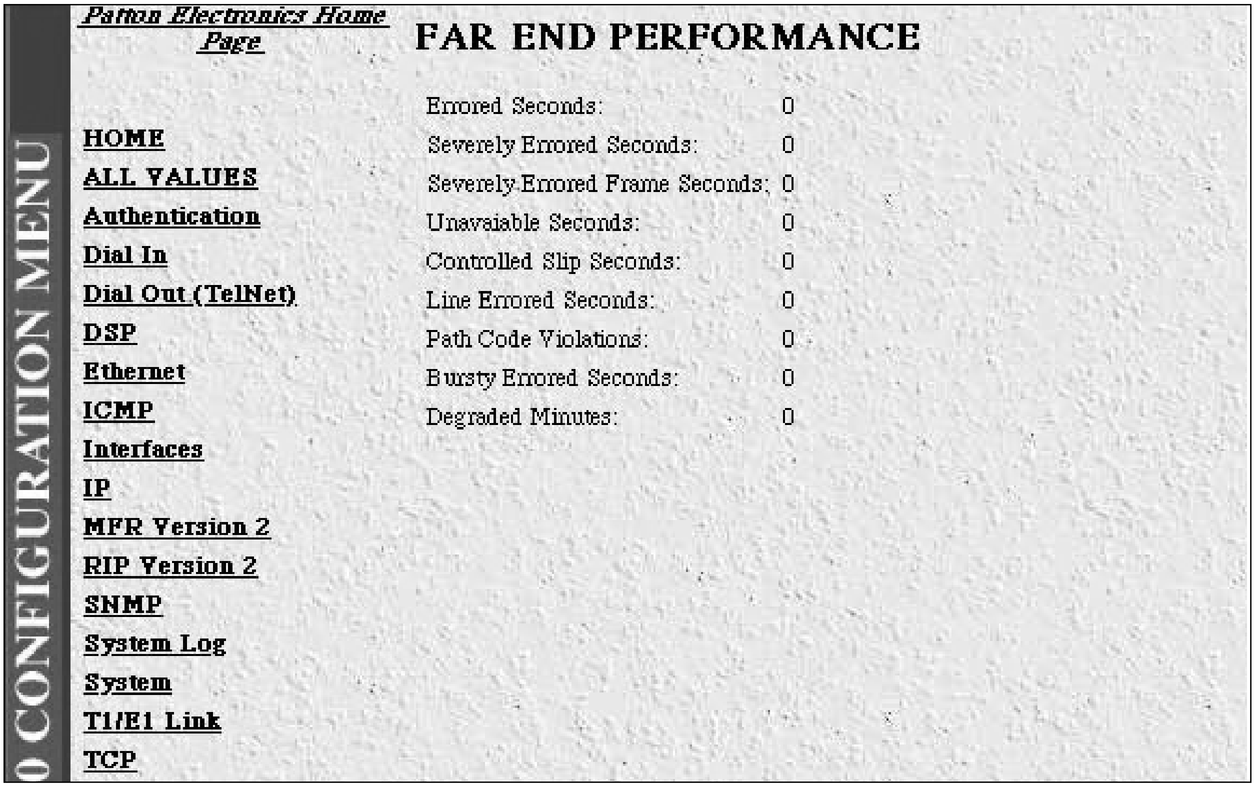
Degraded Minutes (dsx1FarEndIntervalDMs) The number of Far End Degraded Minutes (DMs) encountered by a DS1 interface in one of the previous 96, individual 15 minute, intervals.

Line Code Violations (dsx1FarEndIntervalLCVs) The number of Far End Line Code Violations (LCVs) encountered by a DS1 interface in the current 15 minute interval.

Far End Line Statistics - Totals

Select **Far End Line Statistics - Totals** to show sums of far end error statistics collected over the previous 24 hour interval (see Figure A-69, below).

Figure A-69. Far End Performance - Totals



FAR END PERFORMANCE

Errored Seconds:	0
Severely Errored Seconds:	0
Severely Errored Frame Seconds:	0
Unavaiable Seconds:	0
Controlled Slip Seconds:	0
Line Errored Seconds:	0
Path Code Violations:	0
Bursty Errored Seconds:	0
Degraded Minutes:	0

Errored Seconds (dsx1FarEndTotalESs) The number of Far End Errored Seconds encountered by a DS1 interface in the previous 24 hour interval."

Severly Errored Seconds (dsx1FarEndTotalSESs) The number of Far End Severely Errored Seconds encountered by a DS1 interface in the previous 24 hour interval.

Severely Errored Frame Seconds (dsx1FarEndTotalSEFSs) The number of Far End Severely Errored Framing Seconds encountered by a DS1 interface in the previous 24 hour interval.

