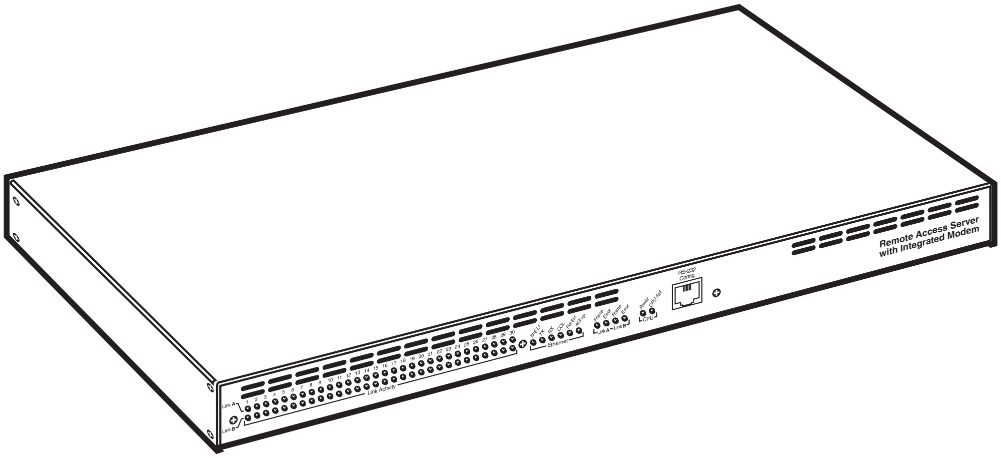
BLACK BOX®

NETWORK SERVICES

MAY 1999<br>
LRA2800A-12<br>
LRA2800A-24<br>
LRA2800A-30<br>
LRA2800A-48<br>
LRA2800A-60<br>
LRA2190A

# Remote Access Server with Integrated Modems



**CUSTOMER SUPPORT INFORMATION**

Order **toll-free** in the U.S. 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**<br>
FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**<br>
Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018<br>
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

## FEDERAL COMMUNICATIONS COMMISSION
## AND
## CANADIAN DEPARTMENT OF COMMUNICATIONS
## RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

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

*This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.*

*Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.*

## INSTRUCCIONES DE SEGURIDAD (Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

**TRADEMARKS**

The trademarks mentioned in this manual are the sole property of their owners.

## Additional References

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

### RFCs

You can use a Web browser to find online copies of the following Request for Comments (RFC) documents at this site: http//nic.mil/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.*

## CONTENTS

# 1. Specifications

## 1.1 Architecture

- 1,023 MIPS (Million Instructions per Second) maximum sustained performance via integrated RISC CPU
- Multiple DSPs (Digital Signal Processors)
- 4 MB Flash
- 8 MB DRAM, expandable to 32 MB
- Serial Connection: One RS-232 (RJ-45) configuration port
- System monitoring with “watchdog” automatic reset
- Self-test at power-up for all sub-systems

## 1.2 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
- Network loop diagnostics

## 1.3 LAN Connection

- 802.3 AUI and 10BASE-T Ethernet port with high-speed 32-bit LAN coprocessor and automatic polarity correction

## 1.4 Physical

- 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; (1) DB25 female and (1) RJ-45 802.3 Ethernet connection; (1) IEC-320 shrouded male power connector, dual independent cooling fans
- Compliance: FCC Part 15, Class A; FCC Part 68; UL 1950; Canadian cMET, Canadian CS-03, EMC Directive 89/336/EEC; Low Voltage Directive 73/23/EEC (EN60950); CTR-4; Year 2000 Compliant
- Environmental: Operating Temperature: 32 to 104 °F (0 to 40 °C); Operating Humidity: 5 to 90% noncondensing

- Power Supply: Internal Universal Input 90-260 VAC, 50/60/400 Hz, 35 watts, IEC-320 shrouded male connector
- Size: 1.75"H x 17"W x 8"D (4.4 x 43.2 x 20.3 cm)
- Weight: 4.5 lb. (2 kg)

## 1.5 Analog and Digital Modem Services

- Supports up to 30 concurrent dial-up connections, either analog (V.34+) or digital (K56flex™, V.90/, or ISDN)
- Modem modulations: V.90, 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

## 1.6 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

## 1.7 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 a proprietary 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 Remote Access Server parameters
- Built-in HTTP server for complete configuration and control using a standard Web browser

## 1.8 Security

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

# 2. Introduction

## 2.1 About this Manual

This manual is intended to be used by qualified systems administrators and network engineers to successfully configure the Remote Access Server with Integrated Modems. Knowledge of basic networking and routing concepts is assumed. The manual consists of five chapters and one appendix.

- **Chapter 1, Specifications,** lists technical specifications for the Server.
- **Chapter 2, Introduction** (this chapter), describes the Server, including product features, terminology descriptions, product applications, connections, and LED descriptions.
- **Chapter 3, Getting Started**, describes how the Server works, how to set and save initial operating parameters, and T1/E1/ISDN provisioning parameters.
- **Chapter 4, Configuring the PSTN Line Interface**, describes how to set up the Server's PSTN Line Interface.
- **Chapter 5, Configuring Authentication**, describes how to set up the Server's Local or RADIUS™ Authentication parameters.
- **Appendix, Using the Internal HTML Management Pages**, provides a description of the Server's internal HTTP/HTML management pages.

## 2.2 Documentation Conventions

**Bold Helvetica Text** describes configuration commands or parameters that you may enter or change to configure the Server.

**NOTE**

**Denotes important additional information.**

**WARNING**

**Means that a failure to take appropriate safety measures could result in physical injury.**

**CAUTION**

**Means that you should proceed with caution or should contact appropriate technicians. Failure to do so could result in damage or injury.**

**(snmpObject)** denotes SNMP or Enterprise MIB variables.

## 2.3 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 still growing fast, and 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 they need.

The Remote Access Server is designed to provide a second-wave access solution: a compact, software upgradable platform that allows dial-up access to Internet and intranet services, and has the flexibility to operate cost-effectively as a stand-alone or networked device.

## 2.4 Advantages of Digital Modem Technology

- Efficient and consistent performance—Because no signal information is lost, performance is repeatable.
- Migration path—Easily accommodated by *software* 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 means increased reliability.

## 2.5 The Remote Access Server with Integrated Modems

The Remote Access Server simulaneously 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 Server incorporates channel-bank, terminal-server, router, and modem functionality in a self-contained, compact package.

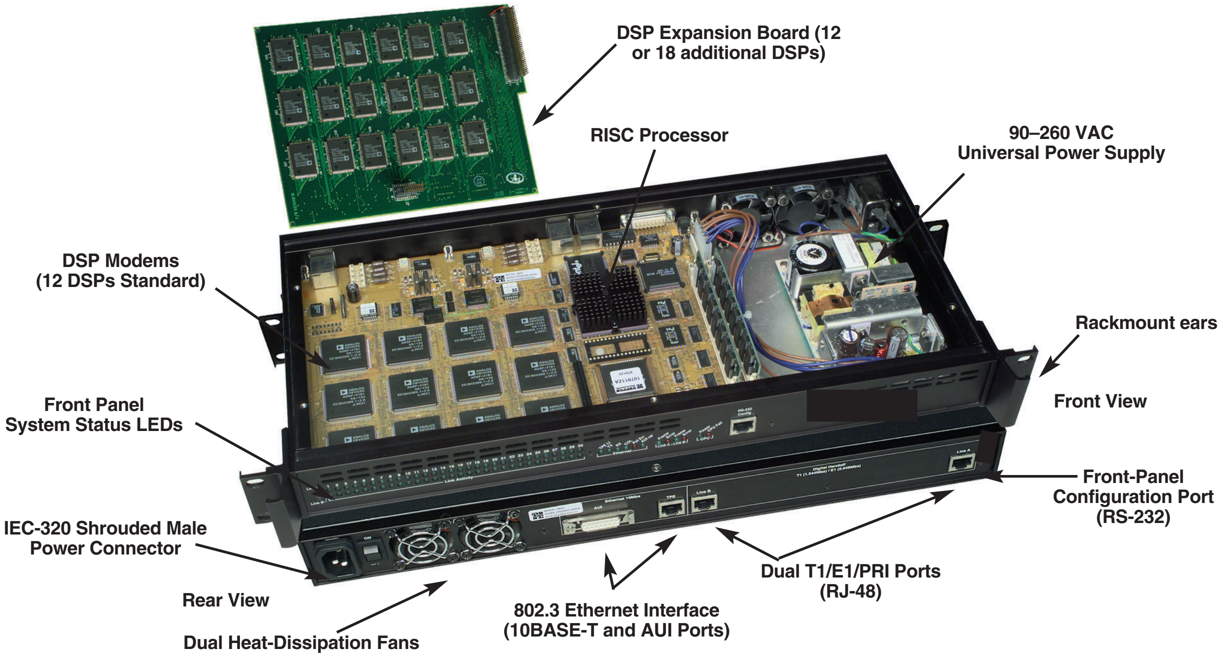

DSP Expansion Board (12 or 18 additional DSPs)
RISC Processor
90–260 VAC Universal Power Supply
DSP Modems (12 DSPs Standard)
Rackmount ears
[redacted]
Front View
Front Panel System Status LEDs
Front-Panel Configuration Port (RS-232)
IEC-320 Shrouded Male Power Connector
Dual T1/E1/PRI Ports (RJ-48)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

**Figure 2-1. The Remote Access Server.**

### Chassis Architecture and Hardware at-a-Glance

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

## 2.6 Where to Use the Remote Access Server

The Remote Access Server 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 Server can assume a critical role in a variety of applications.

## 2.7 Preview of Applications

1. ISP Access—The Remote Access Server 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 Remote Access Server provides a cost-effective remote Point-of-Reference.
3. Corporate Network Access—The Remote Access Server puts the corporate network just a phone call away, with e-mail, 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 Remote Access Servers can be deployed in local calling areas and linked through Frame Relay.
5. The Remote Access Server offers a drop-and-insert connection to the corporate PABX, allowing voice and data access through a single T1/E1 line.

### 2.7.1 ISP Access

Most Internet Service Providers (ISPs) begin operations by offering service to smaller communities of individuals in a distinct geographical area. The Remote Access Server is ideal for this start-up situation. In the configuration shown in **Figure 2-2**, the Remote Access Server 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.

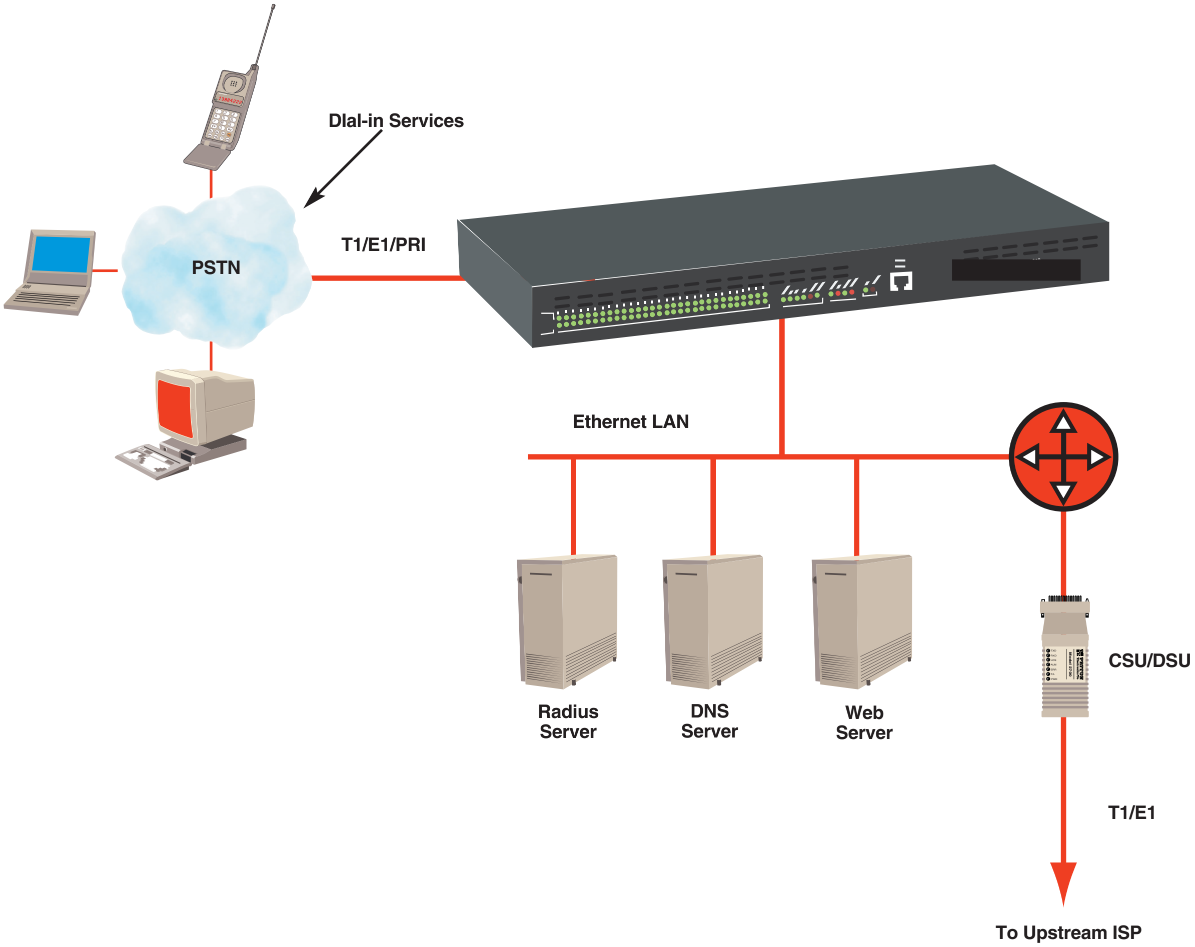


**Figure 2-2. ISP Access.**

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

The Remote Access Server provides an additional T1/E1 port for a direct uplink 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. New users are not forced to purchase high-end solutions to provide advanced Internet services to their customers.

### 2.72 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.

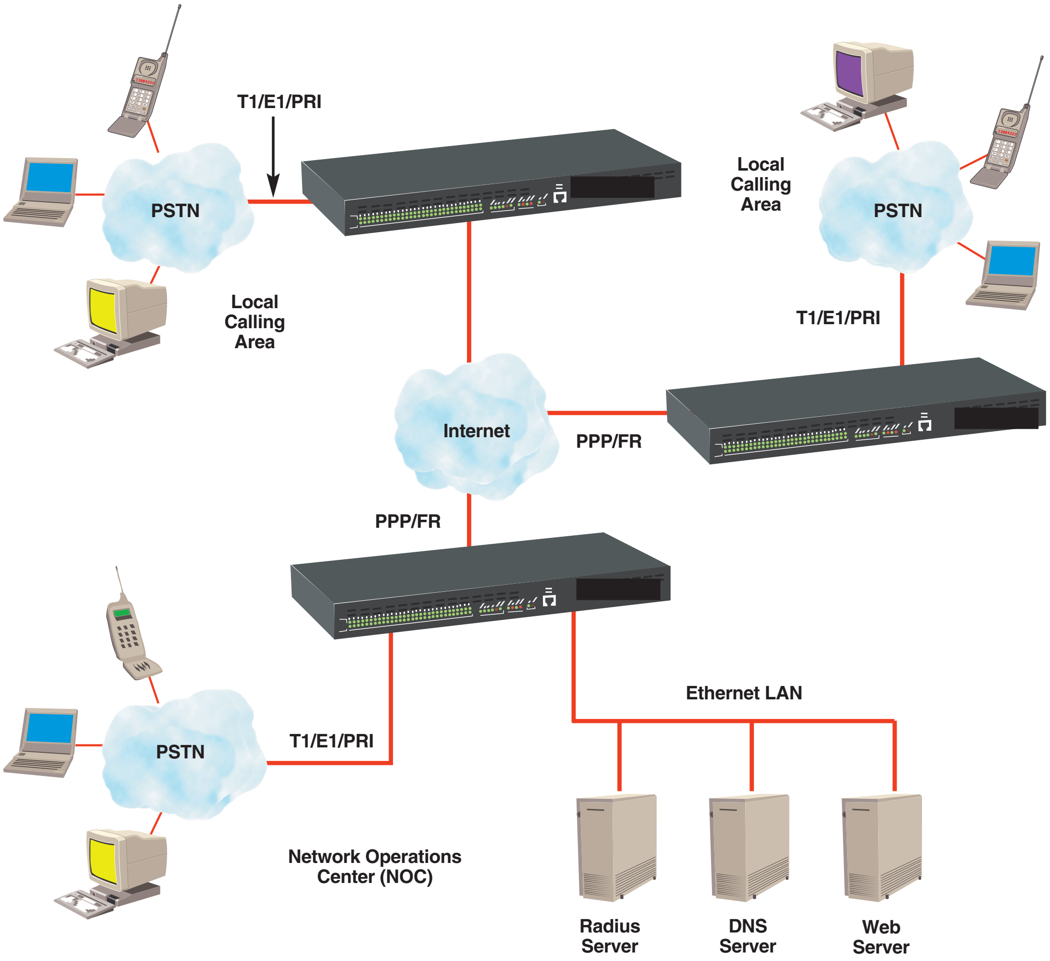


**Figure 2-3. ISP Expansion.**

In the new calling area, the Remote Access Server 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 Remote Access Server 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 e-mail servers at a central site. The Remote Access Server 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.

### 2.7.3 Corporate Network Access

With the growth of work-at-home, remote offices, flexible work hours and e-mail 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 e-mail, online information, and Internet access. The Remote Access Server provides these vital corporate services.

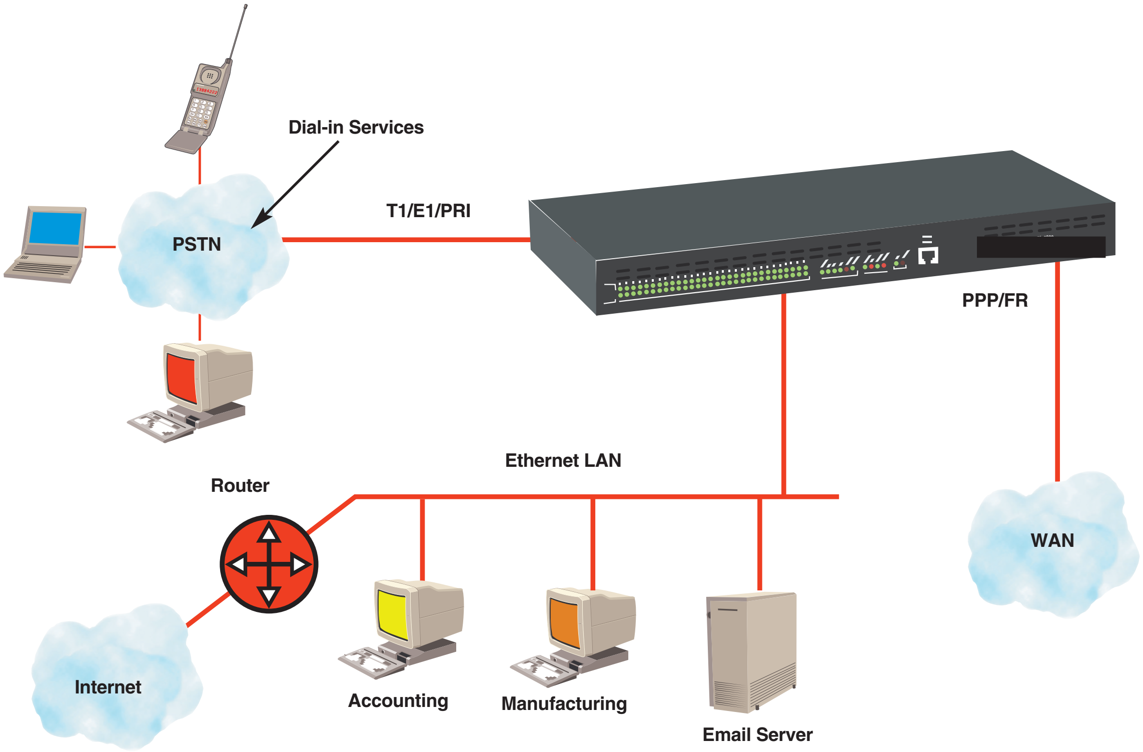


**Figure 2-4. Corporate Network Access.**

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

As users dial in to the Remote Access Server, modem calls are answered by one of the on-board processors. An integrated Ethernet port allows the Server 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, the Remote Access Server will also integrate a branch office into a larger corporate network or provide a link to Internet access.

### 2.7.4 Dial Access for Wide Area Networks

As corporations opt to outsource their dial-up connections for traveling salespersons, dealer networks, and remote users, telecommunication service providers are deploying remote access servers in local calling areas. The Remote Access Server 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 Server and Frame Relay, corporate network users remove the complexity and use a simple IP router to receive dial-in calls.

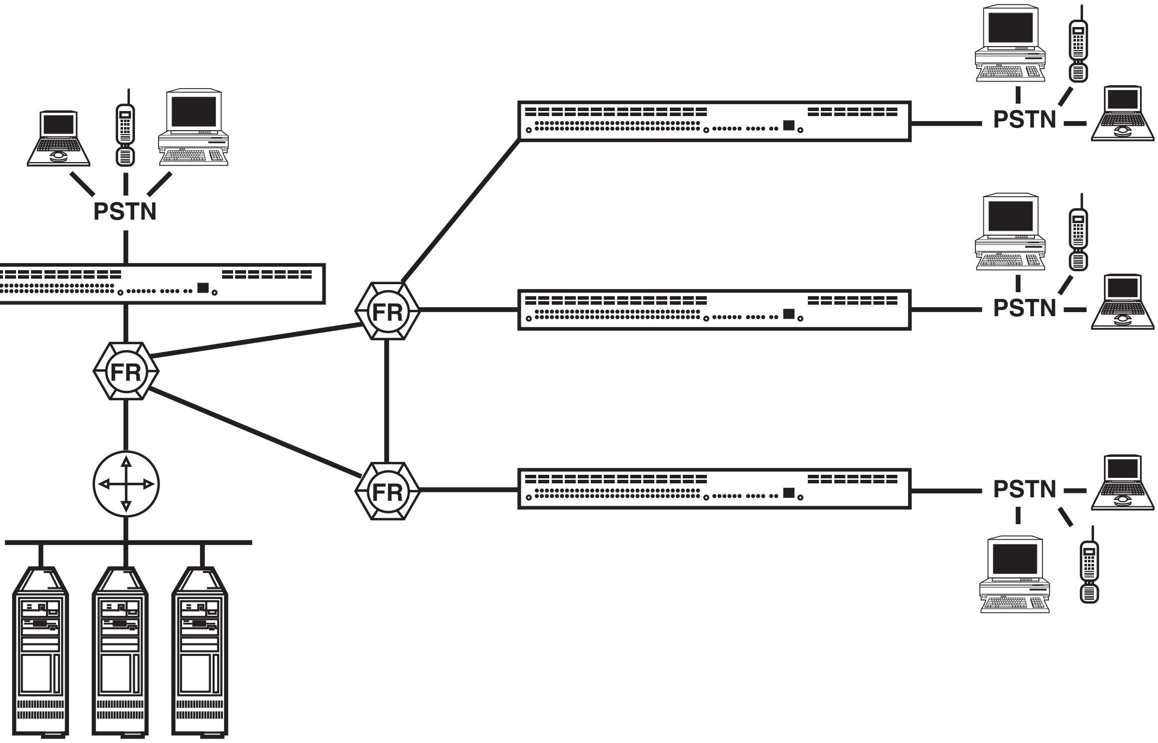


Figure 2-5. Dial Access for Wide Area Networks.