Unavailable Seconds (dsx1FarEndTotalUASs) The number of Unavailable Seconds encountered by a DS1 interface in the previous 24 hour in-24 hour interval."

Controlled Slip Seconds (dsx1FarEndTotalCSSs) The number of Far End Controlled Slip Seconds encountered by a DS1 interface in the previous 24 hour interval.

Line Errored Seconds (dsx1FarEndTotalLESs) The number of Far End Line Errored Seconds encountered by a DS1 interface in the previous 24 hour interval."

Path Code Violations (dsx1FarEndTotalPCVs) The number of Far End Path Coding Violations reported via the far end block error count encountered by a DS1 interface in the previous 24 hour interval.

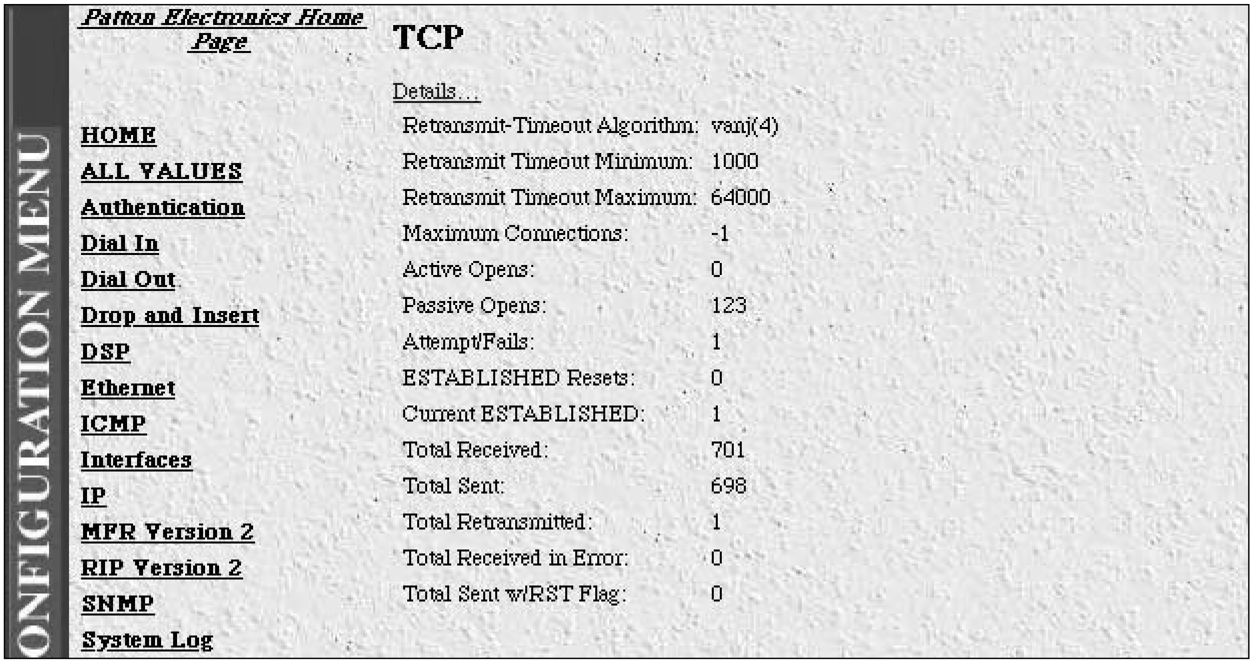
Bursty Errored Seconds (dsx1FarEndTotalBESs) The number of Bursty ErroredSeconds (BESs) encountered by a DS1 interface in the previous 24 hour interval.

Degraded Minutes (dsx1FarEndTotalDMs) The number of Degraded Minutes (DMs) encountered by a DS1 interface in the previous 24 hour interval."

TCP

Transmission Control Protocol (TCP) is the most widely used protocol among the TCP/IP suite. The 2800 provides management and statistical information on TCP. Detailed information regarding the SNMP MIB variables may be downloaded from ***RFC1213: Management Information Base for Network Management of TCP/IP-based internets:MIB-II***. Select TCP from the 2800 Configuration Menu to monitor TCP statistics. Following Figure A-70 are descriptiosn for each object on this page.

Figure A-70. TCP Main Screen



TCP

Details...

Retransmit-Timeout Algorithm:	vanj(4)
Retransmit Timeout Minimum:	1000
Retransmit Timeout Maximum:	64000
Maximum Connections:	-1
Active Opens:	0
Passive Opens:	123
Attempt/Fails:	1
ESTABLISHED Resets:	0
Current ESTABLISHED:	1
Total Received:	701
Total Sent:	698
Total Retransmitted:	1
Total Received in Error:	0
Total Sent w/RST Flag:	0

Retransmit-Timeout Algorithm (tcpRtoAlgorithm) The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.