### 2.7.5 Corporate Voice/Data Integration

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

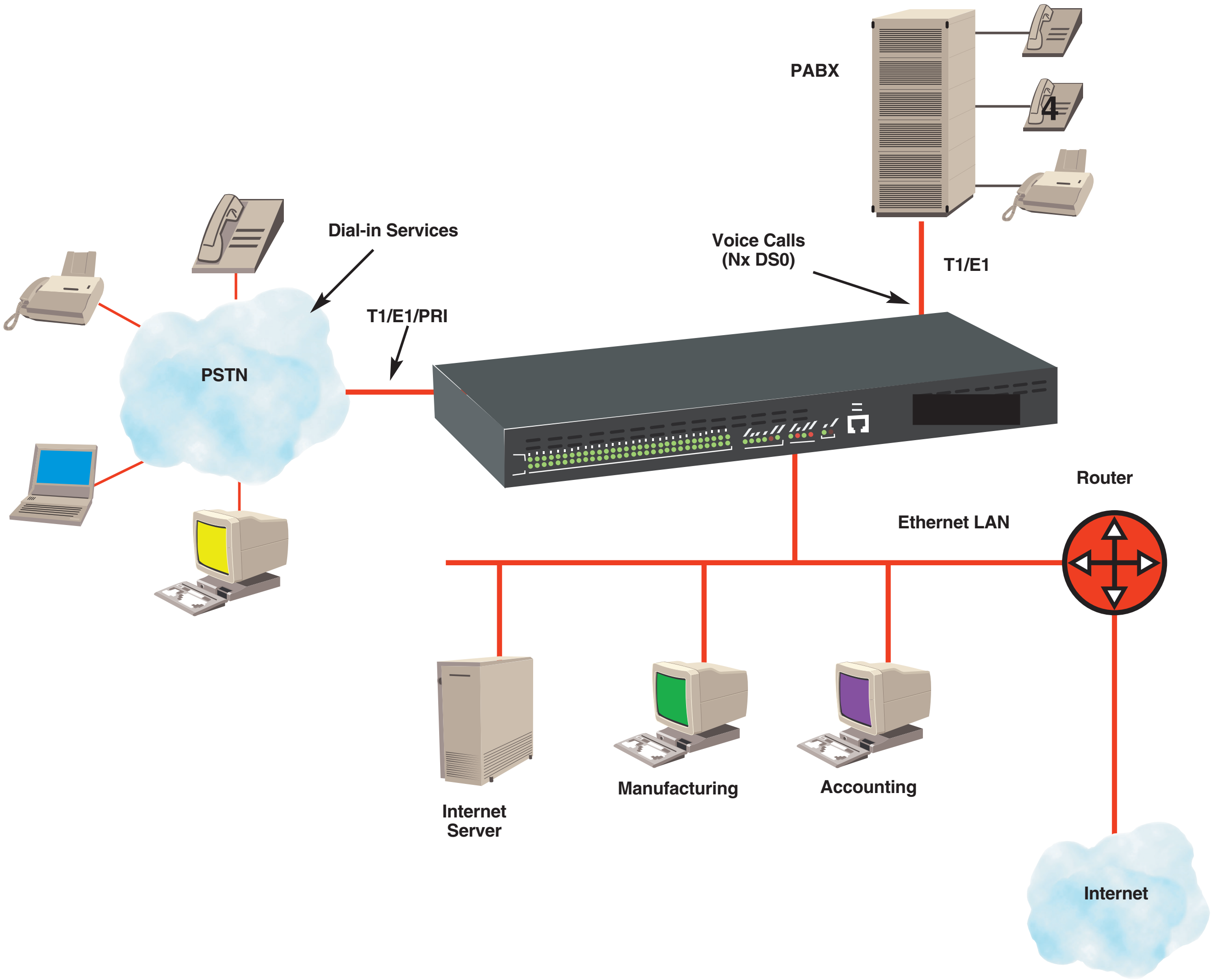


**Figure 2-6. Corporate/Voice Data Integration.**

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

The Remote Access Server supports the flexible integration of voice service into the corporate data network, making better use of valuable corporate resources than ever before.

## 2.8 System Requirements

Before you can install and configure your Remote Access Server, make sure you have the following items available.

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

## 2.9 What the Package Includes

The following items are included in your package. If anything is missing or damaged, please contact Black Box at 724-746-5500.

- (1) Remote Access Server with Integrated Modems
- (1) 6-ft. (1.8-m) UPC standard power cord
- Console cable
- Rackmount ears
- This user's manual

## 2.10 Making Connections

The Remote Access Server is equipped with two T1/E1/PRI ports, an Ethernet AUI port, a 10BASE-T 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. **Figures 2-7** and **2-8** show the rear and front panels of the Server, respectively.

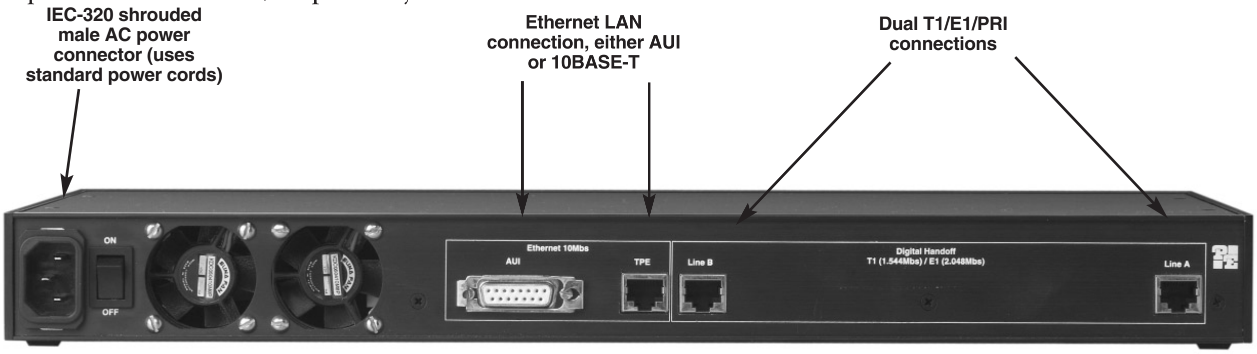

IEC-320 shrouded male AC power connector (uses standard power cords)
Ethernet LAN connection, either AUI or 10BASE-T
Dual T1/E1/PRI connections
ON
OFF
Ethernet 10Mbs
AUI
TPE
Line B
Digital Handoff
T1 (1.544Mbs) / E1 (2.048Mbs)
Line A

**Figure 2-7. Rear Panel of the Remote Access Server.**

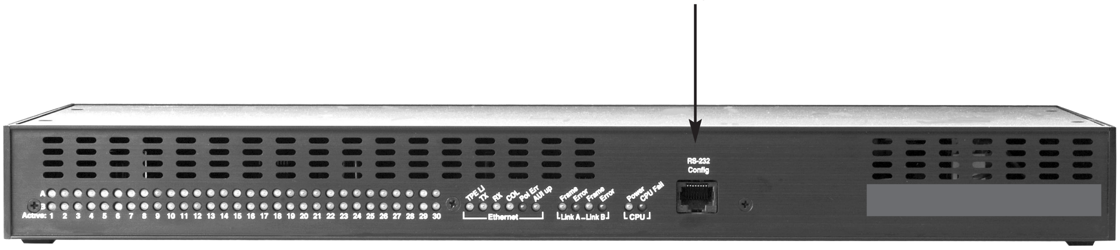


**Figure 2-8. Front Panel of the Remote Access Server.**

### 2.10.1 Connecting the Ethernet Ports

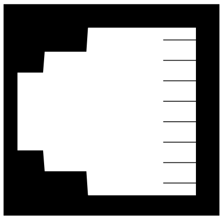
The Remote Access Server has AUI and 10BASE-T interfaces for connection to your Ethernet LAN. The Server may be connected directly to an Ethernet hub via RJ-45 cable, or to a host or backbone directly via DB15 AUI cable or an AUI-to-10BASE2 transceiver. This section describes how to connect the Router 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. We recommend that you disable 10BASE2 or 10BASE5 network operations before installing the Server.**

*Connecting the 10BASE-T Ethernet Port*

The RJ-45 Ethernet port on the rear of the Remote Access Server is designed to connect directly to a 10BASE-T network. **Figure 2-9** shows the pinout for the 10BASE-T RJ-45 port. Please refer to the following instructions when constructing cables to connect 10BASE-T ports to the Server. You may make connections up to 330 feet (100 m) away using Type 4 or 5 cable.



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

**Figure 2-9. 10BASE-T Ethernet Port Pinout.**

*Connecting a 10BASE-T Hub to the Remote Access Server*

The Ethernet 10BASE-T port on the rear of the Server is designed to connect directly to a 10BASE-T hub or repeater using RJ-45 unshielded twisted-pair cable that is wired straight through. Follow **Figure 2-10** to construct a straight-through cable to connect a 10BASE-T Hub to the Server's 10BASE-T port.

| 10BASE-T Hub | Remote Access Server 10BASE-T Port |
|---|---|
| **RJ-45 Pin No.** | **RJ-45 Pin No.** |
| 1 (RX+)< - - - - - - - - - - - - - - - - - - - - - - - - | 1 (TX+) |
| 2 (RX-)< - - - - - - - - - - - - - - - - - - - - - - - - | 2 (TX-) |
| 3 (TX+)- - - - - - - - - - - - - - - - - - - - - - - - - | >3 (RX+) |
| 6 (TX-) - - - - - - - - - - - - - - - - - - - - - - - - - | >6 (RX-) |

**Figure 2-10. Straight-through cable pinning.**

*Connecting a 10BASE-T Workstation to the Remote Access Server*

The 10BASE-T port on the Remote Access Server may also be connected directly to a 10BASE-T workstation via a cross-connect cable. Follow **Figure 2-11** to build a cross-connect cable to connect the 10BASE-T port on a workstation's NIC to the Remote Access Server's 10BASE-T port.

| 10BASE-T Workstation | Remote Access Server 10BASE-T Port |
|---|---|
| **RJ-45 Pin No.** | **RJ-45 Pin No.** |
| 1 (TX+)- - - - - - - - - - - - - - - - - - - - - - - - - | >3 (RX+) |
| 2 (TX-) - - - - - - - - - - - - - - - - - - - - - - - - - | >6 (RX-) |
| 3 (RX+)< - - - - - - - - - - - - - - - - - - - - - - - - | 1 (TX+) |
| 6 (RX-)< - - - - - - - - - - - - - - - - - - - - - - - - | 2 (TX-) |

**Figure 2-11. Cross-connect cable pinning.**

*Connecting to the AUI Ethernet Port*

The Remote Access Server incorporates one female (DTE) DB15 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—10BASE-T, 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.

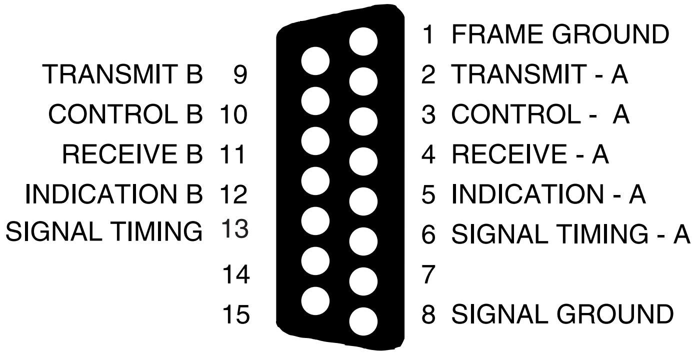


**Figure 2-12. Remote Access Server AUI Interface.**

*Connecting a Transceiver to the Remote Access Server AUI Port*

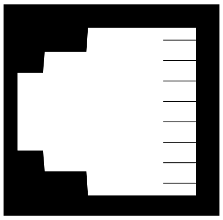
The DB15 female AUI port on the Server is designed to interface directly with a DB15 male AUI to 10BASE-T, 10BASE2, or FOIRL transceiver either directly or via an AUI cable (see **Figure 2-13**).

```
Tranceiver AUI Port                    Remote Access Server AUI Port
DB15 male Pin No.                      DB15 female 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)
```

**Figure 2-13. Pinning for Transceiver to Server AUI Port.**

### 2.10.2 Connecting the T1/E1/PRI Port

An active T1/E1/PRI is not necessary to configure the Remote Access Server. However, an active T1/E1/PRI connection is required to receive or make calls. The default configuration of the Server has the primary T1/E1 port enabled and the secondary T1/E1 port disabled. **Figure 2-14** shows the pin assignments on the T1/E1 RJ-48C jack of the Remote Access Server.



```
1< - - - - - - - - - - 1 (RX) Receive (RING)
2< - - - - - - - - - - 2 (RX) Receive (TIP)
3 - - - - - - - - - - - 3
4 - - - - - - - - - - - >4 (TX) Transmit (RING)
5 - - - - - - - - - - - >5 (TX) Transmit (TIP)
6 - - - - - - - - - - - 6
7 - - - - - - - - - - - 7
8 - - - - - - - - - - - 8
```

**Figure 2-14. T1/E1/PRI Interface on the Remote Access Server.**

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

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

### 2.10.3 Connecting the Power Supply

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

### 2.10.4 Connecting the RS-232 Configuration Port

The RS-232 configuration port on the front panel of the Server is configured as DCE. Using the enclosed RJ-45 serial cable, connect the Server's configuration port to the computer's serial communications port.

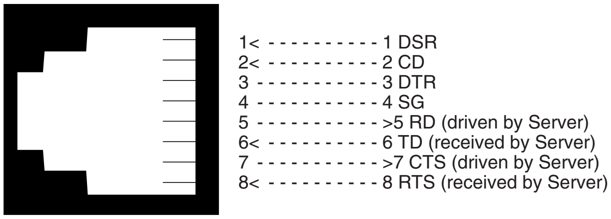

1< - - - - - - - - - - 1 DSR
2< - - - - - - - - - - 2 CD
3 - - - - - - - - - - - 3 DTR
4 - - - - - - - - - - - 4 SG
5 - - - - - - - - - - - >5 RD (driven by Server)
6< - - - - - - - - - - 6 TD (received by Server)
7 - - - - - - - - - - - >7 CTS (driven by Server)
8< - - - - - - - - - - 8 RTS (received by Server)

**Figure 2-15. RS-232 Front-Panel Configuration Port on the Server.**

Set the configuration of your communications software (ProComm, HyperTerminal, BitCom, pcANYWHERE, etc.) 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 RS-232 configuration port.**

### 2.10.5 Reading the LED Status Indicators

The Server front panel has numerous status LEDs to visually inform you of the current operations status and health of the Server. **Figure 2-16** shows the LED on the Server's front panel.

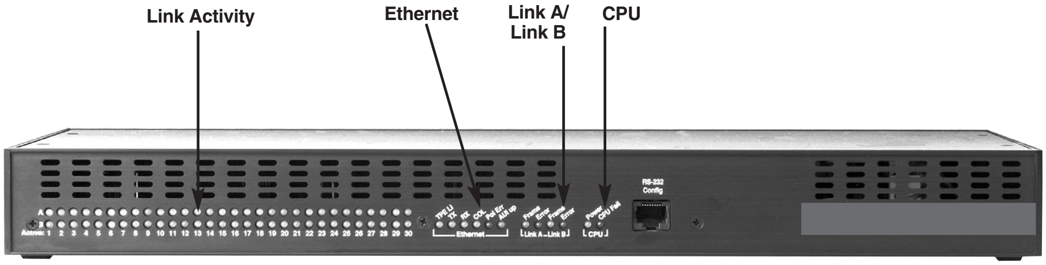


**Figure 2-16. LEDs on the Front Panel of the Server.**

*Link Activity LED Indicators*

The first group of LEDs is the Link Activity group, which includes two rows of LEDs: one row for LINK A and one row for LINK B. There's an LED for each channel, or time slot, on each WAN connection. If you have the LRA2800A-24, only LEDs 1-24 will be active. If you have the LRA2800A-30, LEDs 1-30 will be active.

**Table 2-1. Link Activity LED Status Indicators.**

| LED | Function/Color | Description |
|---|---|---|
| Link A | Channel Link/Green | Off=Idle<br>On=Active<br>Double Pulse=ringing<br>Flashing=connecting |
| Link B | Channel Link/Green | Off=Idle<br>On=Active<br>Double Pulse=ringing<br>Flashing=connecting |

*Ethernet LED Indicators*

The second group of LEDs is the Ethernet group. It conveys which interface is selected, activity, and collisions on the Ethernet link.

**Table 2-2. Ethernet LED Status Indicators.**

| LED | Function/Color | Description |
|---|---|---|
| TPE LI | Twisted Pair Link Indication/ Green | On=10BASE-T Ethernet is the active LAN connection<br>Off=10BASE-T is not the active LAN connection |
| TX | Transmit Data from PAR-1 to LAN/Green | On=Data is being transmitted<br>Off=No Data is being transmitted |
| RX | Receive Data to PAR-1 from LAN/Green | On=Data is being received<br>Off=No Data is being received |
| COL | Collision Detected on Ethernet/ Green | On=Collision Detected<br>Off=No Collision Detected |
| POL ERR* | Polarity Error/Red | On=Polarity is reversed on 10BASE-T connection<br>Off=Polarity is correct on 10BASE-T connection |
| AUI up | Attachment Unit Interface/ Green | On=AUI port is being used or no connection either Ethernet port |

## *NOTE

**The Remote Access Server will correct for polarity errors in the Ethernet line automatically.**

*Link A/Link B LED Indicators*

The third group of LEDs is the LINK A/LINK B group. It monitors the Link A and Link B WAN connections and displays the health status of the WAN connections.

**Table 2-3. Link A/Link B LED Status Indicators.**

| LED | Function/Color | Description |
|---|---|---|
| Frame | Frame/Green | On=WAN link is in frame<br>Off=Server is not detecting a WAN signal<br>Flashing=Server detects out of frame signal<br>Flashing=connecting |
| Error | Error Condition/Red | On=WAN link is unavailable for communications<br>Off=WAN link is available for communications |

### *CPU LED Indicators*

The fourth group of LEDs is the CPU group, which shows that power is applied to the Server and also shows the health of the CPU.

**Table 2-4. CPU LED Status Indicators.**

| LED | Function/Color | Description |
|---|---|---|
| Power | Power Condition/Green | On=Power is on<br>Off=Power is off |
| CPU Fail | Channel Link/Red | On=CPU Boot Failure<br>Off=CPU executed internal boot program successfully |

# 3. Getting Started

## 3.1 How the Remote Access Server Works

Older installations that use analog-to-digital conversion result in lower connection speeds. These same systems also require separate analog modems and ISDN terminal adapters. The Remote Access Server's significant advantage is its use of digital signal processors (DSPs) as dynamic communications processors. The Server's DSPs terminate both analog and ISDN connections within the same hardware and using the same PSTN trunk, for the highest possible connecting speeds.

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

The Server supports all common remote access methods (SLIP, PPP, TELNET) as well as providing integrated routing and forwarding. Authentication and network management offer control and detailed monitoring from any Web browser.

The Server connects to the network through integrated routing and forwarding, and dynamic routing protocols keep the Server synchronized with other network devices.

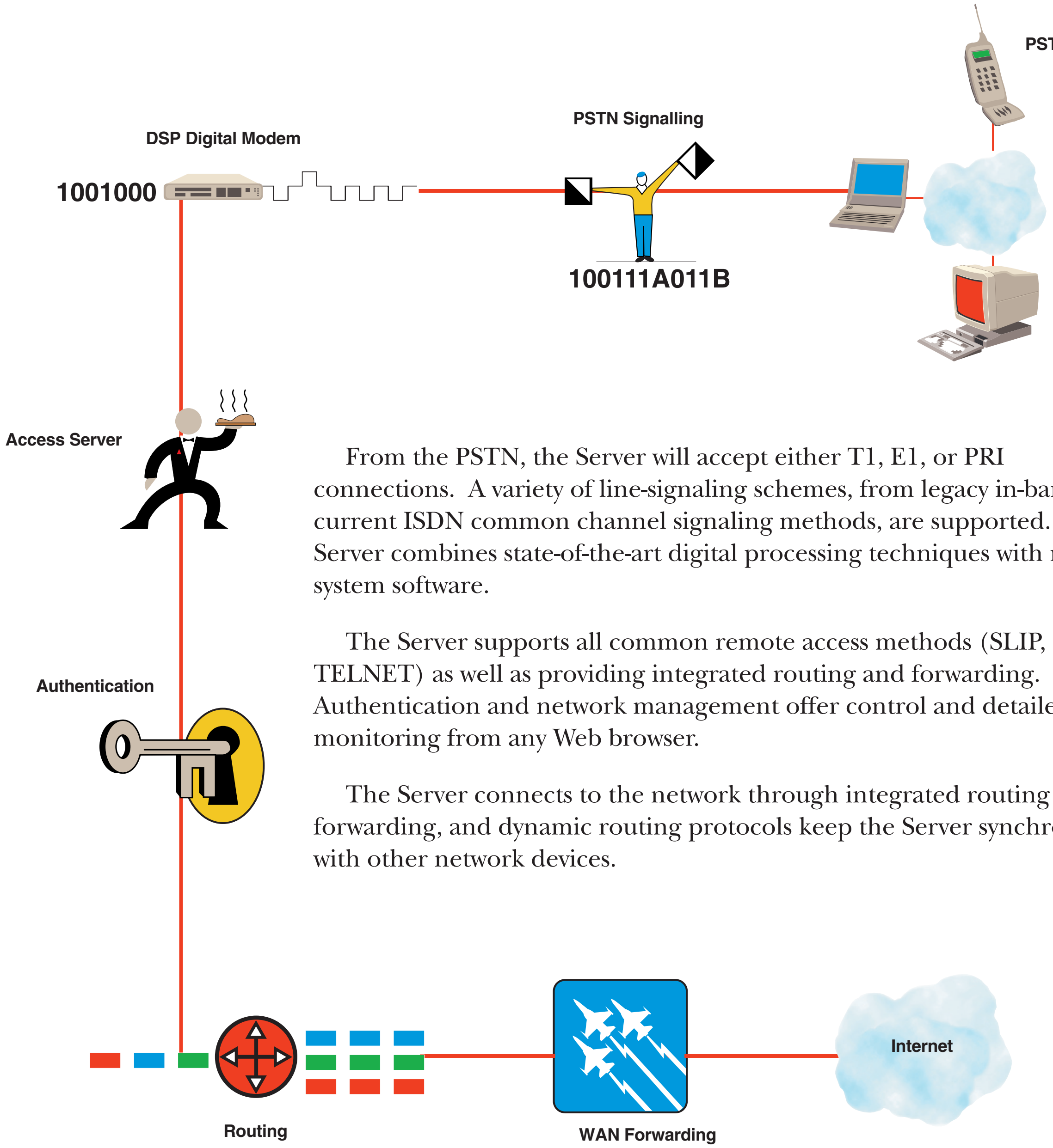


**Figure 3-1. How the Server Works.**

### 3.1.1 PSTN SIGNALLING

The PSTN trunk connections are terminated by the Remote Access Server 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 Server 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 Server using two basic signaling methods: Channel Associated Signaling (CAS) and Common Channel Signaling (CCS).

*Channel Associated Signaling (CAS)*

CAS is a method of signaling in which call-processing information is embedded 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 indicates 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 signaling. 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 Server 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 Server to provide 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 Server 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 Server, at the time a call is placed, whether the call is an analog voice/modem or digital ISDN call. The Server 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 standard 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 Server supports CTR-4, NET5, TS014, INS1500, NI1, AT&T/Lucent, and DMS switching equipment.

### 3.1.2 DSP DIGITAL MODEM

The Remote Access Server's T1/E1/PRI line termination connects to the DSPs via an internal PCM highway. The Server'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 process 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. This software-driven DSP processing provides an inherent migration path to future technologies.

*Processing V.34+ Calls*

When 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 Server 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 Remote Access Server can support synchronous PPP to connect remote ISDN Terminal Adapters (TAs) over B channels. Using Multilink PPP (MP), multiple 64-kbps channels can be “glued” together to permit larger-bandwidth connections as well as bandwidth on demand.

*Processing 56K Calls*

New standardized modem technology brings faster connections to users. 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 Server’s DSPs negotiate these new modulations by loading V.8bis for call processing. The Server, a software-driven device, easily adapts to new modem standards as they develop—only a flash software upgrade is required.

The Server’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.

### 3.1.3 Access Server

After successfully negotiating a modem link, the Server lets you connect to protocol-related services. Two types of connection to these services are available from the Server: unframed and framed.

*Unframed Connections*

Unframed connections, or connections without any underlying protocol, will receive a login prompt. After the Server has received the login information, it will authenticate the user. You may be authenticated against the internal user static database or through RADIUS. Upon successful authentication, you will be granted service either based on 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 Server 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 Server’s success banner is user-customizable 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 Server will automatically detect 7E flags and begin a PPP session. In the link-establishment phase, the Server and the caller (also known as the peer) will negotiate network-specific options.

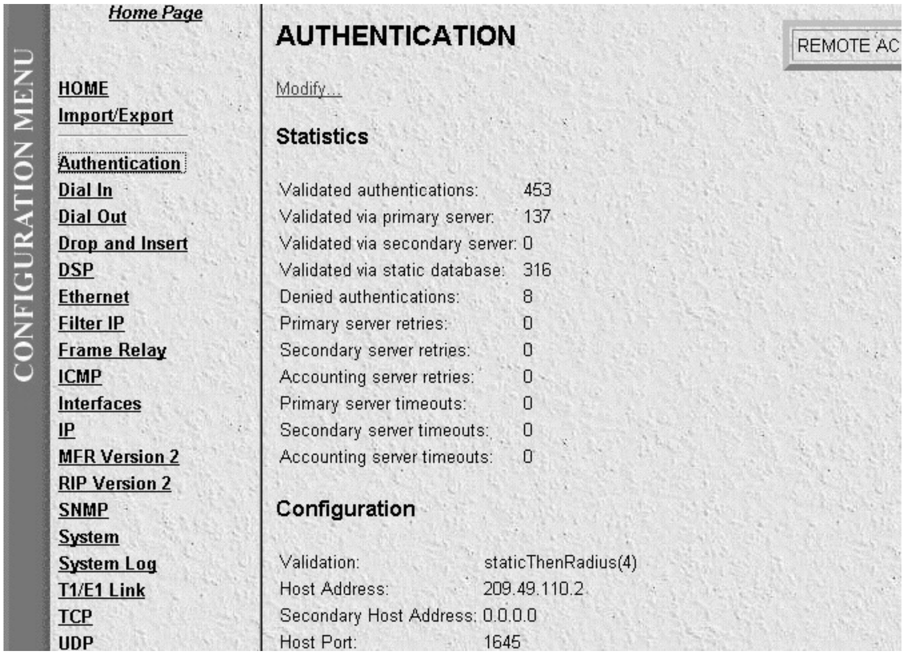
Multilink PPP (MP) is similar to PPP in that it allows the aggregation of multiple smaller connections to create a single large-bandwidth connection. (Basic Rate ISDN, supported by the Server, offers the possibility of opening these multiple simultaneous channels between systems. This gives you additional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

*Custom Configuration*

The Server allows custom configuration of various connection parameters. For example, the Server 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.

### 3.1.4 AUTHENTICATION

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



AUTHENTICATION

Statistics

| | |
|---|---|
| Validated authentications: | 453 |
| Validated via primary server: | 137 |
| Validated via secondary server: | 0 |
| Validated via static database: | 316 |
| Denied authentications: | 8 |
| 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: | staticThenRadius(4) |
| Host Address: | 209.49.110.2 |
| Secondary Host Address: | 0.0.0.0 |
| Host Port: | 1645 |

**Figure 3-2. Authentication screen.**

*Local Authentication*

For local authentication, the Server incorporates an internal database supporting over 100 users. Once the user connects, the Server 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 Server will obtain the user information for processing by the Server authentication manager.

*RADIUS Authentication*

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

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. Any user passwords sent between the client and the RADIUS server are in encrypted format.

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

### 3.1.5 Routing/Forwarding

The Server 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 Server receives a packet, it will scan the table for the best route. If no route is found by the Server, the packet will be sent to the default gateway. You can then configure static routes with the Server, using either a gateway, host, or interface route. To automatically locate the next hop for a packet, when that is possible, the Server uses ARP and RIP routing protocols.

*ARP*

The Address Resolution Protocol (ARP) is the means by which IP addresses are associated with a physical Ethernet address. The Server 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 Server are Routing Information Protocol (RIP) version 1 and version 2. These protocols identify which networks each router is currently connected to, and assist the Server—along with ARP—in automatically locating the next hop for a particular IP packet.

*Forwarding*

For additional network connectivity, you can also use the Server's second T1/E1 connection as a Frame Relay uplink. You can configure user bandwidth on a time-slot basis. Using RFC 1490 encapsulation and the Server's sub-interface architecture, each Data Link Connection Identifier (DLCI) is specified as its own point-to-point connection. The Server will then add entries in the routing table to forward packets to and from each DLCI.

### 3.1.6 Network Management Overview

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

*The Server as a Managed Node (SNMP)*

As a managed node, the Server 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 Server 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 Server 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 Server supports MIB II and is able to access SNMP configuration and statistics information through standard SNMP MIBs. The Server also offers extended management functionality through the Enterprise MIB.

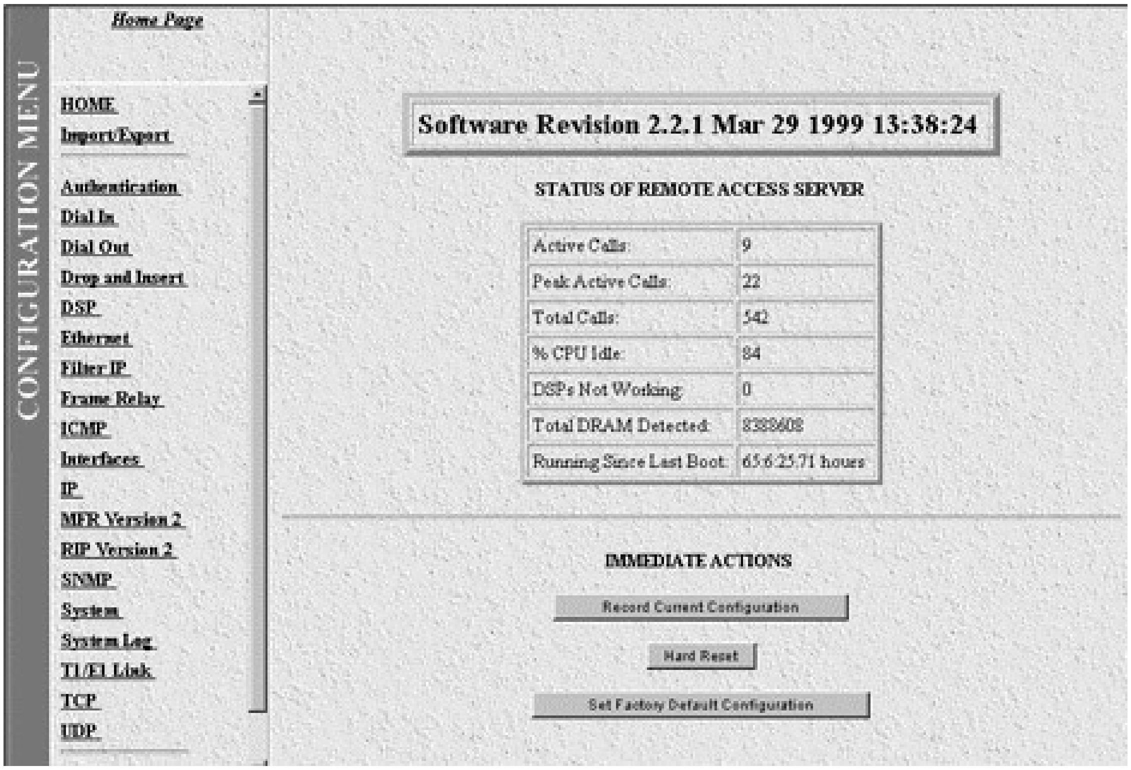
The Server supports two SNMP community names: one permits read-only access and the other permits read-and-write access. These community names also serve as the passwords for the Web-based and control-port interfaces.

*The Server 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, and there is no need for dedicated management workstations.

As a management application, the Remote Access Server runs its own built-in HTTP (version 1.0) Web server. This allows systems equipped with standard browsers (for example, 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 Server in an intuitive, graphical manner (see the sample screen in **Figure 3-3**). Navigation using this management system is as simple as following a link or pressing “submit.” The Server’s main menu displays twenty-two separate configuration links. These links allow complete system configuration, as well as displaying all Server 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 Server for immediate change.

Two levels of security are provided to allow controlled access to the Server’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 Server configuration parameters.



Software Revision 2.2.1 Mar 29 1999 13:38:24

STATUS OF REMOTE ACCESS SERVER

| | |
|---|---|
| Active Calls: | 9 |
| Peak Active Calls: | 22 |
| Total Calls: | 542 |
| % CPU Idle: | 84 |
| DSPs Not Working: | 0 |
| Total DRAM Detected: | 8388608 |
| Running Since Last Boot: | 65:6:25.71 hours |

IMMEDIATE ACTIONS

**Figure 3-3. Home Page.**

*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 Server 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 Server can be connected to a larger, centrally located server that multiple Remote Access Servers may use.

## 3.2 Booting the Remote Access Server

### NOTE

**If you are starting the Remote Access Server 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, HyperTerminal, BitCom, pcANYWHERE, 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 Remote Access Server.

3. Turn on the Remote Access Server.

4. After the Server is turned on, it will enter a series of diagnostic tests to exercise the internal sub-systems in the box. The terminal display during the power-up sequence will look something like the display shown in **Figure 3.4**. (The actual display will appear much longer. The following is only shown as an example.)

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

**Figure 3-4. Terminal Display During Power-Up.**

5. The Server will continue on to test the DSPs, Ethernet LAN, T1/E1/PRI WAN, and other interfaces. If the operational code (the code that actually runs the Server) is verified to be valid, the Server will display the login banner and user prompt shown in **Figure 3-5**:

```
Black Box Corporation
Remote Access Server with Integrated Modems

Username>
```

**Figure 3-5. Login Banner and User Prompt.**

6. Enter the following username and press the return key:

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

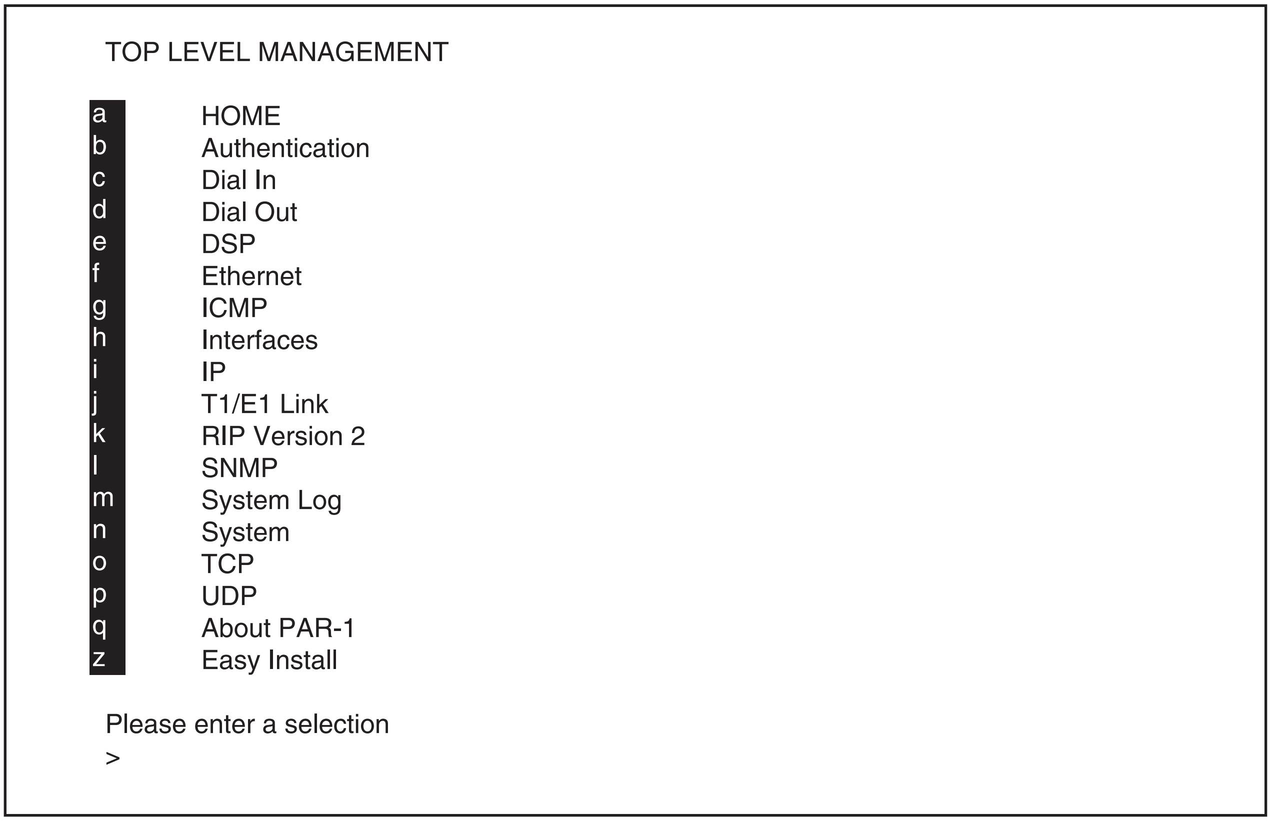
**Figure 3-6. Entering the Username.**

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

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

**Figure 3-7. Entering the Password.**

8. After you have successfully logged in, the Server will display the one of the main menu configuration screens. **Figure 3-8** shows the configuration menu when using the front panel RS-232 configuration port.



```
TOP LEVEL MANAGEMENT

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
>
```

**Figure 3-8. Top Level Management screen.**

## NOTE

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

## 3.3 Initial Setup

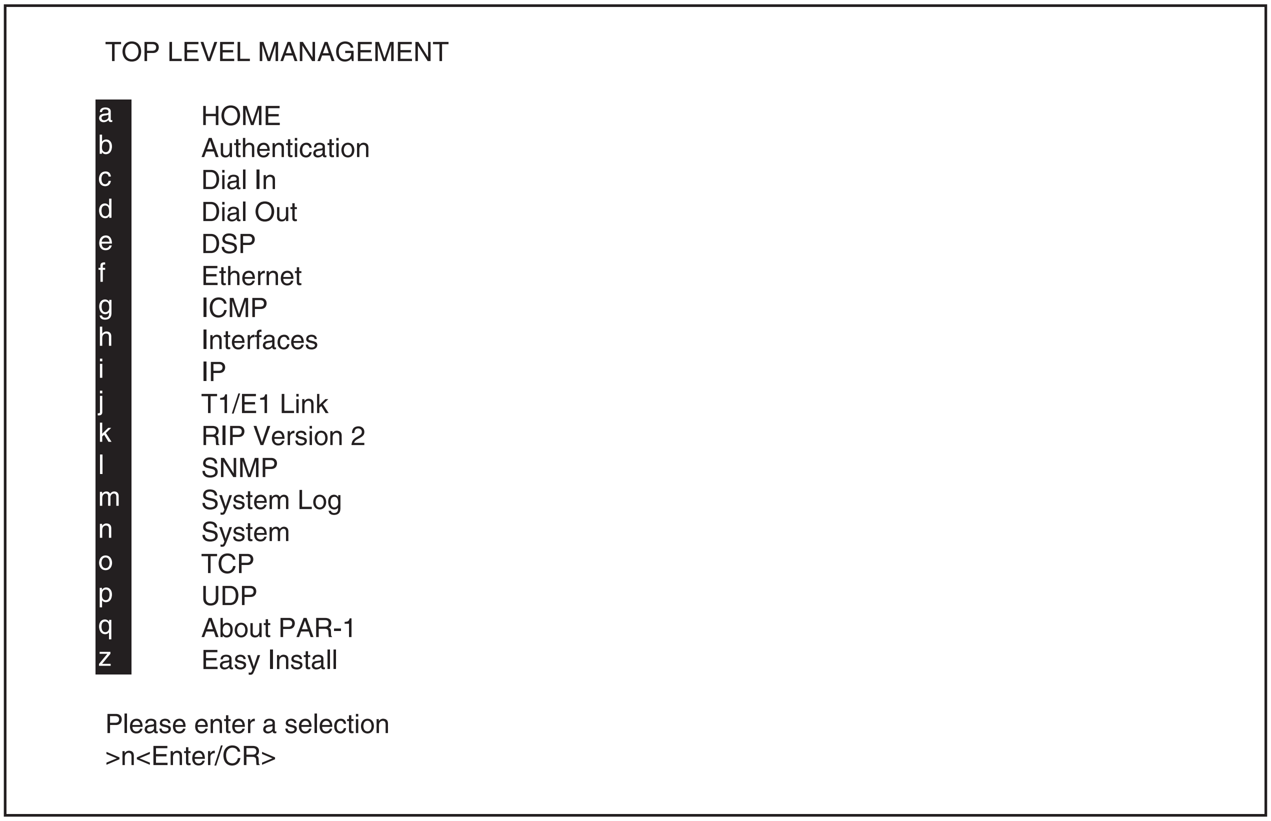
To operate the Remote Access Server, you must define the LAN Address Technique, LAN IP address, and Subnet Mask to be dedicated for use in the Server. You must log into the front-panel RS-232 configuration port to complete the initial configuration. After setting the parameters above, you may change 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 Server and have successfully logged into the RS-232 configuration port.

## NOTE

**Under normal circumstances, the RS-232 port should be used only for 1) initial setup; 2) out-of-band backup; and 3) external network management.**

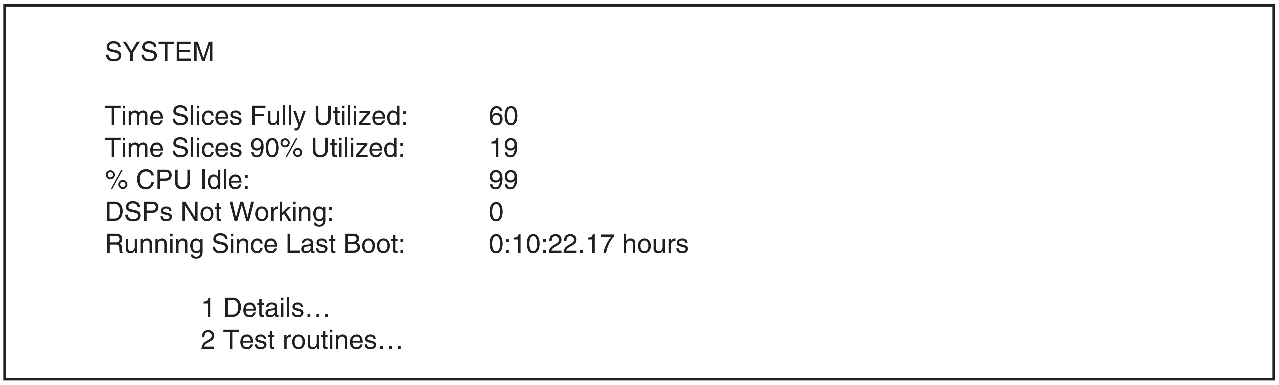
1. Enter Option **n, System**, from the main menu, as shown in **Figure 3-9**.



```
TOP LEVEL MANAGEMENT

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
>n<Enter/CR>
```

**Figure 3-9. Main Menu, System option selected.**

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

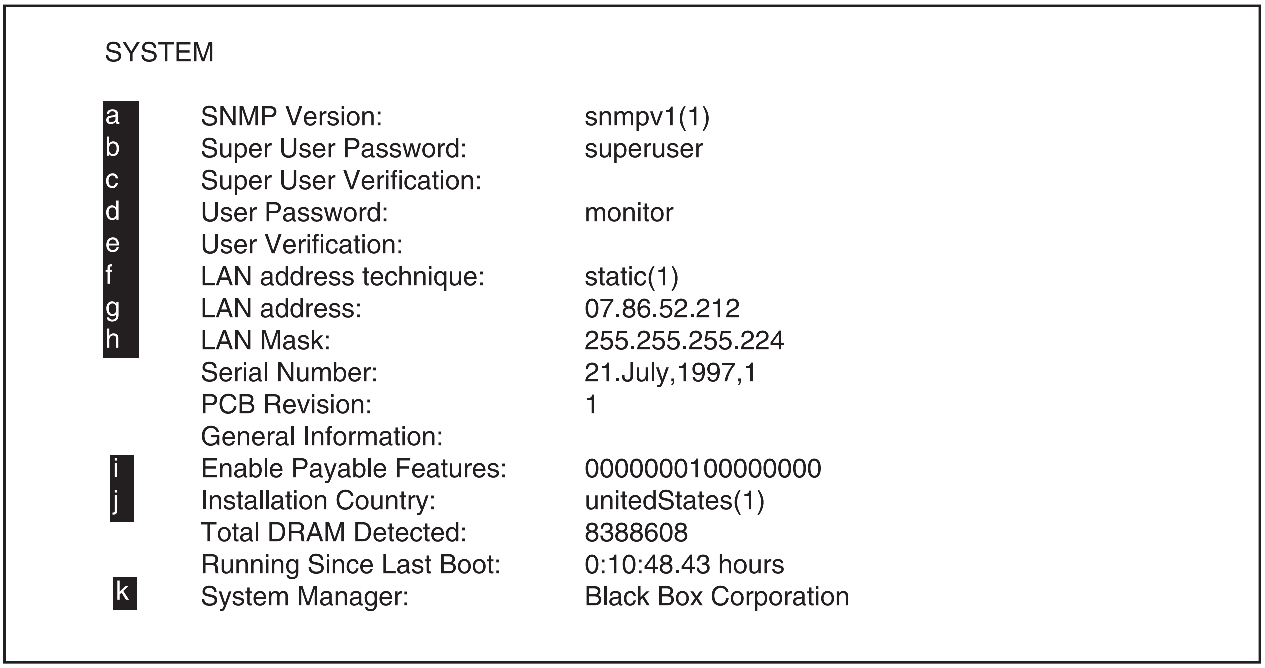


```
SYSTEM

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…
```

**Figure 3-10. System Menu.**

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

4. Option **1 Details** displays the system configuration information shown in **Figure 3-11**.



```
SYSTEM

a   SNMP Version:                 snmpv1(1)
b   Super User Password:          superuser
c   Super User 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:               Black Box Corporation
```

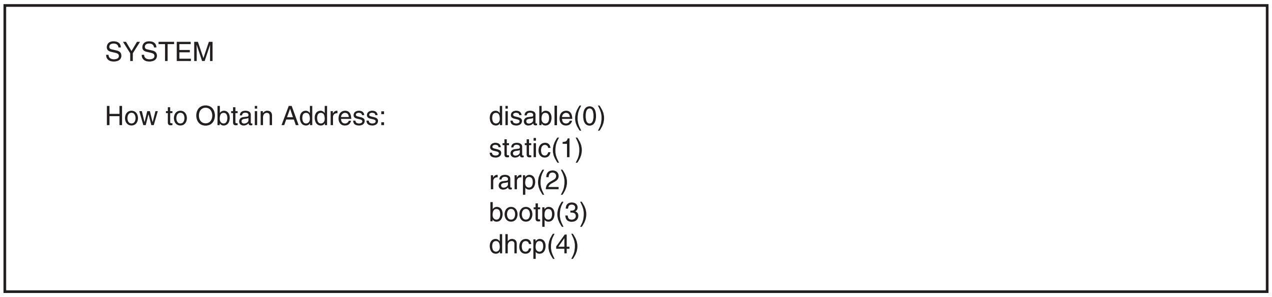
**Figure 3-11. Details of the System Configuration.**

5. You are now ready to set the LAN address technique, LAN IP address, and Subnet Mask as described in **Section 3.3.1**.

### 3.3.1 Setting the LAN Address Technique

You must select the LAN address technique in order for the Server to be able to determine the source of its IP address. Please refer to **Section A.15, System**, for more information about LAN addressing. Follow the instructions below to set the LAN address technique for the initial installation of the Remote Access Server.