Retransmit-Timeout Minimum (tcpRtoMin) The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.

Retransmit-Timeout Maximum (tcpRtoMax) The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.

Maximum Connections (tcpMaxConn) The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

Active Opens (tcpActiveOpens) The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

Passive Opens (tcpPassiveOpens) The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

Attempt/Fails (tcpAttemptFails) The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

ESTABLISHED Resets (tcpEstabResets) The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

Current ESTABLISHED (tcpCurrEstab) The number of TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT.

Total Received (tcpInSegs) The total number of segments received, including those received in error. This count includes segments received on currently established connections.

Total Sent (tcpOutSegs) The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

Total Retransmitted (tcpRetransSegs) The total number of segments retransmittedñthat is, the number of TCP segments transmitted containing one or more previously transmitted octets.

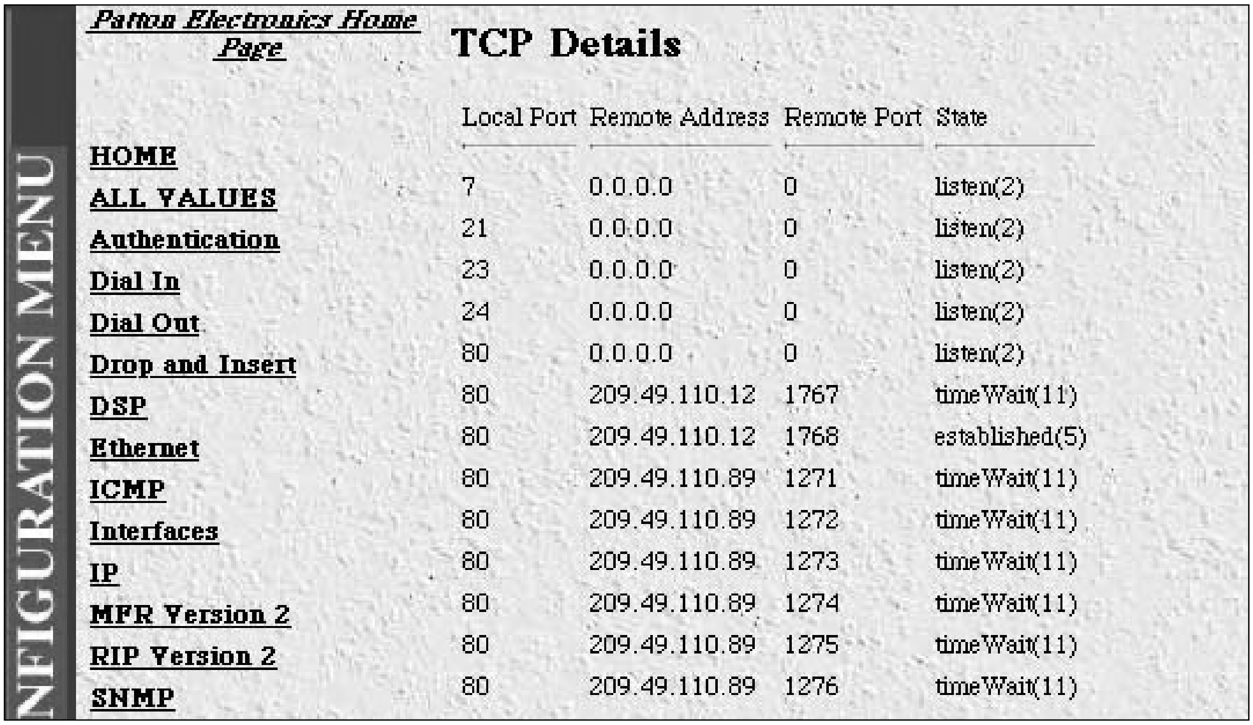
Total Received in Error (tcpInErrs) The total number of segments received in error (e.g., bad TCP checksums).

Total Sent w/RST Flag (tcpOutRsts) The number of TCP segments sent containing the RST flag.

TCP (Details)

From this screen you can view port details for remote and localTCP connections (See Figure 3.71, below). You must enable the Facility Data Link (FDL) object in the T1/E1 Link section to read remote TCP port connectons. To reach this screen, scroll down from the previous screen.

Figure A-71. TCP Details



TCP Details

Local Port	Remote Address	Remote Port	State
7	0.0.0.0	0	listen(2)
21	0.0.0.0	0	listen(2)
23	0.0.0.0	0	listen(2)
24	0.0.0.0	0	listen(2)
80	0.0.0.0	0	listen(2)
80	209.49.110.12	1767	timeWait(11)
80	209.49.110.12	1768	established(5)
80	209.49.110.89	1271	timeWait(11)
80	209.49.110.89	1272	timeWait(11)
80	209.49.110.89	1273	timeWait(11)
80	209.49.110.89	1274	timeWait(11)
80	209.49.110.89	1275	timeWait(11)
80	209.49.110.89	1276	timeWait(11)

Local Port (tcpConnLocalPort) The local port number for this TCP connection.