1. Select Option **f LAN address technique** from the SYSTEM menu.
2. The Server will display the menu shown in **Figure 3-12**.



```
SYSTEM

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

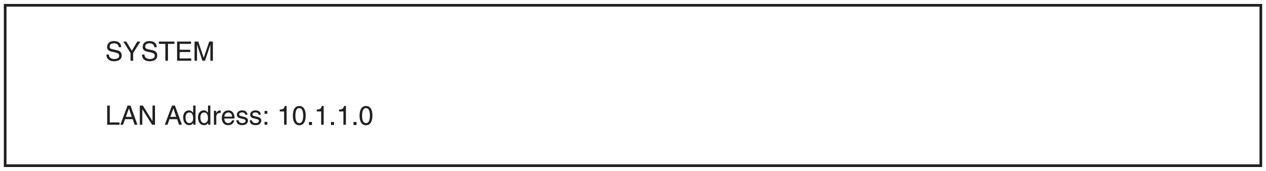
**Figure 3-12. Setting the LAN Address screen.**

3. Select **static(1)**.
4. Press the left arrow key (¨) to return to the System menu.

### 3.3.2 Setting the IP Address

The IP address must be the IP address dedicated to the Remote Access Server. 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 Server will display the screen shown in **Figure 3-13**.



```
SYSTEM

LAN Address: 10.1.1.0
```

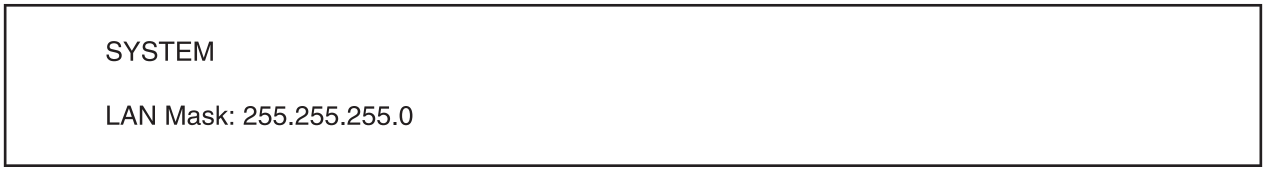
**Figure 3-13. Setting the LAN address screen.**

3. Enter the dedicated IP address for the Remote Access Server.
4. Press the left arrow key (¨) to return to the SYSTEM menu.

### 3.3.3 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 Remote Access Server will display the menu shown in **Figure 3-14**.



```
SYSTEM

LAN Mask: 255.255.255.0
```

**Figure 3-14. LAN Mask menu.**

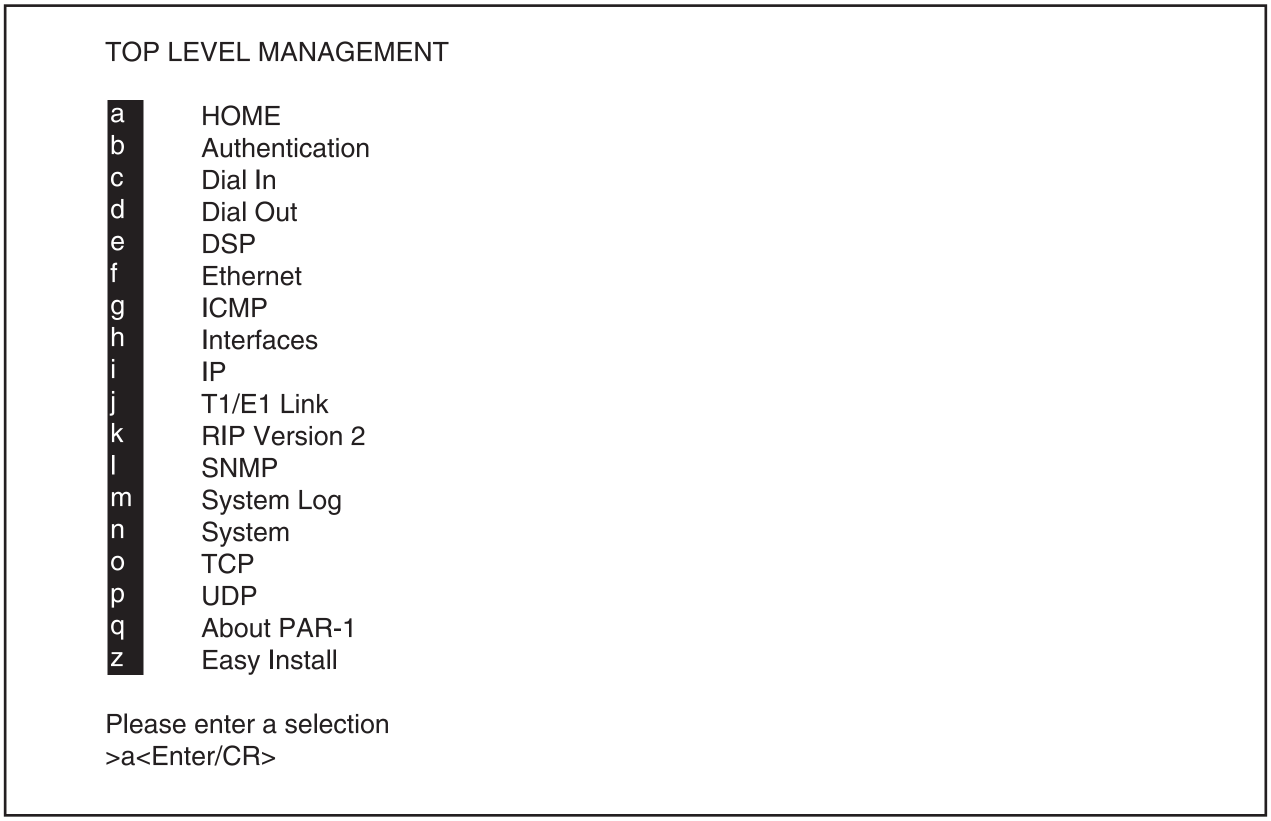
3. Enter the LAN subnet mask for the Remote Access Server.
4. Press the left arrow key to return to the Main Configuration menu.

You may now configure the box by using a standard Web browser such as Netscape Navigator or Microsoft Internet Explorer. To use the Web configuration tool, connect your Ethernet port and enter the IP address of your Server in the “Location” field of your browser.

## 3.4 Saving, Re-booting and Re-setting

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

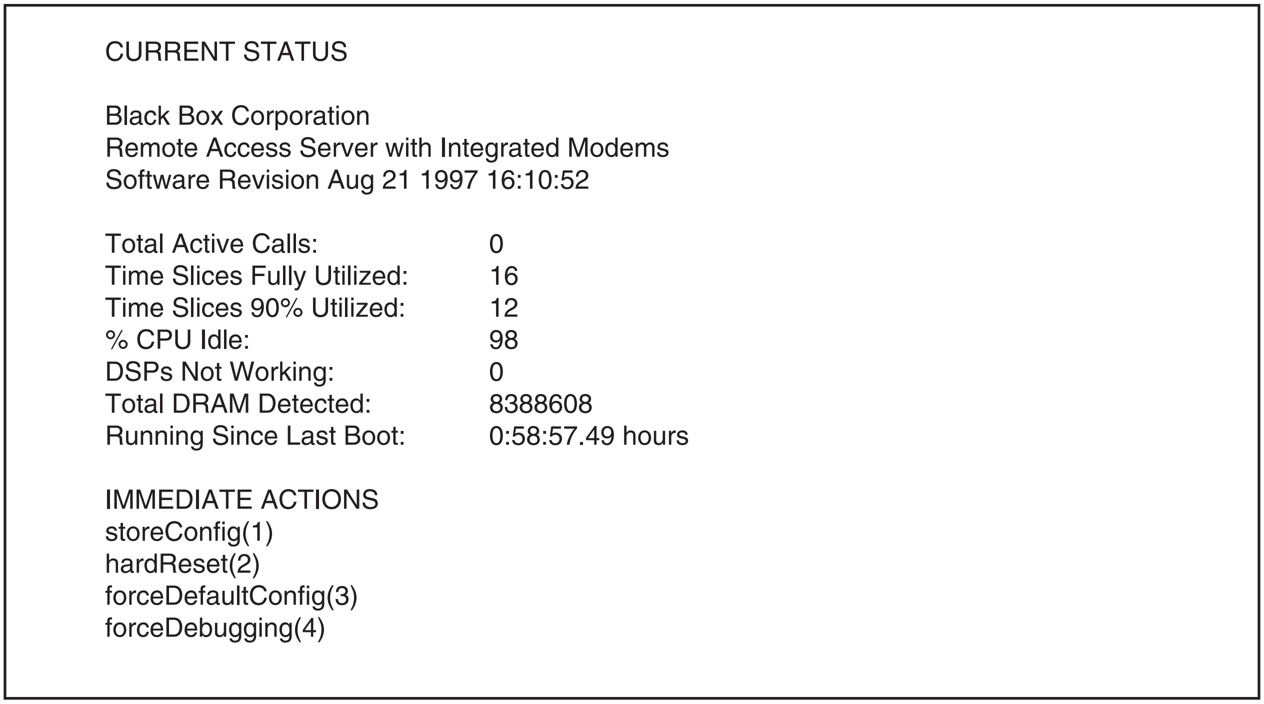
1. Enter Option **a HOME** from the main menu, as shown in **Figure 3-15**.



```
TOP LEVEL MANAGEMENT

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
>a<Enter/CR>
```

**Figure 3-15. Selecting the HOME option from the main menu.**

2. Option **n System** displays the CURRENT STATUS menu shown in **Figure 3-16**.



```
CURRENT STATUS

Black Box Corporation
Remote Access Server with Integrated Modems
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)
```

**Figure 3-16. Current Status menu.**

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

### 3.4.1 Saving the Current System Configuration

Any changes made to the 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 you have selected **storeConfig(1)**. Any changes made and not stored in flash memory will be lost when you power off or reset the Server.

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

### 3.4.2 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. You are not required to restart the system after making changes to the system configuration. All changes take place immediately.

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

### 3.4.3 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 Server. 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 Server over an IP network.

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

## 3.5 T1/PRI (Message Oriented) Planning

### 3.5.1 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 set up the Server.

- Switch Type. There are four basic switch types in North America, as described in **Table 3-1**.

**Table 3-1. ISDN Switch Types.**

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

### 3.5.2 Setting Up the Remote Access Server for T1 Access

To make a dial-in call to the Server for an T1 (DS1) line, you must configure the following variables. The 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)

### 3.5.3 Setting Up the Remote Access Server for ISDN PRI Access

To make a dial-in call to the Server for an ISDN PRI line, you must configure the following variables. The 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)

# 4. Configuring the PSTN Line Interface

## 4.1 Introduction to the PSTN Interface

The Remote Access Server has two built-in PSTN line connections labeled “Line A” and “Line B” (see **Figure 4-1**). 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 Server’s PSTN interface to enable it to answer calls. This chapter describes how to configure the PSTN line interface using a 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 2, Introduction**.

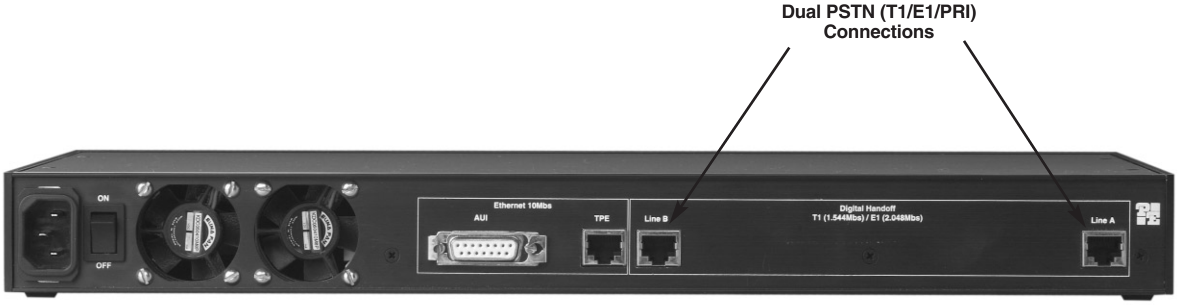


**Figure 4-1. Rear Panel of the Remote Access Server.**

## 4.2 Things You Will Need to Know

To setup your Remote Access Server 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 telephone company (for example, LBO, FDL, etc)

## 4.3 Enabling the Web Browser

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

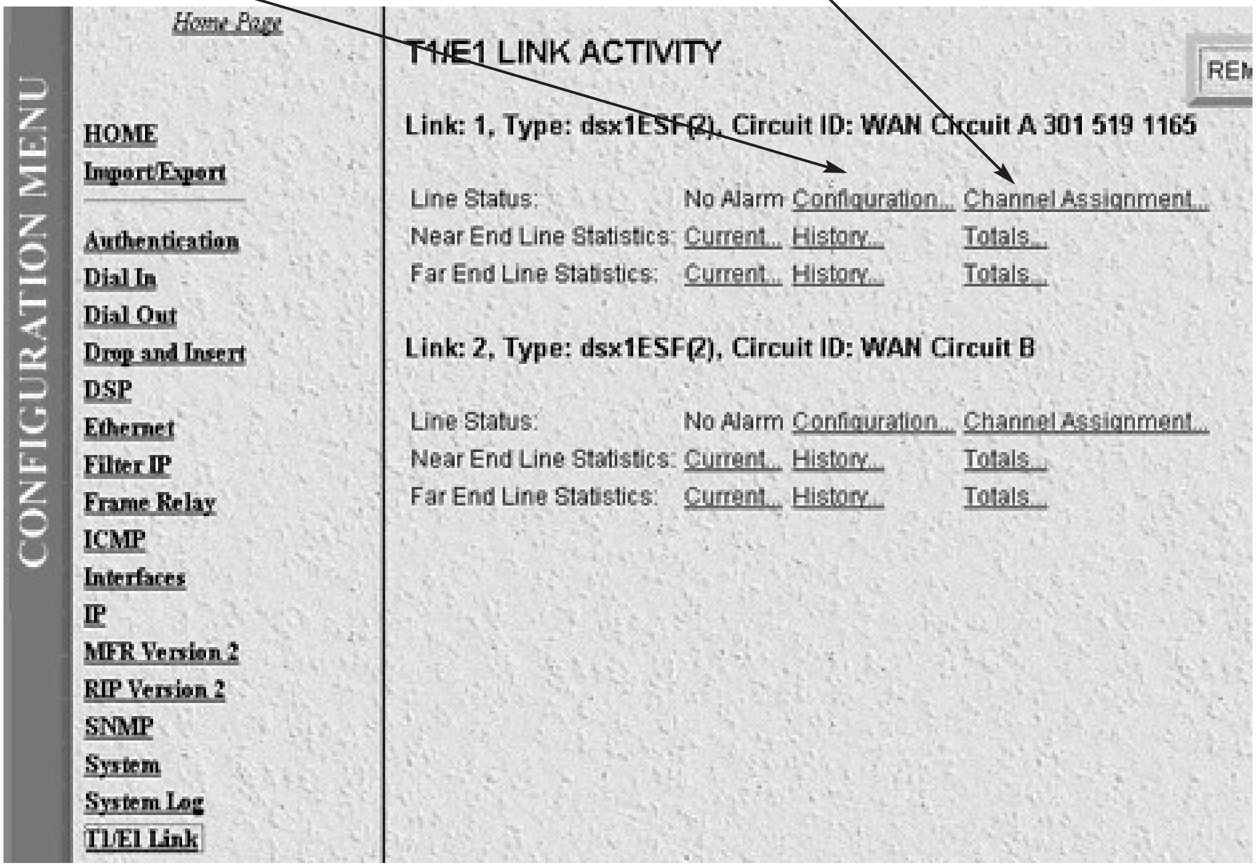
After logging on to the Server's Configuration Menu, click "**T1/E1 Link**" to configure T1/E1 Link objects.

## 4.4 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 4-2**) 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**



T1/E1 LINK ACTIVITY

Link: 1, Type: dsx1ESF(2), Circuit ID: WAN Circuit A 301 519 1165

```
Line Status:                No Alarm  Configuration...  Channel Assignment...
Near End Line Statistics:   Current...  History...      Totals...
Far End Line Statistics:    Current...  History...      Totals...
```

Link: 2, Type: dsx1ESF(2), Circuit ID: WAN Circuit B

```
Line Status:                No Alarm  Configuration...  Channel Assignment...
Near End Line Statistics:   Current...  History...      Totals...
Far End Line Statistics:    Current...  History...      Totals...
```

**Figure 4-2. T1/E1 Link Main screen.**

1. To change Configuration objects, click **Configuration**, then click **Modify** on the next screen.
2. To change Channel Assignment objects, click **Channel Assignment**.

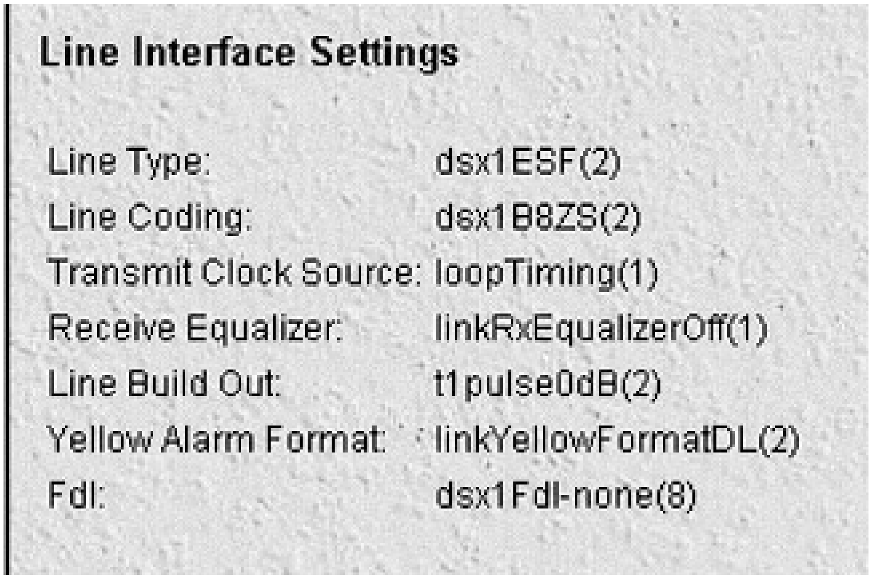
The following sections describe how to set up **Configuration** and **Channel Assignment**.

## 4.5 T1/PRI Line Interface Configuration

To receive incoming calls on a robbed-bit T1 or ISDN PRI line, you must set up the Line Interface, Test, and Signalling settings.

### 4.5.1 LINE INTERFACE SETTINGS

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



Line Interface Settings

| | |
|---|---|
| Line Type: | dsx1ESF(2) |
| Line Coding: | dsx1B8ZS(2) |
| Transmit Clock Source: | loopTiming(1) |
| Receive Equalizer: | linkRxEqualizerOff(1) |
| Line Build Out: | t1pulse0dB(2) |
| Yellow Alarm Format: | linkYellowFormatDL(2) |
| Fdl: | dsx1Fdl-none(8) |

**Figure 4-3. Line Interface Settings.**

- 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 provider's setting.  The most common options are:

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

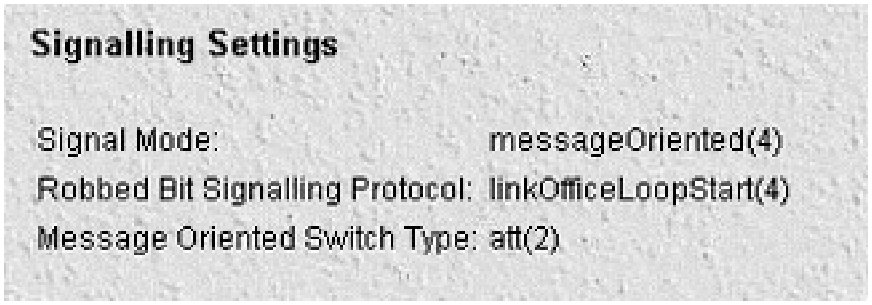
  For ISDN PRI service, set the line coding to **dsx1B8ZS**.
- Transmit Clock Source—Set this option to **loopTiming**.  This means the Server will use the network as the clock source.

- Receive Equalizer—Set this option to **linkRxEqualizerOFF** if you are within 655 feet (200 m) of the provider's network termination jack. If you are farther then 655 feet (200 m) 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.

### 4.5.2 Signalling Settings

These parameters determine how the Remote Access Server communicates with the provider's switch.



**Signalling Settings**

| | |
|---|---|
| Signal Mode: | messageOriented(4) |
| Robbed Bit Signalling Protocol: | linkOfficeLoopStart(4) |
| Message Oriented Switch Type: | att(2) |

**Figure 4-4. Signalling Settings.**

- 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 Remote Access Server will handle Yellow alarms on the T1 link. For T1s with D4/AMI settings, this should be set to **linkYellowFormatBit**. For T1s with ESF/B8ZS, this should be set to **linkYellowFormatDL**.
- Signalling Protocol—For Robbed-Bit T1s, 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 perform maintenance tests.

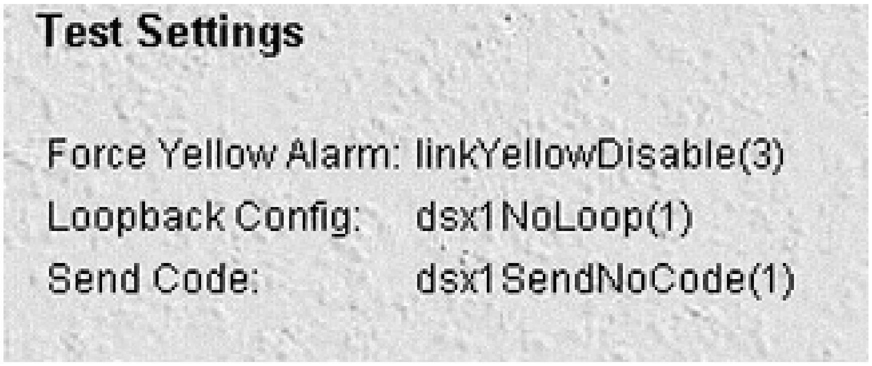
  The current standard is ANSI T1.403. Older FDL protocols can be used by selecting **dsx1Att-54016**.

  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.

### 4.5.3 Test Settings

The Remote Access Server 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 Black Box Technical Support asks you to use them. Selecting these options may disable your link or activate alarms at the central office.



Test Settings

Force Yellow Alarm: linkYellowDisable(3)
Loopback Config: dsx1NoLoop(1)
Send Code: dsx1SendNoCode(1)

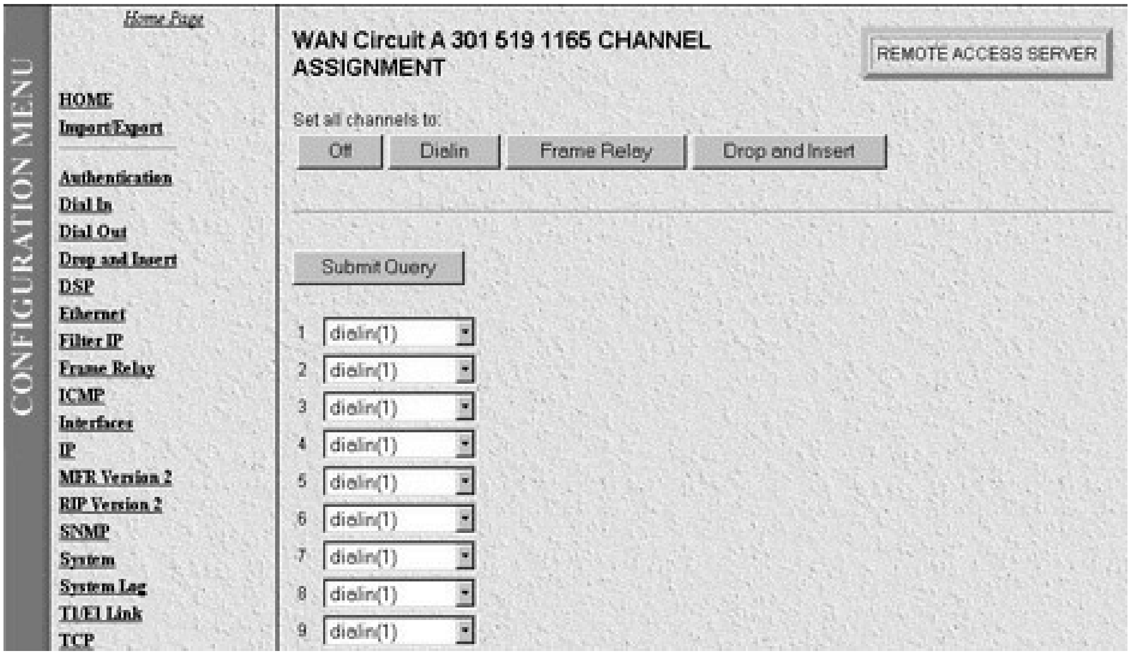
**Figure 4-5. Test Settings.**

| | |
|---|---|
| **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.

## 4.6 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.



WAN Circuit A 301 519 1165 CHANNEL ASSIGNMENT

Set all channels to:

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)

**Figure 4-6. Channel Assignment.**

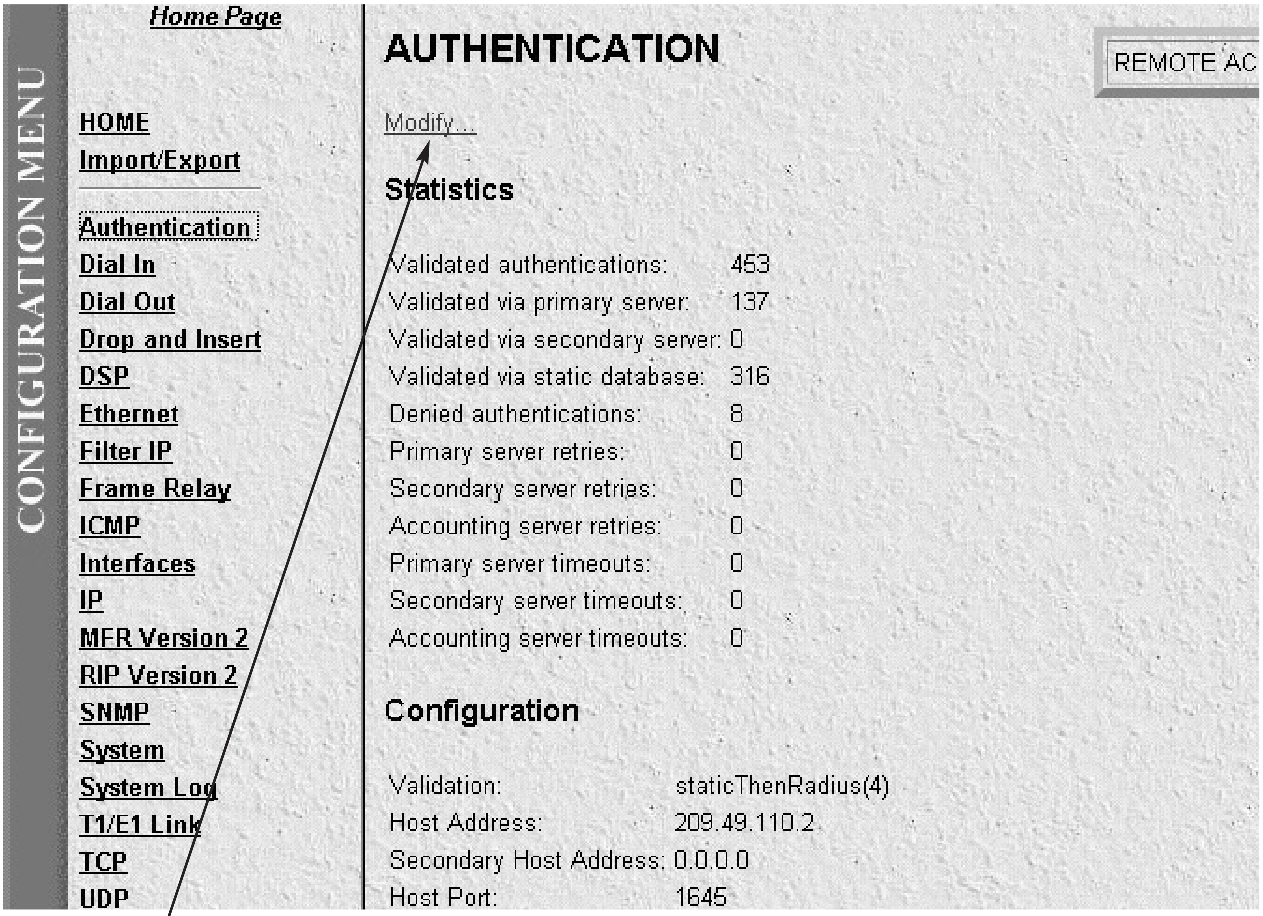
This page shows each of the available channels. Turn on each channel for dial-in service by selecting dialin for each active channel. For T1 ISDN PRI service, channel 24 is used as the signaling channel and can be left off.

You Remote Access Server is now setup and ready to receive incoming calls.

# 5. Configuring Authentication

## 5.1 Introduction to Authentication

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



AUTHENTICATION

Statistics

```
Validated authentications:      453
Validated via primary server:   137
Validated via secondary server: 0
Validated via static database:  316
Denied authentications:         8
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:              staticThenRadius(4)
Host Address:            209.49.110.2
Secondary Host Address:  0.0.0.0
Host Port:               1645
```

**Figure 5-1. Authentication Main Screen.**

Select Modify to change Remote Access Server Authentication parameters.

## 5.2 Selecting the Authentication Method

After selecting Modify, you must choose the method the Remote Access Server will use to validate users. Pull down the Validation sub-section and select from one of the available choices (see **Figure 5-2**). Following **Figure 5-2** are descriptions for each variable on this page.

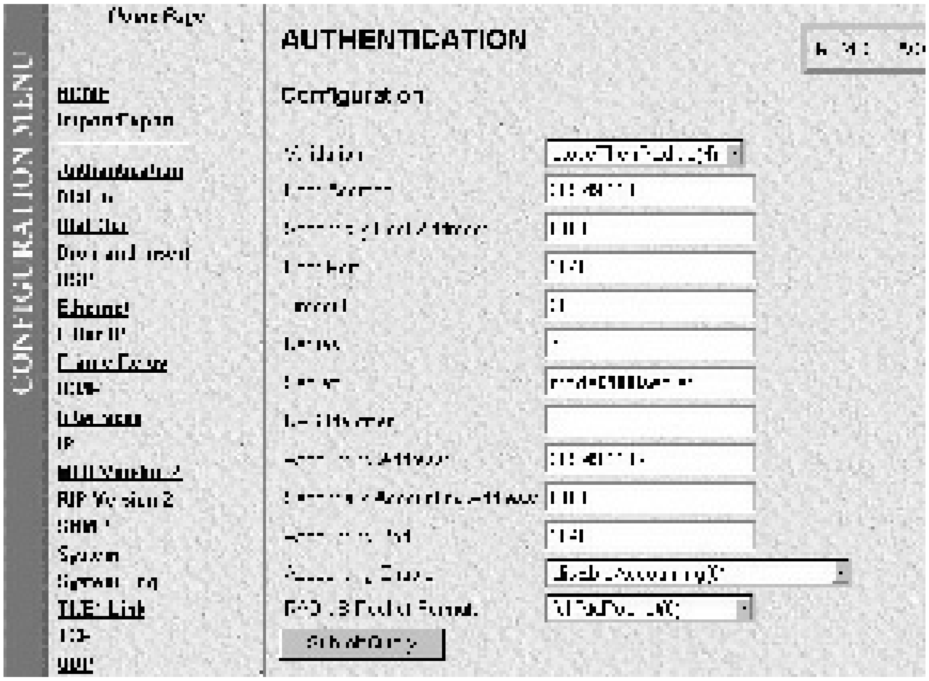


**Figure 5-2. Authentication—Validation screen.**

- **Validation (auValidation)**—Selects how the Server will authenticate an incoming call. Select from:

- **No Validation(0)**—Select this to allow un-authenticated calls into the Remote Access Server, and on to your LAN, using the default service.

- **static Users(1)**—Use the Server's internal user database only to authenticate. Static users are users and passwords entered into the Server'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 offer an excellent method for managing user dial-in security. Any RADIUS entries will require an associated server to process authentication requests from the Server or the Server will reject users' access. For more information about RADIUS, see RADIUS User Authentication, in **Section 5.5**.

- **tacacs Users(3)**—This option had no effect in the current version. It is included to make room for future upgrades.

- **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)**—This option had no effect in the current version. It is included to make room for future upgrades.

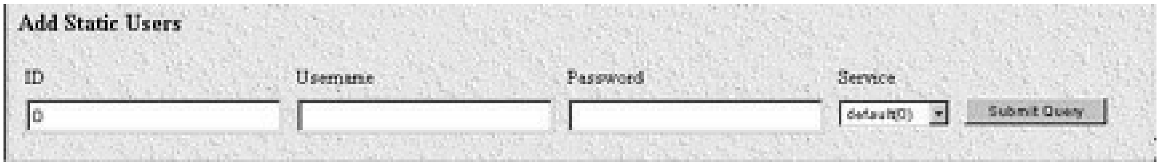
## NOTE

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

- **Host Address (auHostAddress)**—tells the Remote Access Server the IP address of the external 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 Remote Access Server 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 Server will retransmit an authentication request to an external authentication server.
- **Retries (auRetries)**—This option specifies the number of times the Server 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 (Server) and the authentication server (RADIUS). It is used to secure communication between the client and server. The secret on the Remote Access Server 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 Server to the remote authentication server. If this option is blank, then the Server will use its IP address to identify itself to the remote server.
- **Acct Address (auAcctAddress)**—This 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)**—This is the UDP port on the accounting server specified in Acct Address that the Server 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)**—This is a switch which lets you enable or disable the reporting of accounting information on the Server. Select **enableAccounting** to begin accounting of RADIUS authenticated users. Select **disableAccounting** to disable the accounting feature.

## 5.3 Static User Authentication

Static users are simply users and passwords entered into the Server's internal users database. The Server database will accept up to 100 users (see **Figure 5-3**). You must have superuser access make changes to the static user database. Following **Figure 5-3** are descriptions for each variable on this page.



Add Static Users

| ID | Username | Password | Service |
|---|---|---|---|
| 0 | | | default(0) |

**Figure 5-3. Authentication—Static User Identification Setup.**

- **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 the user database.
- **Username (suUsername)**—This is a unique name, to be provided at login time.
- **Password (suPassword)**—This is the password for the user entered in "Username."
- **Service (suService)**—This option instructs the Server 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 Server to Rlogin into another specified host. |
| telnet | Causes the Server to Telnet into another specified host. |
| ppp | Server will to negotiate a PPP session. |
| cppp | Server will to negotiate a Compressed-PPP session (see note below). |
| slip | Server will negotiate a SLIP connection. |
| cslip | Server will negotiate a Compressed-SLIP connection. |
| dialout | Server will give a dialout connection. The dialout connection is an AT command set driven connection into one of the Server modems. On line help is provided by typing "at help <cr>." |

## NOTE

**If a user attempts to login in using a service different from the one he/she has been provisioned with, the Server 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 the Username.
3. Enter the Password.
4. Select the Service type for the user.
5. Select Submit to store the user information.

## NOTE

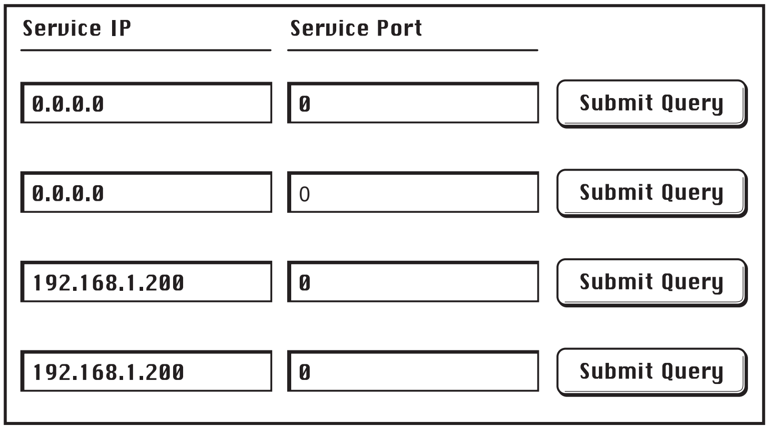
**All changes made to the running configuration must be saved to flash by selecting Record Current Configuration under Immediate Actions on the HOME page of the Server. Failure to do so will cause all configuration information to be lost the next time the Server is re-booted.**

- **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.

## 5.4 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 5-4**). Following **Figure 5-4** are descriptions for each variable on this page.



| 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 |

**Figure 5-4. Authentication—Rlogin and Telnet Users.**

- **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 and changes have been completed, select Submit to save the user in the current running configuration.

### NOTE

**All changes 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 Server. Failure to do so will cause all configuration information to be lost the next time the Server is re-booted.**

## 5.5 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 provide an excellent method for managing user dial-in security. Any RADIUS entries will require an associated server to process authentication requests from the Server or the Server will reject the user's access.

### 5.5.1 How RADIUS Works

RADIUS is a client-server authentication system that consists of two parts:

1. The RADIUS client (your Remote Access Server).
2. RADIUS server.

The server is installed on one or more central computers that 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, 1812; for RADIUS accounting, 1813.

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

Here is the typical sequence of events the Remote Access Server uses to authenticate a user with RADIUS:

1. A user dials in to the Server.
2. The Server obtains the username and password. This can be through the Server 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 Server has the username and password, the Server 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 that the user 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 specified length of time, the request is re-sent a number of times. The timeout and number of times the Server will retry is determined by the TIMEOUT and RETRIES options in the Server configuration. Once the RADIUS server receives the request, it will first validate the Server initiating the request. A request from a Server for which the RADIUS and the Server'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, the 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 what host the user should be connected to (Telnet) or what port and service the user is allowed. If any condition is not met, the RADIUS server sends an access-reject response indicating that the user request is invalid.

### 5.5.2 Integrating RADIUS

To use the Server 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 Server can be routed to and from the RADIUS server. This allows a centrally located RADIUS server to authenticate multiple Servers in remote POPs, using the Internet to pass the IP packets.**

### 5.5.3 Starting the RADIUS Daemon

Install the RADIUS binaries as per the instructions. To start the RADIUS daemon, from the command line enter RADIUSD. The RADIUS daemon has many options that 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 bring 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 an 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.

### 5.5.4 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 Server and the shared secret. Here is the format:

**client shared secret**

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

There is no limit to the number of clients a RADIUS daemon can handle. This allows a single server to authenticate many Remote Access Servers.

*Application Tips*

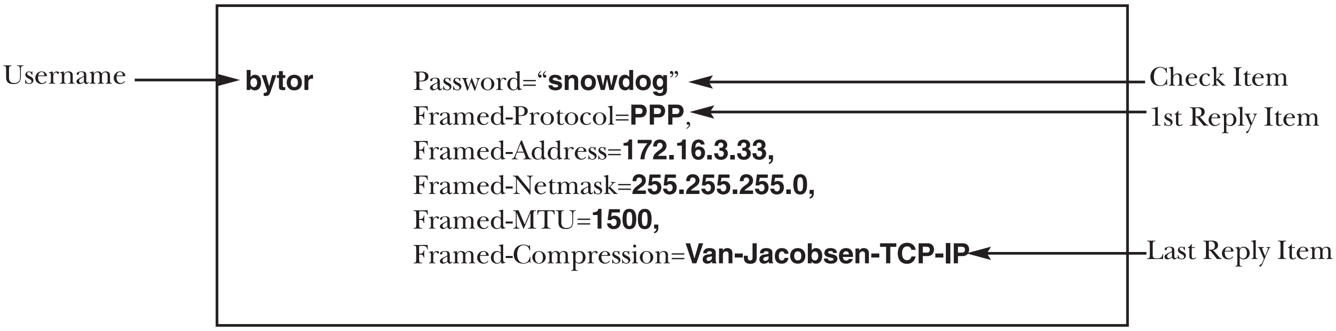
- *As an example of a static ThenRadius option of authentication, a network administrator can program several admin. status user IDs with the bulk of the dial-up users authentication going to RADIUS. This allows the network administrator access to the Remote Access Server and the network in case the RADIUS server is down.*
- *As an example to allow RADIUS to authenticate a PPP or SLIP user, the Server can give out an IP address to the dial-in user. Under <Dial-IN>—><Settings> set the default IP address pool using your local IP addresses. In the RADIUS users file, add the following:*

| | |
|---|---|
| username | Password="**userpassword**" |
| User-Service-Type | **Framed-User** |

### 5.5.5 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
```

**Figure 5-5. Example of a RADIUS User Entry.**

- **Username**—The username ("bytor" in the example above) 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 Server or to a specific interface on a Server. 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 Server 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.

## 5.6 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 Server. You must enable Server mode accounting by selecting Accounting Enable (auAccountingEnable) on the Authentication page.

### 5.6.1 How RADIUS Accounting Works

RADIUS accounting consists of an accounting server and accounting clients. 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 Server Accounting Port determines which port the Server 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 Server 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 Server to acknowledge receipt of the request.

3. If the Server 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 Server 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.**