Remote Address (tcpConnRemAddress) The remote IP address for this TCP connection.

Remote Port (tcpConnRemPort) The remote port number for this TCP connection."

State (tcpConnState) The state of this TCP connection. The only value which may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to set this object to any other value.

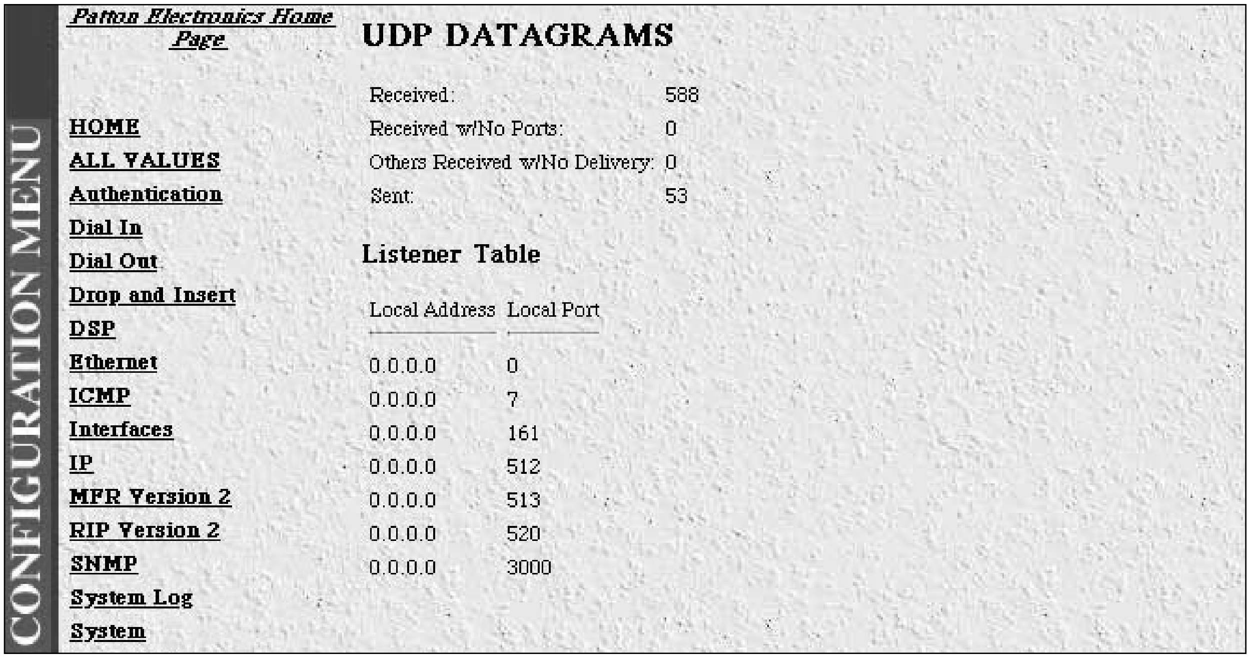
If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the TCB (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably).

closed(1),
listen(2),
synSent(3),
synReceived(4),
established(5),
finWait1(6),
finWait2(7),
closeWait(8),
lastAck(9),
closing(10),
timeWait(11),
deleteTCB(12)

UDP

User Datagram Protocol (UDP) is supported by the Patton 2800. Detailed information regarding the SNMP MIB variables can be found in ***RFC1213: Management Information Base for Network Management of TCP/IP-based internets:MIB-II***.. To manage and collect statistics on UDP, select UDP from the 2800 Configuration Menu (see Figure A-72, below). Following Figure A-72 are descriptions for each object on the screen.

Figure A-72 UDP Datagrams Main Screen



UDP DATAGRAMS

Received:	588
Received w/No Ports:	0
Others Received w/No Delivery:	0
Sent:	53

Listener Table

Local Address	Local Port
0.0.0.0	0
0.0.0.0	7
0.0.0.0	161
0.0.0.0	512
0.0.0.0	513
0.0.0.0	520
0.0.0.0	3000

Received (udpInDatagrams) The total number of UDP datagrams delivered to UDP users.

Received w/No Ports (udpNoPorts) The total number of received UDP datagrams for which there was no application at the destination port.

Others Received with No Delivery (udpInErrors) The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

Sent (udpOutDatagrams) The total number of UDP datagrams sent from this entity.

Listener Table (udpTable) A table containing UDP listener information.

Local Address (udpLocalAddress) The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.

Local Port (udpLocalPort) The local port number for this UDP listener.