**Figure 5-6** shows an example of a Server 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 17 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
```

**Figure 5-6. Example of RADIUS Accounting Start and Stop Information.**

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

### 5.6.2 Listing of RADIUS Accounting 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.
4. Access-Challenge—The RADIUS server may send the user a challenge requiring a response.

Within these packets there are attributes that carry specific authentication, authorization, information, and configuration details for the request. When the Server 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 Server will act on those changes. If a service (for example, Framed User) is specified, then the Server will default to the link default.

The listing below describes the configuration options as used in the /etc/raddb/users file that will work on the Server. 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

**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*
Description: 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 requesting authentication of the user.
Message Type: Access-Request

**NOTE**

**The Server port numbers range for a T1 system is 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 (below) for specifying a particular Protocol).

**Framed-Protocol (7)** *integer*
Description: Indicates the the framed protocol to be 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

**NOTE**

**If the IP address is 255.255.255.255, then the Server will allow the user to specify the address. If the address is 255.255.255.254, then the Remote Access Server will assign an IP from the IP pool of addresses in the Server.**

**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 configured 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 Server which system to connect users to.
Message Type: Access-Request and Access-Accept

**Login-Service (15)** *integer*
Description: This attribute indicates the service that 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 user 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 that 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 Server 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 Server.
Message Type: Access-Accept and Access-Request

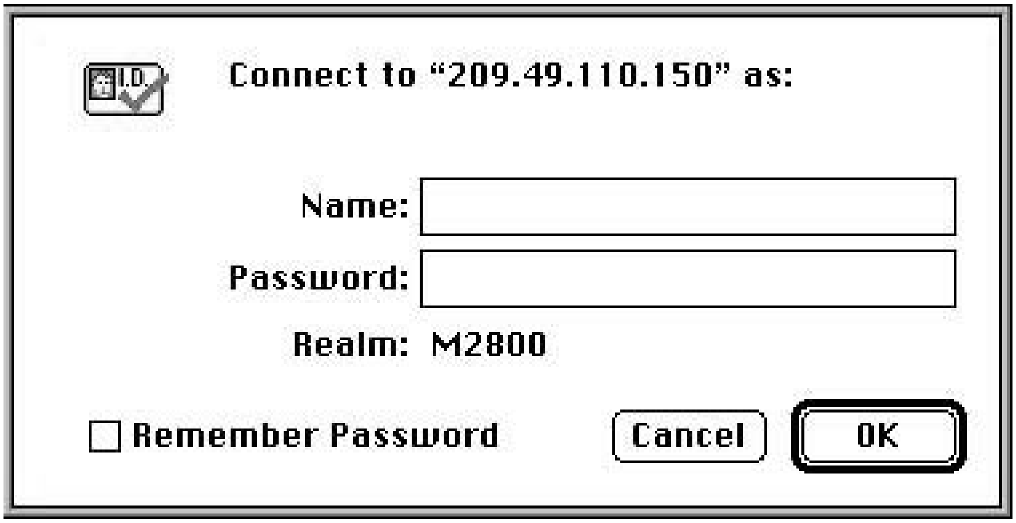
# Appendix: Using the Internal HTML Management Pages

## A.1 Introduction to the Internal HTTP/HTML Management Pages

You may configure the Remote Access Server 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 Server. If you plan to access this product via the Internet, your system administrator will need to acquire a registered IP address from the InterNIC. If not, the system administrator can make up his own IP address based on his own addressing schemes.

### A.1.1 Logging Into the HTTP/HTML Pages

To log into the HTTP/HTML Management pages, you must enter the 4-octet IP address (for example, 192.168.15.12) as the URL (Universal Resource Locator) into a Web browser. After you enter the IP address, the Server will ask for your user name and password. **Figure A-1** shows an example of the Login Screen.



Connect to “209.49.110.150” as:

Realm: M2800

**Figure A-1. Login Screen.**

There are two levels of administration passwords associated with the operation of your Remote Access Server. They are: **1. superuser**: allows full permission to change and view any parameters in the Server; and **2. monitor**: allows full viewing of any variables that are not protected by the superuser password. We suggest that you change these passwords immediately after initial configuration.

### A.1.2 HTTP/HTML and SNMP Object Format

Starting on **page 129**, we describe variables on each of the internal HTTP/HTML pages, including brief descriptions of the Enterprise MIB or SNMP MIB II object identifiers wherever pertinent.

### A.1.3 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:

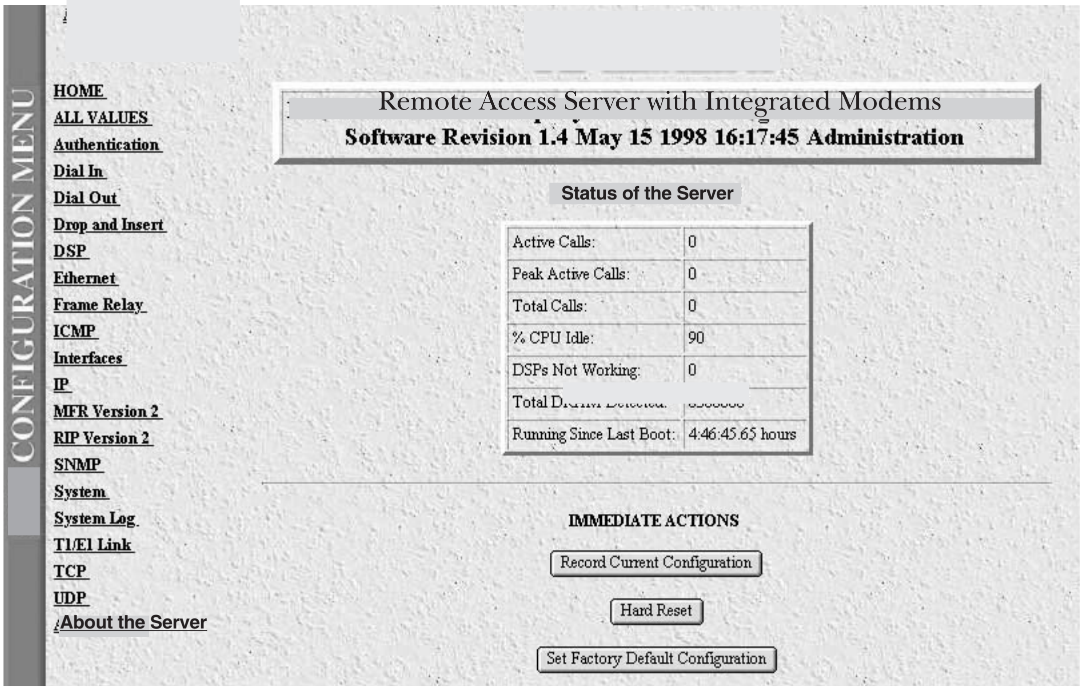
1. Select the appropriate Modify screen.
2. Make the change to the parameter.
3. Select Submit.
4. Return to the HOME screen.
5. Select Record Current Configuration.

## NOTE

**If you don't save changes as shown above, you will lose them when you power-cycle the Remote Access Server.**

## A.2 Home

HOME is the first HTTP/HTML page that you will reach after you log into the Remote Access Server. 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.



Remote Access Server with Integrated Modems

**Software Revision 1.4 May 15 1998 16:17:45 Administration**

**Status of the Server**

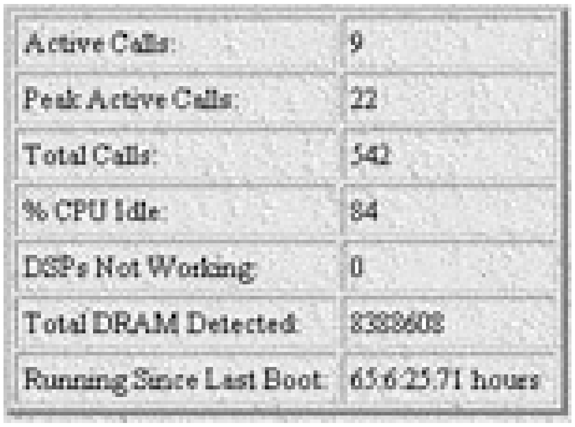
| | |
|---|---|
| Active Calls: | 0 |
| Peak Active Calls: | 0 |
| Total Calls: | 0 |
| % CPU Idle: | 90 |
| DSPs Not Working: | 0 |
| Total D[illegible] | [illegible] |
| Running Since Last Boot: | 4:46:45.65 hours |

**IMMEDIATE ACTIONS**

Figure A-2. Home Page.

### A.2.1 Operating Status Variables

There are seven system variables that describe the immediate operating status of the Remote Access Server. These variables are shown in **Figure A-3** and are described in the section that follows.



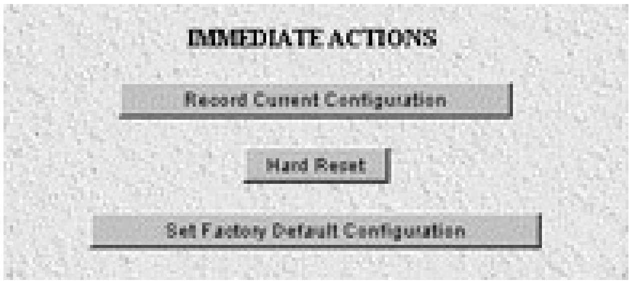
| | |
|---|---|
| Active Calls: | 9 |
| Peak Active Calls: | 22 |
| Total Calls: | 542 |
| % CPU Idle: | 84 |
| DSPs Not Working: | 0 |
| Total DRAM Detected: | 8388608 |
| Running Since Last Boot: | 65:6:25.71 hours |

**Figure A-3. STATUS Menu.**

- **Active Calls (diActive)**—This number, ranging from 0 to 60, displays the total number of calls being processed (connecting, dead, authenticating, etc.) in a Server at the time the HOME page was brought up.
- **Peak Active Calls (diMaxActive)**—The maximum number of active calls at one time.
- **Percentage CPU Idle (boxIdleTime)**—The amount of system CPU power that is not being used by the Remote Access Server. 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 DSPs in the Remote Access Server 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, since the Server will automatically remove the non-working DSP from the resource pool. One symptom of a DSP failure is that the Server isn't handling as many calls as it should. A DSP may be taken out of service if it fails to respond to the Server 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 Remote Access Server has been running since the it was last reset. It displays the number of hours and rolls over after 1,193 hours (497 days).

### A.2.2 Immediate Actions

Immediate actions, which can be executed only in superuser mode, take effect as soon as the command is executed.


IMMEDIATE ACTIONS

Record Current Configuration
Hard Reset
Set Factory Default Configuration

**Figure A-4. Immediate Actions.**

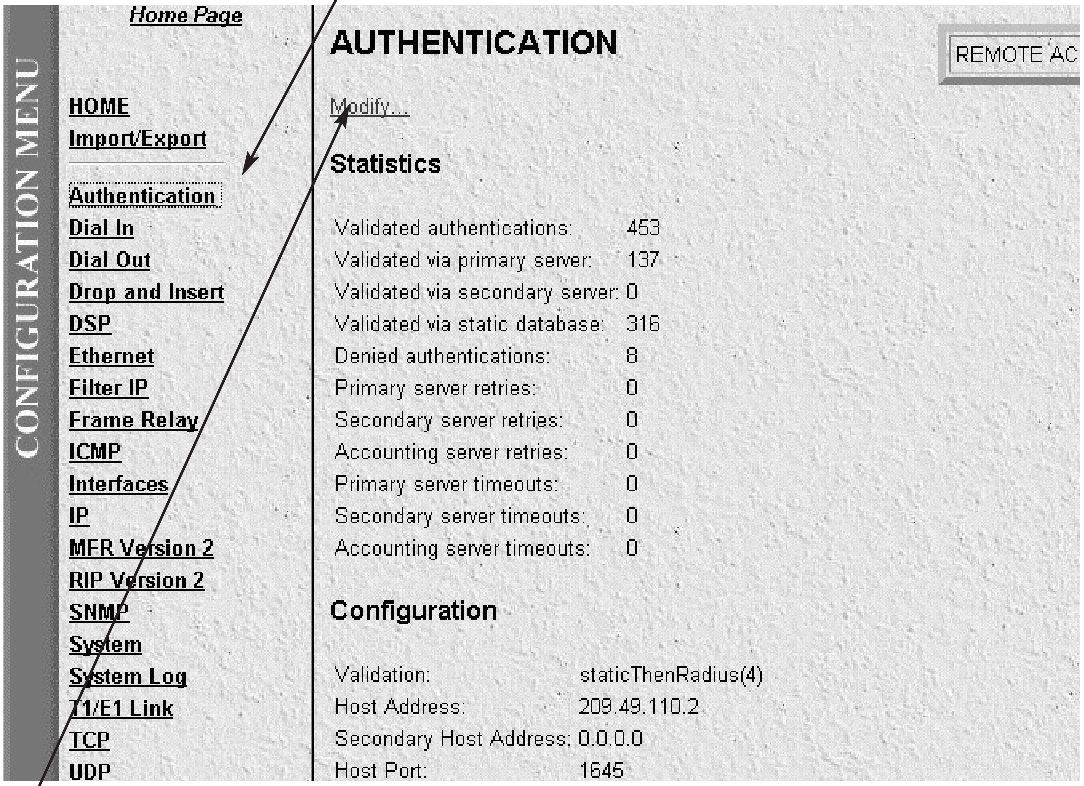
- **Record Current Configuration**—RECORD CURRENT CONFIGURATION causes the current configuration to be stored in flash memory. Any changes made to the Remote Access Server configuration are stored in non-volatile RAM first. This allows you to set the box up with a working configuration before commiting 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 Server is re-booted.
- **Hard Reset**—HARD RESET causes the Remote Access Server to restart. When you select HARD RESET, the Server confirms that you want to execute this command. Then, the Server will disconnect all current sessions, re-initialize the interfaces, and re-load configuration parameters from flash.
- **Set Factory 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 Server until it is re-booted.

## NOTE

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

## A.3 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 Server 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 Server Configuration Menu as shown below. This section describes Static User and RADIUS parameters.



AUTHENTICATION

Statistics

Validated authentications: 453
Validated via primary server: 137
Validated via secondary server: 0
Validated via static database: 316
Denied authentications: 8
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: staticThenRadius(4)
Host Address: 209.49.110.2
Secondary Host Address: 0.0.0.0
Host Port: 1645

**Figure A-5. Authentication Main Screen.**

Select Modify to set up or change Server Authentication parameters.

### A.3.1 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 retries (auPrimaryServerRetries)**—The number of authentication attempts made by the Server to the primary RADIUS authentication server.
- **Secondary server retrys (auSecondaryServerRetrys)**—The number of authentication attempts made by the Server to the secondary RADIUS authentication server.
- **Accounting server retries (auAccountingServerRetries)**—The number of accounting attempts made by the Server 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.

### A.3.2 Configuration (Static and RADIUS)

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)**), configure the additional parameters as shown in **Figure A-6** to configure RADIUS parameters.

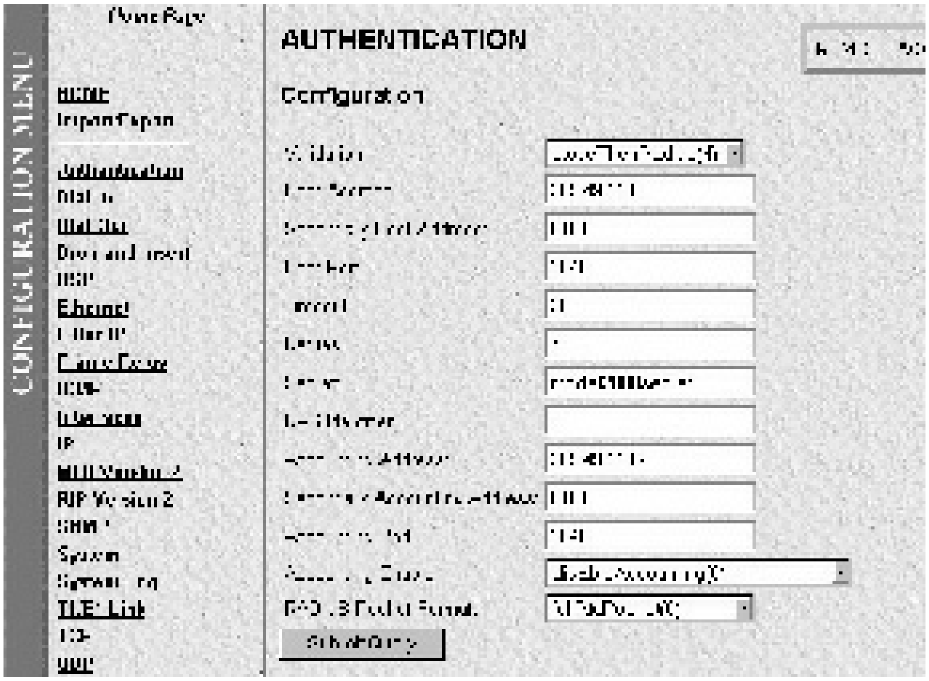


**Figure A-6. Configuration Screen.**

- **Validation (auValidation)**—Selects how the Server will authenticate an incoming call. Select from:

  **No Validation(0)**—Select this to allow un-authenticated calls into the Server, and onto your LAN, using the default service.

  **static Users(1)**—Use the Server's internal user database only to authenticate. Static users are simply users and passwords entered into the Server'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 they're an excellent method for managing user dial-in security. Any RADIUS entries will require an associated server to process authentication requests from the Server or the Server will reject users' access. For more information about RADIUS, see RADIUS User Authentication.

  **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 Server the IP address of the external authentication server. This must be the IP since the Server 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 Server 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 Server will retransmit an authentication request to an external authentication server.

- **Retries (auRetries)**—This option specifies the number of times the Server will resend an authentication request to a RADIUS server after a timeout occurs. If this number is exceeded, the user will be rejected.

- **Secret (auSecret)**—The Secret variable sets the shared secret between the authentication client (Remote Access Server) 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 Remote Access Server 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 Remote Access Server to the remote authentication server. If this option is blank, then the Remote Access Server will use its IP address to identify itself to the remote server.

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

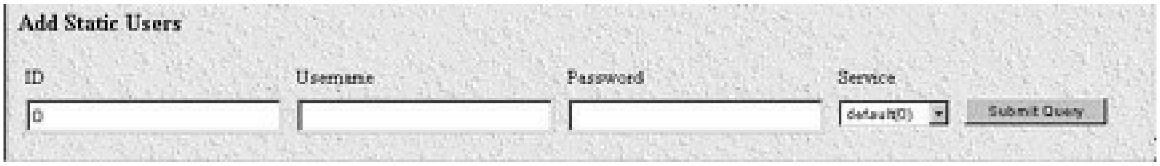
- **Secondary Acct Address (auSecondaryAcctAddress)**—When using a remote accounting server (such as RADIUS Accounting), this variable provides the IP address of the accounting server.

- **Acct Port (auAcctPort)**—This is the UDP port on the accounting server specified in Acct Address that the Server 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)**—This is a switch that allows the enabling or disabling of the reporting of accounting information on the Server. Select enableAccounting to begin accounting of RADIUS authenticated users. Select disableAccounting to disable the accounting feature.

### A.3.3 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 Server's internal users database. You may add up to are 100 static users in the Server (see **Figure A-7**). You must have superuser access make changes to the static user database. Following **Figure A-7** are descriptions for each variable on this page.



Add Static Users

| ID | Username | Password | Service |
|---|---|---|---|
| 0 | | | default(0) |

**Figure A-7. Static User Identification Setup.**

- **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 for the user entered in the "Username."

- **Service (suService)**—This option instructs the Server 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 Server to rlogin into another host.
telnet: Causes the Server to telnet into another host.
ppp: Server will try to negotiate a PPP session.
cppp: Server will try to negotiage a Compressed-PPP session (see note below).
slip: Server will negotiate a SLIP connection.
cslip: Server will negotiate a Compressed-SLIP connection.
dialout: Server will give a dialout connection. The dialout connection is an AT-command-set-driven connection into one of the Server's modems. On-line help is provided when you type "at help <cr>."

## NOTE

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

## NOTE

**Save all changes to the running configuration to flash by selecting "Record Current Configuration" under Immediate Actions on the HOME page of the Server. If you don't, the next time you reboot the Server, the changes to your configuration will be lost.**

- **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).

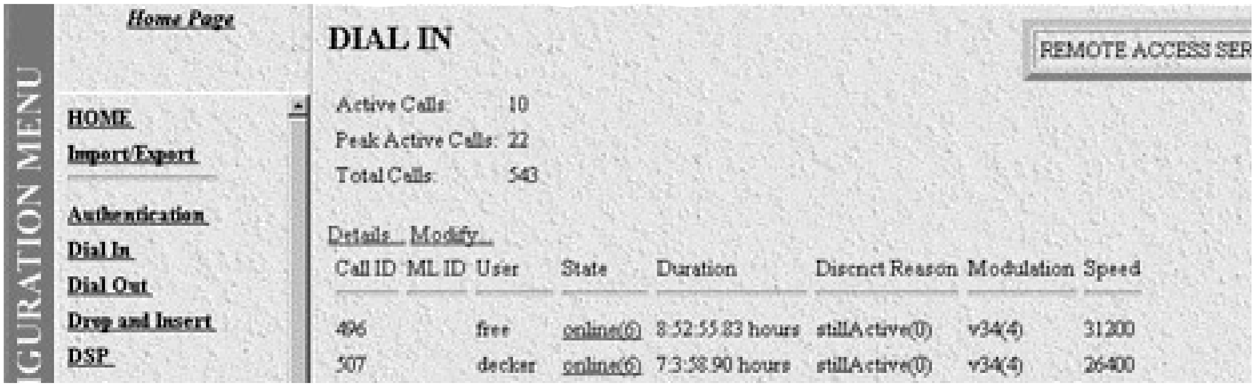
## NOTE

**Save all changes to the running configuration to flash by selecting "Record Current Configuration" under Immediate Actions on the HOME page of the Server. If you don't, the next time you reboot the Server the changes to your configuration will be lost.**

## A.4 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 Server Configuration Menu (see **Figure A-8**). Following **Figure A-8** are descriptions for each variable.



DIAL IN

Active Calls: 10

Peak Active Calls: 22

Total Calls: 543

Details Modify

| Call ID | ML ID | User | State | Duration | Discnct Reason | Modulation | Speed |
|---|---|---|---|---|---|---|---|
| 496 | | free | online(6) | 8:52:55.83 hours | stillActive(0) | v34(4) | 31200 |
| 507 | | decker | online(6) | 7:3:58.90 hours | stillActive(0) | v34(4) | 26400 |

**Figure A-8. Dial In Main Screen.**

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 Statistic**s: show statistics for individual users. 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 user's state, and time that the user has been on the Server.
- **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 Remote Access Server, it can be in one of five states.

1. **Ringing**—The call has been recognized by the Server and is in the process of going off hook.
2. **Connecting**—The unit has assigned a DSP to the incoming call and is now in the process of negotiation of the type of modem modulation: V.34, V.32, ISDN, or 56K.
3. **Authenticating**—The Server is in the process of verifying the users' passwords by using the static or Radius authentication.

4. **Online**—The Server has completed authentication and you are ready to browse the Web.

5. **Dead**—The user has been disconnected. 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.

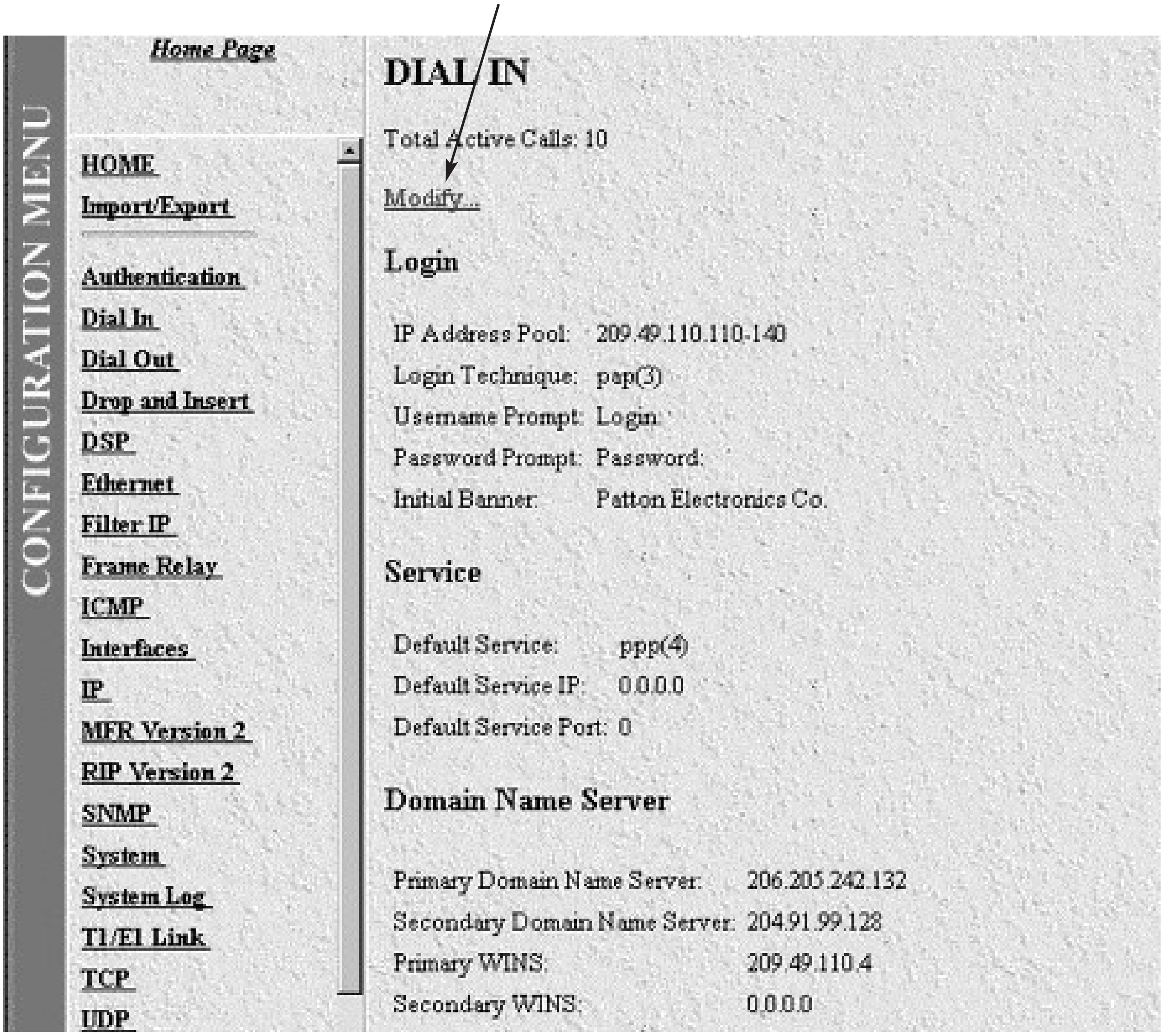
- **Connect Mod (diactModulation)**—The modulation of the link.

  **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.

### A.4.1 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**.



DIAL IN

Total Active Calls: 10

Login

IP Address Pool: 209.49.110.110-140
Login Technique: pap(3)
Username Prompt: Login
Password Prompt: Password:
Initial Banner: Patton Electronics Co.

Service

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

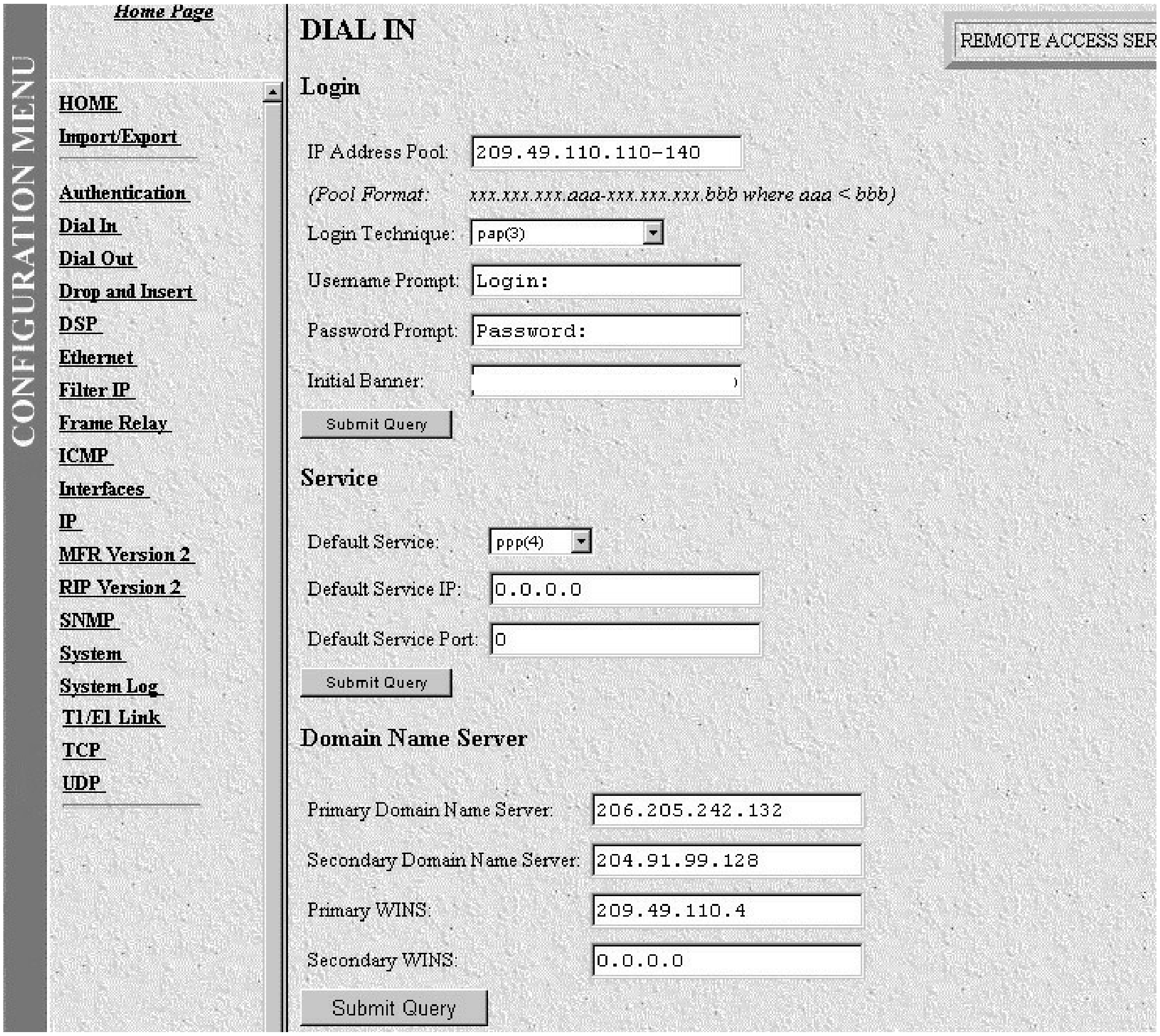
Domain Name Server

Primary Domain Name Server: 206.205.242.132
Secondary Domain Name Server: 204.91.99.128
Primary WINS: 209.49.110.4
Secondary WINS: 0.0.0.0

**Figure A-9. Dial In Details.**

***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**). To reach this screen, select Modify from the main Dial In Details screen.



DIAL IN

Login

IP Address Pool: 209.49.110.110-140

(Pool Format: xxx.xxx.xxx.aaa-xxx.xxx.xxx.bbb where aaa < bbb)

Login Technique: pap(3)

Username Prompt: Login:

Password Prompt: Password:

Initial Banner:

Service

Default Service: ppp(4)

Default Service IP: 0.0.0.0

Default Service Port: 0

Domain Name Server

Primary Domain Name Server: 206.205.242.132

Secondary Domain Name Server: 204.91.99.128

Primary WINS: 209.49.110.4

Secondary WINS: 0.0.0.0

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

*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 209.49.110.110-140. This is the string describing the IP address pool that will be used by this Remote Access Server. You can mix IP networks for example: 209.49.110.151-155 209.49.110.160-165.

- **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

**A user who is not configured for PAP 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

**A user who is not configured for CHAP 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 user's 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 display initially for the user. 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 and if no service is specified on the static users list under Authentication. See Authentication.

  The options are

  **rlogin(1)** User will be automatically given an rlogin prompt.<br>
  **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 that 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 that 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 |

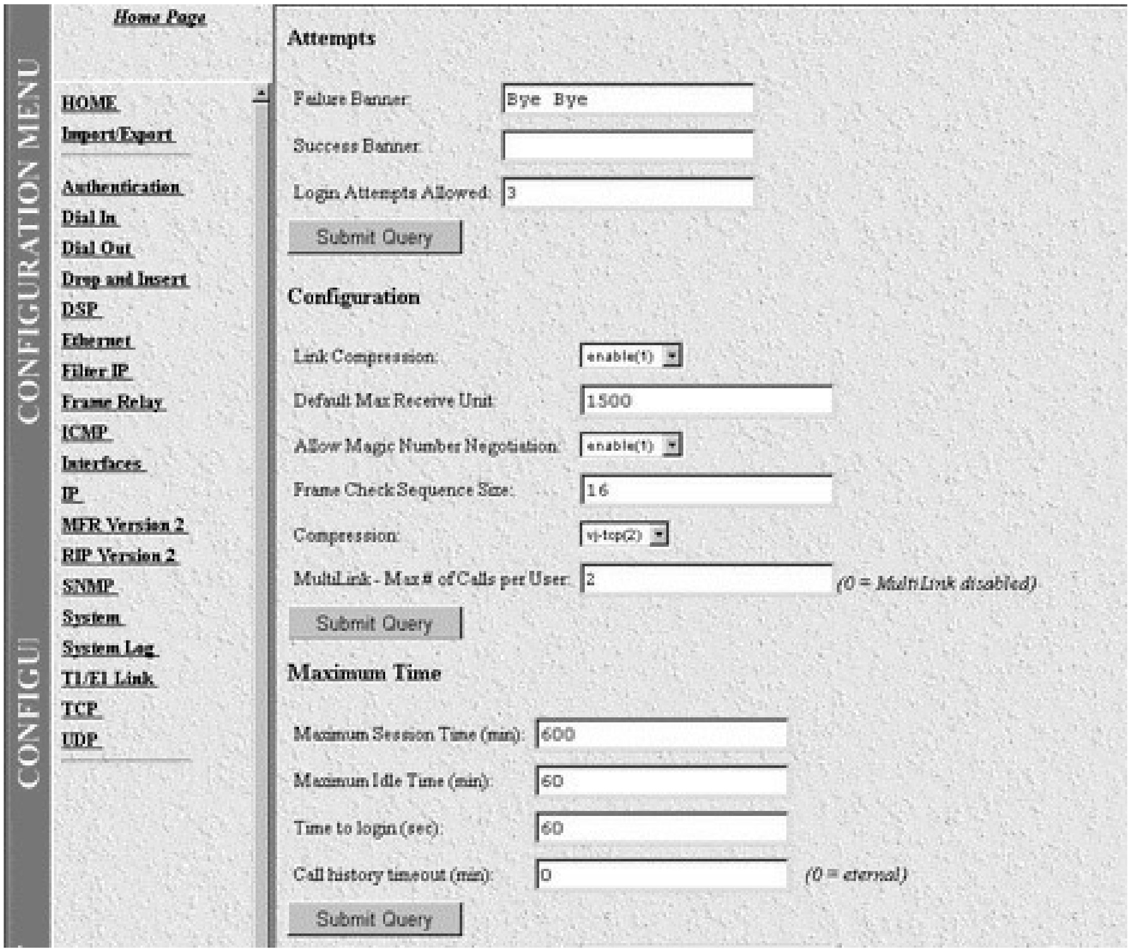
*Domain Name Server*

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). It's the first place to try to resolve host names—for example, IP address 204.91.99.128.
- **Secondary Domain (diSecondaryDNS)**—The secondary domain name server address to pass to the caller (Win95 PPP). It's 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). It's the Windows Internet Naming Service (WINS).
- **Secondary WINS (diSecondaryWINS)**—The secondary Windows name server address to pass to the caller (Win95 PPP). It's 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**). To reach this screen, scroll down from the previous screen.



Attempts

Failure Banner: Bye Bye

Success Banner:

Login Attempts Allowed: 3

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)

MultiLink - Max # of Calls per User: 2 (0 = MultiLink disabled)

Maximum Time

Maximum Session Time (min): 600

Maximum Idle Time (min): 60

Time to login (sec): 60

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

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

*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. The Text string can be 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 on both ends of the link. When disabled, the PPP negotiations will FORCE “no compression” on the PPP link. This is a default setting that 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 asynchronous 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 the receive side of the link will be a combination of the local node's pppLinkConfigReceiveACCMap and the remote node's pppLinkConfigTransmitACCMap. Changing this object will take effect when the link is next restarted.
- **Transmit ACC Map (diConfigTransmitACCMap)**—Desired asynchronous 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)**—The local node will attempt to perform Magic Number negotiation with the remote node.
- **disable(2)**—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 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 Van Jacobsen TCP/IP header compression. 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)**

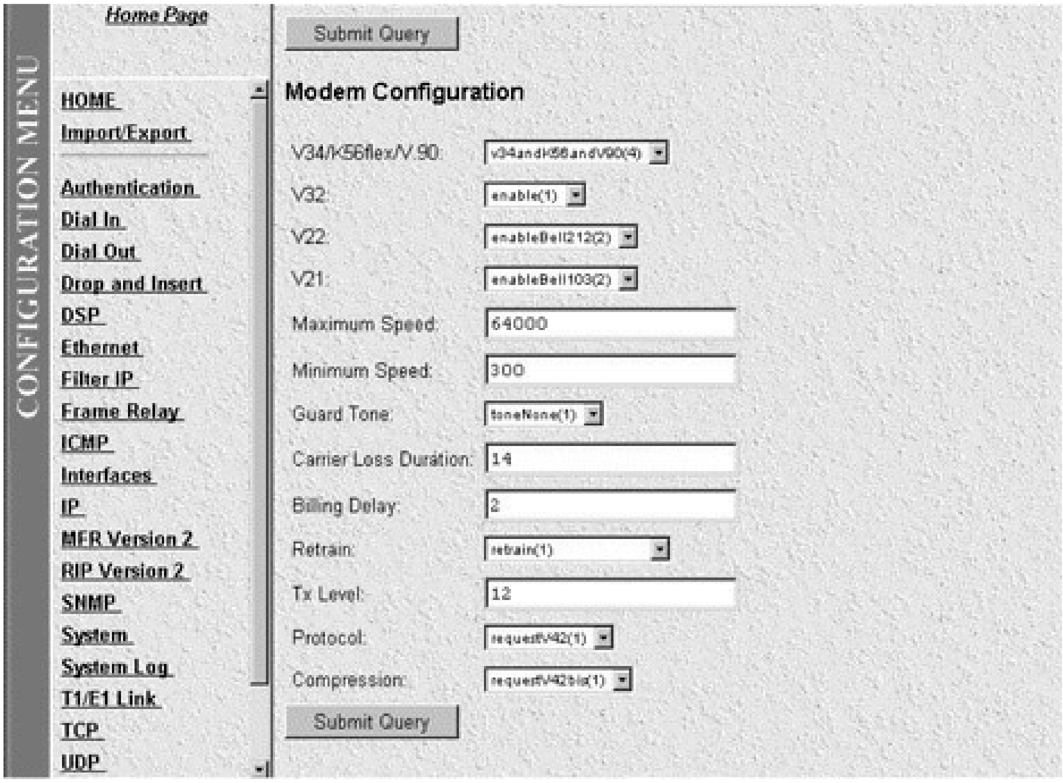
*Maximum Time*

This section contains the timeout for the session, the maximum idle time, the time to login, and the MIB-data linger time.

- **Maximum Session Time (min) (diSessionTimeout)**—This is the maximum time in minutes that 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 that may be overridden by the authentication of a specific user.
- **Maximum Idle Time (min) (diIdleTimeout)**—This is the maximum time in minutes that 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 that may be overridden by the authentication of a specific user.
- **Time to login (sec) (diLoginTimeout)**—This is the maximum time in seconds that a user is given to log in. This is only relevant before the user is authenticated. This setting should take into account any time you need to query a remote authentication server such as a RADIUS server.
- **Call History Timeout (sec) (diLingerTime)**—Number of seconds an 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**). To reach this screen, scroll down from the previous screen.



Modem Configuration

| | |
|---|---|
| V34/K56flex/V.90: | v34andK56andV90(4) |
| V32: | enable(1) |
| V22: | enableBell212(2) |
| V21: | enableBell103(2) |
| Maximum Speed: | 64000 |
| 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) |

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

*Modem Configuration*

Use this section to select the modem connection 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 lets you select 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 lets you select 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 you can insert one. This operates for Phase Shift Key modulations only, not for V.32 or V.34.

  **toneNone(1)**
  **tone1800(3)**

- **CarrierLossDuration (diModemCarrierLossDuration)**—The number of 100-ms intervals the carrier must lose before the connection is considered broken. A setting of 255 indicates forever. The range is 1 through 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, fall back, 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.
- **Protocol (diModemProtocol)**—Selection of the data protocol to use on the modem. This lets you request or force V.42 error-correction protocol.

**Direct(0)**—No error correction will be used.

**requestV42(1)**—Enable V.42. If you select this, then the modem will negotiate V.42 or no correction.

**requireV42(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 you to request or force V.42 compression protocol. This will only be used if V.42 error correction is active.

**Direct(0)**—No compression will be used.

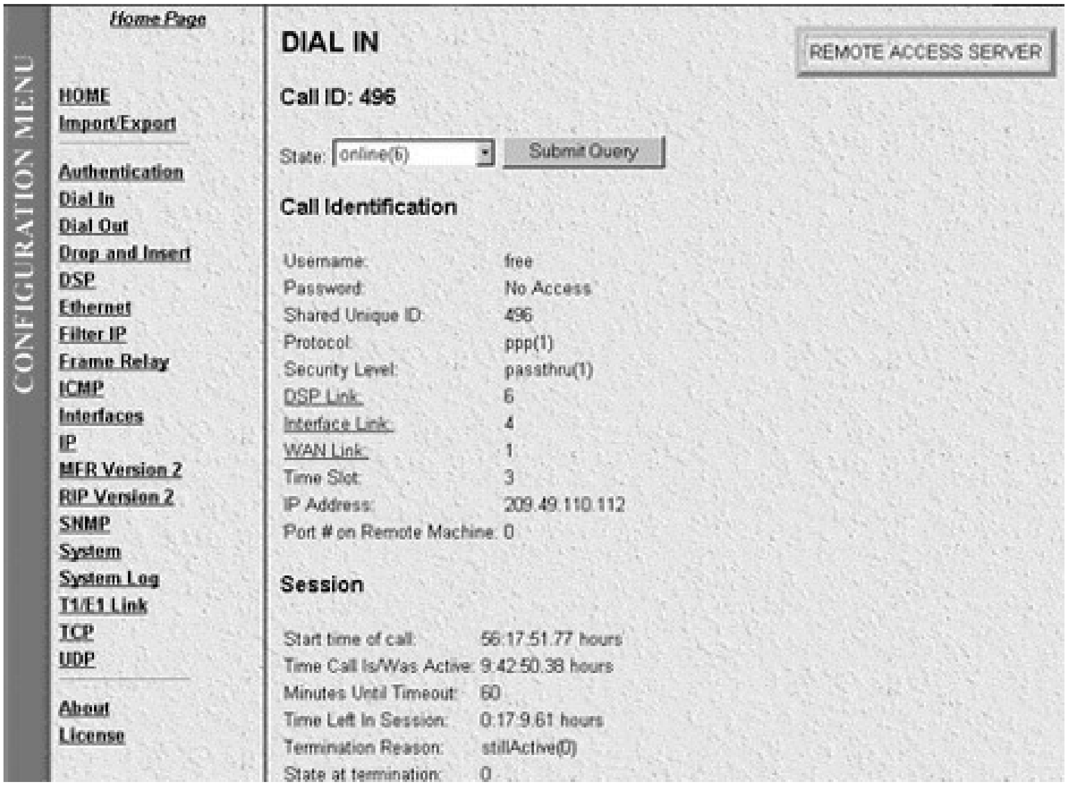
**requestV42bis(1)**—Enable V.42bis. If you select this, then the modem will negotiate V42bis or no correction.

**requestV42bis(2)**—V.42bis is mandatory. If this is not a V.42bis modem, then disconnect.

### A.4.2 User Statistics

*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** shows user information for a Unique ID. The Headings DSP Link, Interface Link, WAN Link, and Time Slice Link 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 Server Configuration Menu.



DIAL IN

Call ID: 496

State: online(6)

Call Identification

```
Username:                  free
Password:                  No Access
Shared Unique ID:          496
Protocol:                  ppp(1)
Security Level:            passthru(1)
DSP Link:                  6
Interface Link:            4
WAN Link:                  1
Time Slot:                 3
IP Address:                209.49.110.112
Port # on Remote Machine:  0
```

Session

```
Start time of call:         56:17:51.77 hours
Time Call Is/Was Active:    9:42:50.38 hours
Minutes Until Timeout:      60
Time Left In Session:       0:17:9.61 hours
Termination Reason:         stillActive(0)
State at termination:       0
```

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

- **Call ID: (diactIndex)**—Unique identification of this active call for internal use.
- **Current Progress (diactState)**—Indicates current progress of the caller and the 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 type of modem modulation: V.34, V.32, ISDN, or 56K.

  **Authenticating**—The Server is in the process of verifying the users' passwords by using the static or Radius authentication.

  **Online**—The Server has completed the authentication and you are now ready to browse the Web.

  **Dead**—The user has been disconnected. This message will go away after the linger time is up.

  **Kill**—The administrator can manually disconnect the user by setting this parameter.
- **Username (diactUsername)**—The username that the caller entered.
- **Password (diactPassword)**—The password that the caller entered.
- **Shared Unique ID (diactMultiIndex)**—Unique identification shared between multilink active calls. This is used for multilink 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 10BASE-T port. This value will always be 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.

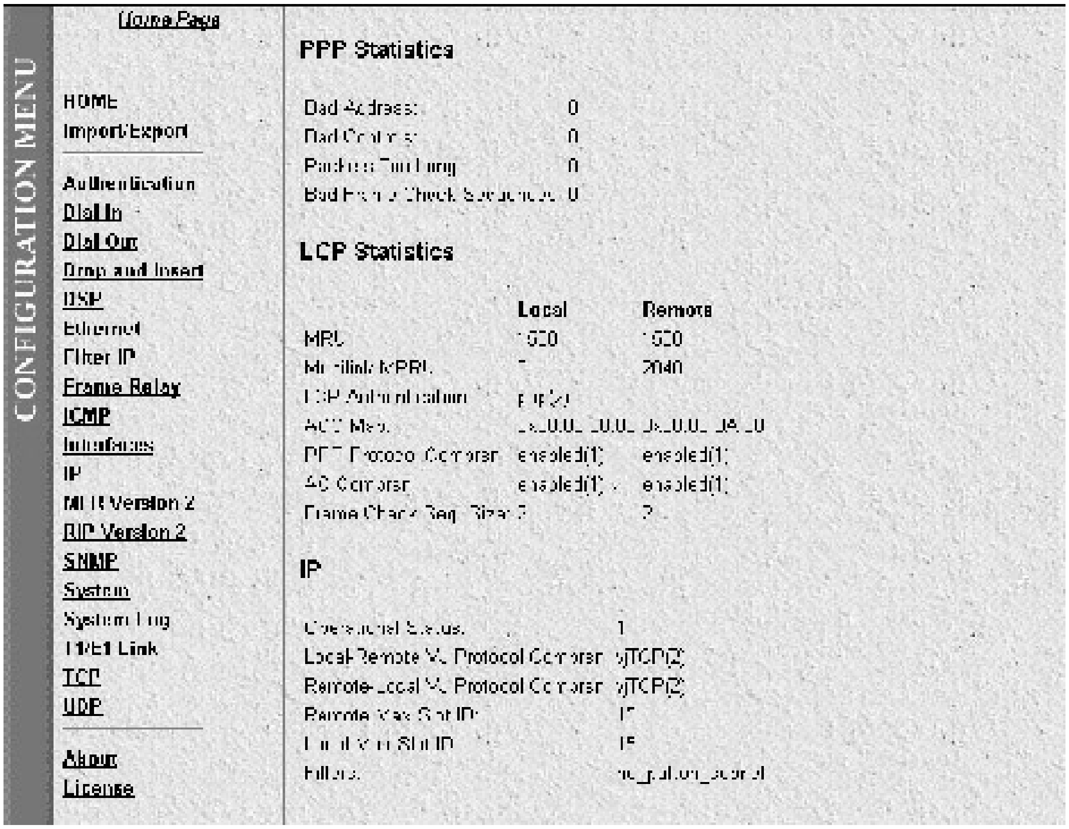
- **Time Slot Link (diactSlotIndex)**—This describes which channel this call is on on the T1/E1. T1 has1-24 channels; E1 has 30 channels. This is a number from 1 to 30.
- **IP Address (diactIP)**—The current assigned IP address from the IP address pool. The remote user’s PC is assigned to this address. 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. It ranges 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** shows PPP Statistics and IP statistics for a specific dial-in user. To reach this screen, scroll down from the previous screen.



**PPP Statistics**

| | |
|---|---|
| Bad Address: | 0 |
| Bad Controls: | 0 |
| Packets Too Long | 0 |
| Bad Frame Check Sequences | 0 |

**LCP Statistics**

| | Local | Remote |
|---|---|---|
| MRU | 1500 | 1500 |
| Multilink MRRU | - | 2040 |
| LCP Authentication | pap(2) | |
| ACC Map | [illegible] | [illegible] |
| PFC Protocol Compression | enabled(1) | enabled(1) |
| AC Compression | enabled(1) | enabled(1) |
| Frame Check Seq. Size | 2 | 2 |

**IP**

| | |
|---|---|
| Operational Status | 1 |
| Local-Remote VJ Protocol Compression | vjTCP(2) |
| Remote-Local VJ Protocol Compression | vjTCP(2) |
| Remote Max Slot ID | 15 |
| Local Max Slot ID | 15 |
| Filters | [illegible] |

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

*PPP Statistics*

This is the section on IP statistics of the current user selected. It is a 32-bit 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 that are longer than the MRU but 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).
- **Local-Peer ACC Map (diStatLocalToPeerACCMap)**—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 to 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 to 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 to 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 settings are:

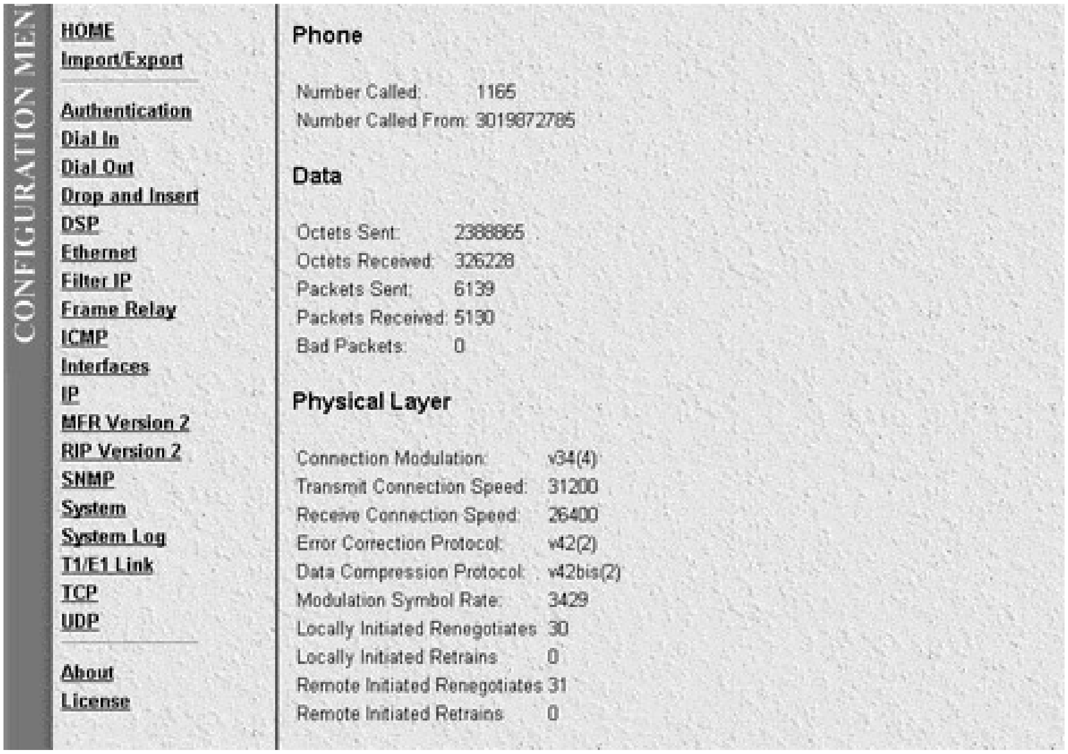
  **none**—no compression
  **vjTCP**—enabled

- **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 will be 0. The range is from 0 to 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 will be 0. The range is from 0 to 255.

*User Statistics (Phone, Data, Physical Layer)*

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



Phone

```
Number Called:        1165
Number Called From: 3019872785
```

Data

```
Octets Sent:          2388865
Octets Received:      326228
Packets Sent:         6139
Packets Received: 5130
Bad Packets:          0
```

Physical Layer

```
Connection Modulation:          v34(4)
Transmit Connection Speed:      31200
Receive Connection Speed:       26400
Error Correction Protocol:      v42(2)
Data Compression Protocol:      v42bis(2)
Modulation Symbol Rate:         3429
Locally Initiated Renegotiates  30
Locally Initiated Retrains      0
Remote Initiated Renegotiates 31
Remote Initiated Retrains       0
```

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

*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 into the Remote Access Server. 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 as a caller ID. This is the calling number.

*Data*

This section describes the amount of PPP data sent and received by this user, including 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 troubleshooting 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—for example, 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.
  **V.90**—Modem modulation with data rates up to 56.

- **Connection Speed (diactSpeed)**—The connected speed of the modem link—for example, 28.8 bps. These are the values in bits per second: 56000, 33600, 31200, 28800, 26400, 28800, 26400, 24000, 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.

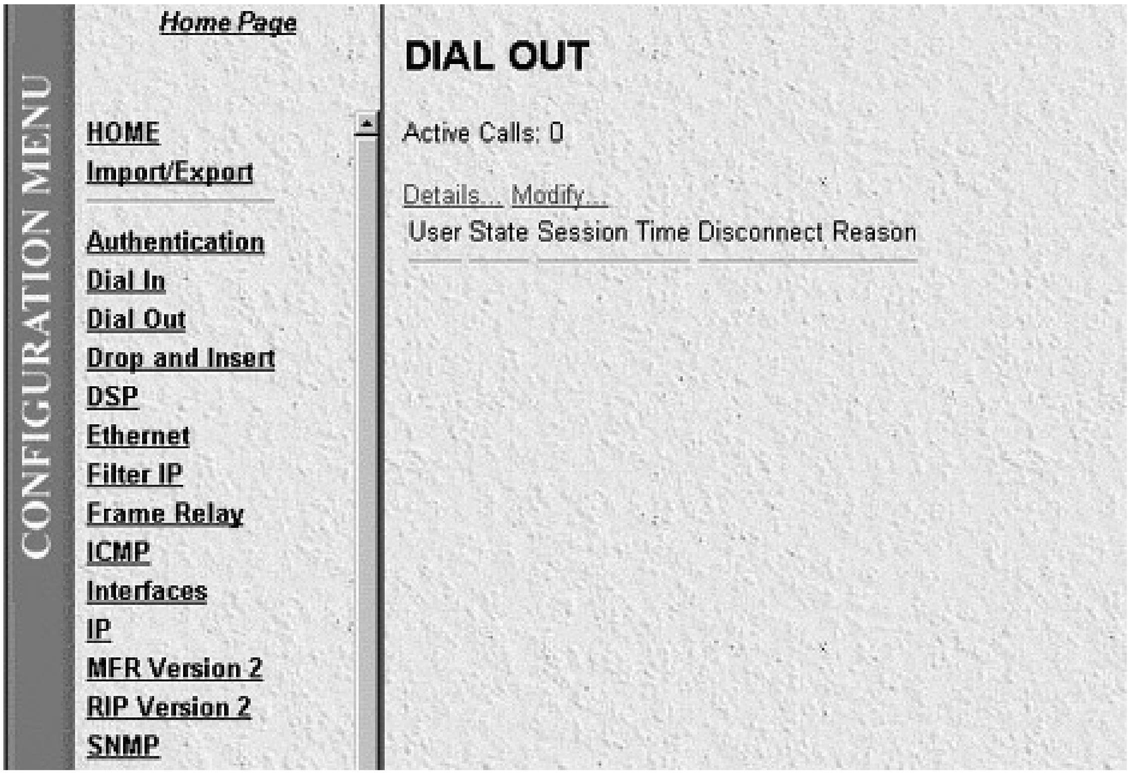
- **Symbol Rate (diactSymbolRate)**—The symbol rate of the call. This is used only when in V.34 modulation type.
- **Locally Initiated Renegotiates (diactLocalRenegotiates)**—The number of times the local side (this unit) has initiated a modem speed renogotiate.
- **Locally Initiated Retrains (diactLocalRetrains)**—The 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.

## A.5 Dial Out

The Dial Out Section contains items that are associated with making dial out connections from the Server 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 Server Configuration Menu (see **Figure A-16**). Following **Figure A-16** are descriptions for each object.



DIAL OUT

Active Calls: 0

| User | State | Session Time | Disconnect Reason |
|---|---|---|---|

**Figure A-16. Dial Out Main Screen.**

### A.5.1 Details (Contains Modifiable Dial Out Objects)

- **User (doactUsername)**—The username that the caller entered.
- **State (doactState)**—Indicates current progress.

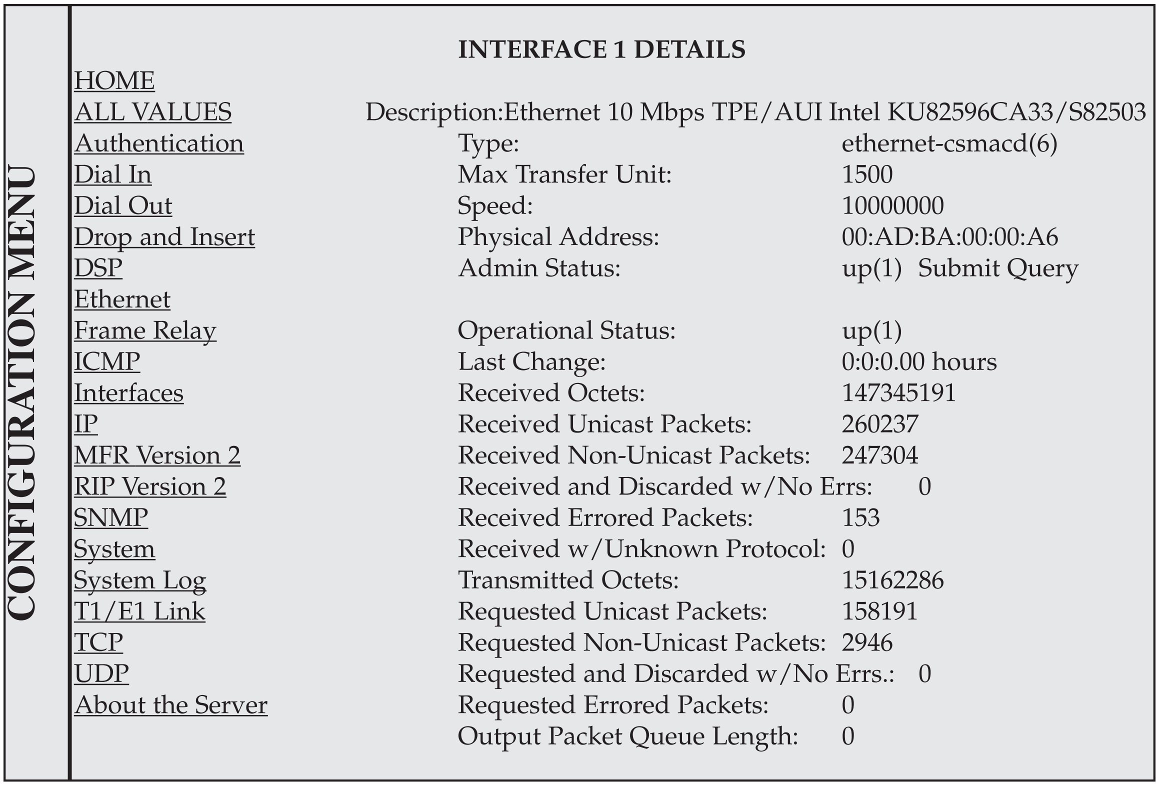
  **authenticating(0),**
  **commandmode(1),**
  **connecting(2),**

**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.

### A.5.2 Dial Out Details

Dial Out Details shows the active Dial Out configuration of the Server. 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**. The objects on this screen will be discussed in the next section.



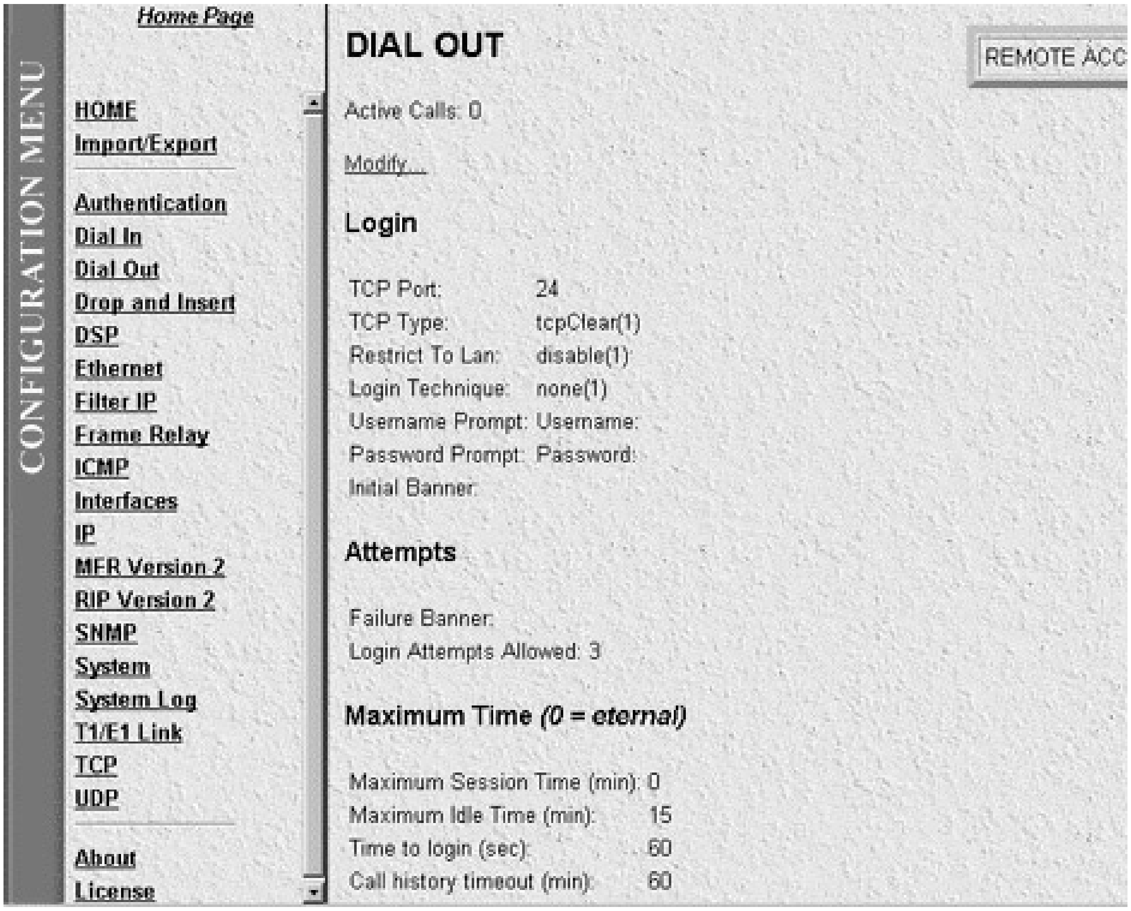
INTERFACE 1 DETAILS

```
Description:Ethernet 10 Mbps TPE/AUI Intel KU82596CA33/S82503
Type:                                ethernet-csmacd(6)
Max Transfer Unit:                   1500
Speed:                               10000000
Physical Address:                    00:AD: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
```

**Figure A-17. Dial Out—Details.**

### A.5.3 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 Server (see **Figure A-18**). To reach this screen, select Modify from the Dial Out Details screen.



DIAL OUT

Active Calls: 0

Modify...

Login

```
TCP Port:          24
TCP Type:          tcpClear(1)
Restrict To Lan:   disable(1)
Login Technique:   none(1)
Username Prompt:   Username:
Password Prompt:   Password:
Initial Banner:
```

Attempts

```
Failure Banner:
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
```

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

- **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 that the dialout should listen on for connections.
- **Restrict to Lan (doRestrictToLan)**—Enabling the restriction to LAN will stop dialout attempts that 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)**—Simple 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 without a 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 user's name. This should be an 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 user's 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.

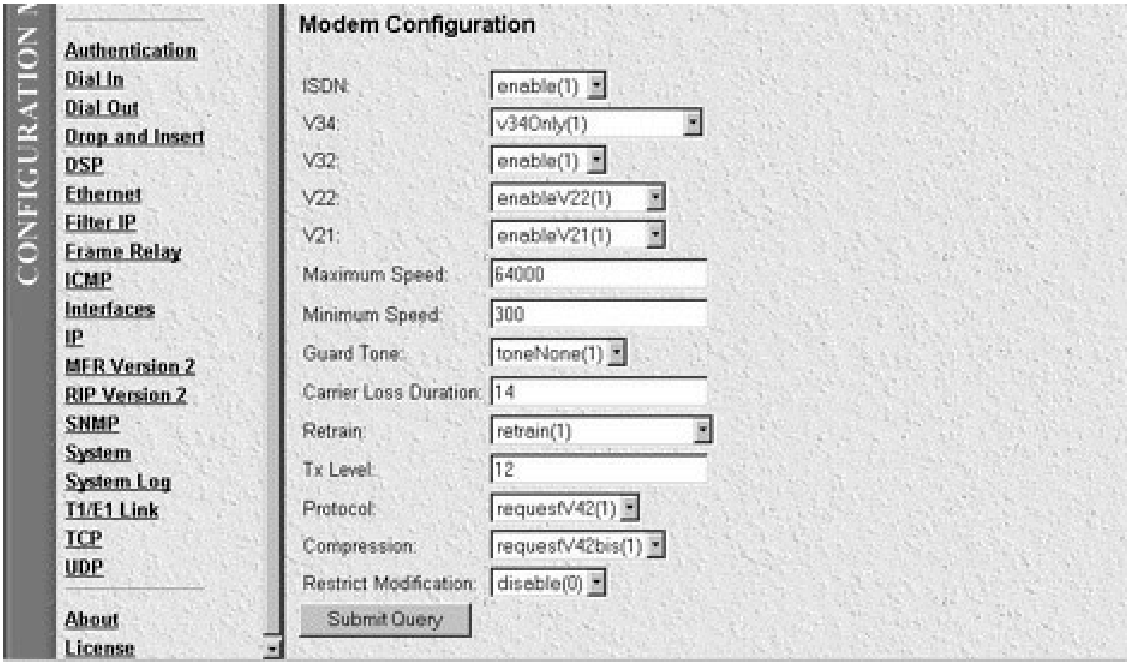
- **Failure Banner (doFailureBanner)**—This defines a message that will be displayed to a user when authentication failed. This is only relevant when the authentication technique was Text.
- **Login Attempts Allowed (doAllowAttempts)**—The maximum number of attempts a user will be given to log in before 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 that 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 that may be overridden by the authentication of a specific user.
- **Maximum Idle Time (doIdleTimeout)**—This is the maximum time in minutes that 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 that 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 log in. This is only relevant before the user is authenticated. This setting should take into account any time required to query a remote authentication server (i.e. RADIUS).
- **Call history timeout (min) (doLingerTime)**—Number of seconds an MIB entry in the Active table will remain after the call is dead.

### A.5.4 Dial Out Details (Modify Modem Configuration)

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



Modem Configuration

ISDN: enable(1)
V34: v34Only(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)

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

*Modem Configuration*

Use this section to configure the outgoing modem configuration.

- **ISDN (doModemISDNEnable)**—Allow V.34 and V.34 annex 12 transmissions.

  **disable(0),**
  **enable(1)**

- **V34 (doModemV34Enable)**—Allow V.34 and V.34 annex 12 transmissions.

  **disable(0),**
  **enable(1)**

- **V32 (doModemV32Enable)**—Allow V.32 and V.32bis transmissions.

**disable(0),**
**enable(1)**

- **V22 (doModemV22Enable)**—Allow V.22 or Bell 212 transmissions.

**disable(0),**
**enableV22(1),**

**enableBell212(2)**

- **V21 (doModemV21Enable)**—Allow V.21 or Bell 103 transmissions.

  **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 you can insert one. 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 the link is considered disconnected. 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 fall-forward for good quality.

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

- **Tx Level (doModemTxLevel)**—Set this variable with caution, normally only after talking to Technical Support. This sets the transmit 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 V.42 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 V.42bis compression protocol. This will only be used if V.42 error correction is active.

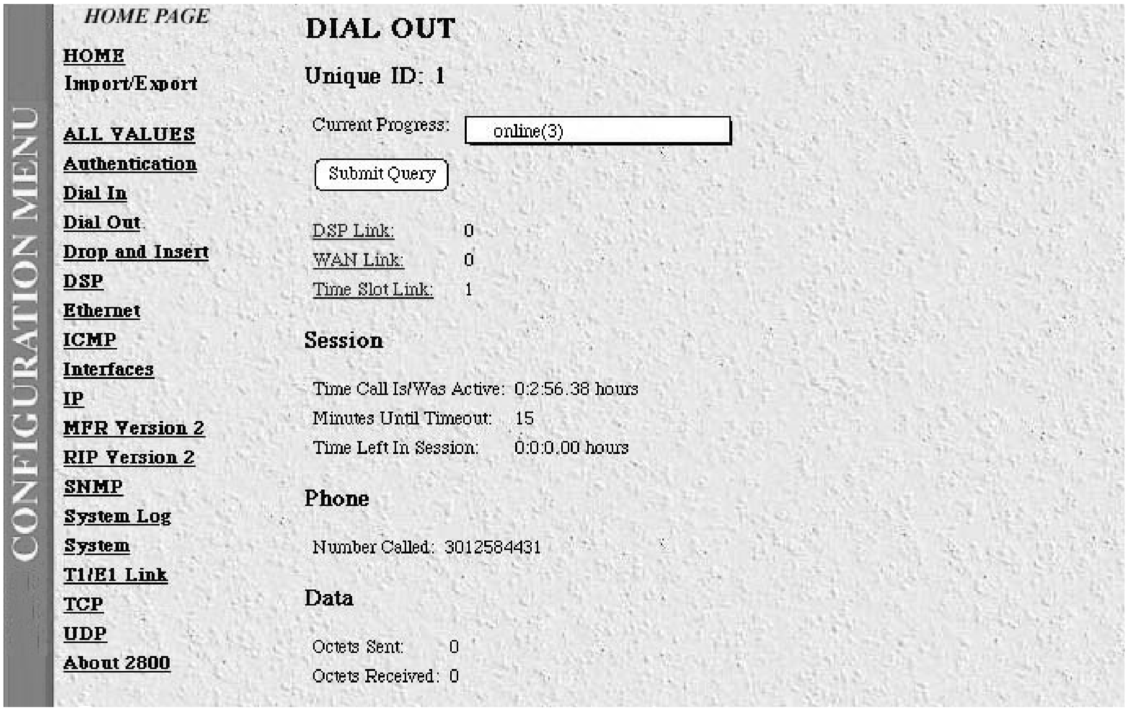
  **direct(0),**
  **requestV42bis(1),**
  **requireV42bis(2)**

- **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)**

### A.5.5 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** 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 Server Configuration Menu.



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

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

- **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 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.

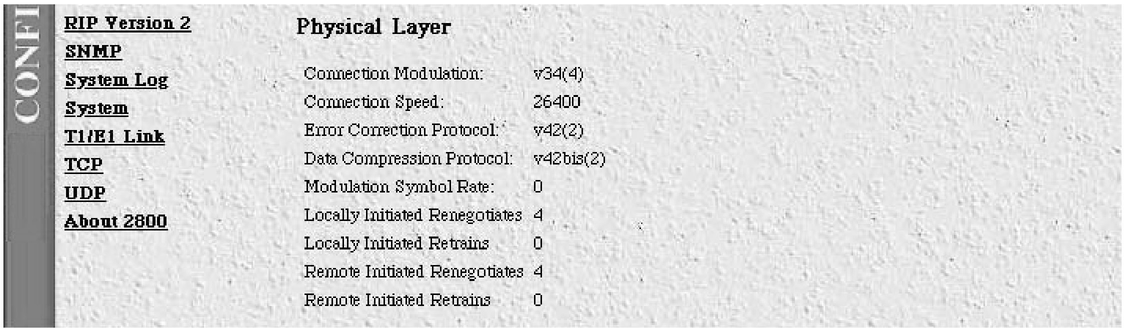
*Data*

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.

### A.5.6 User Statistics (Physical Layer)

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



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
```

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

*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.

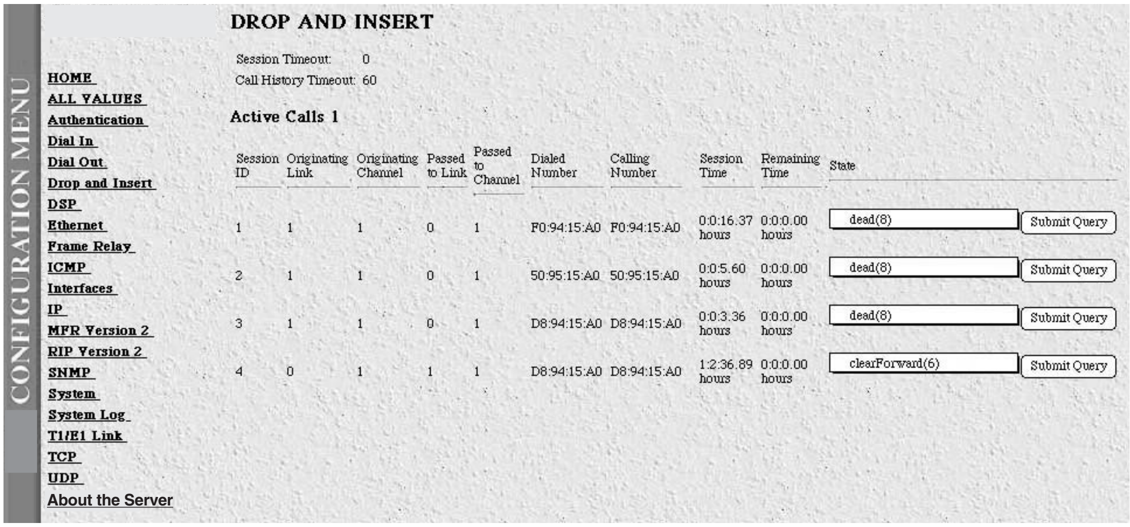
  **unknown(0),**
  **none(1),**
  **v42bis(2),**
  **mnp5(3),**
  **stac(4)**

- **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 (doacRemoteRetrains)**—The number of times the far modem has initiated a modem carrier retrain.

## A.6 Drop and Insert

The Drop and Insert section contains setup objects associated with using the Server 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 Server, this screen will be blank.

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



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) | Submit Query |
| 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) | Submit Query |
| 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) | Submit Query |
| 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) | Submit Query |

**Figure A-22. Drop and Insert Main Screen.**

- **Session Timeout (drSessionTimeout)**—This is the maximum time in minutes that 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).

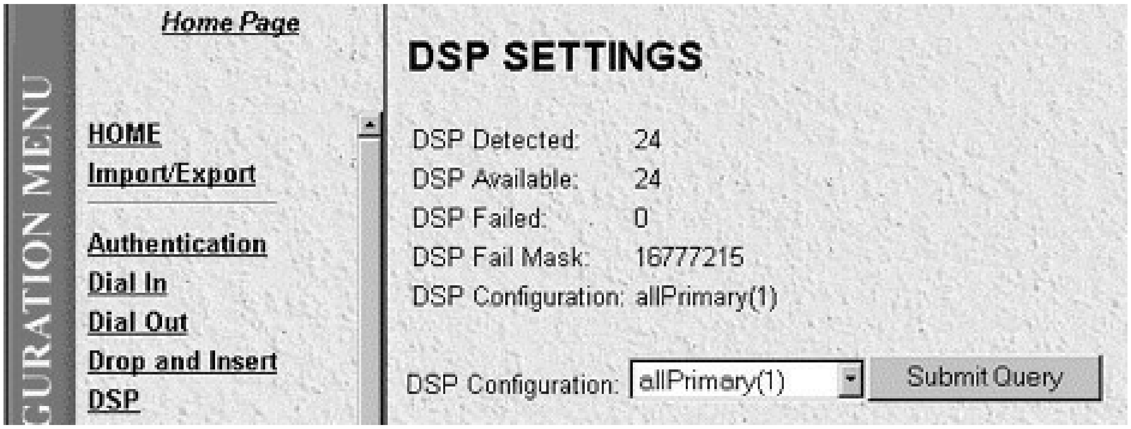
- **State (dractState)**—Indicates current progress.

  **setup(1),**
  **alerting(2),**
  **flash(3),**
  **online(4),**

  **sessiontime(5),**
  **clearForward(6),**
  **clearBackward(7),**
  **dead(8),**
  **kill(9)**

## A.7 DSP (Digital Signal Processing)

The Server 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 that distinguish DSP architectures from other microprocessor and microcontroller architectures. Select DSP from the Configuration Menu to monitor the five variables that describe the current state of the DSPs (see **Figure A-23**). Following **Figure A-23** are descriptions for each variable.



DSP SETTINGS

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

DSP Configuration: allPrimary(1)

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

- **DSP Detected (dspDetected)**—Indicates the number of DSPs the PAR-1 has detected as installed at time of bootup.

- **DSP Available (dspAvailable)**—Indicates the number of DSPs available for operation.

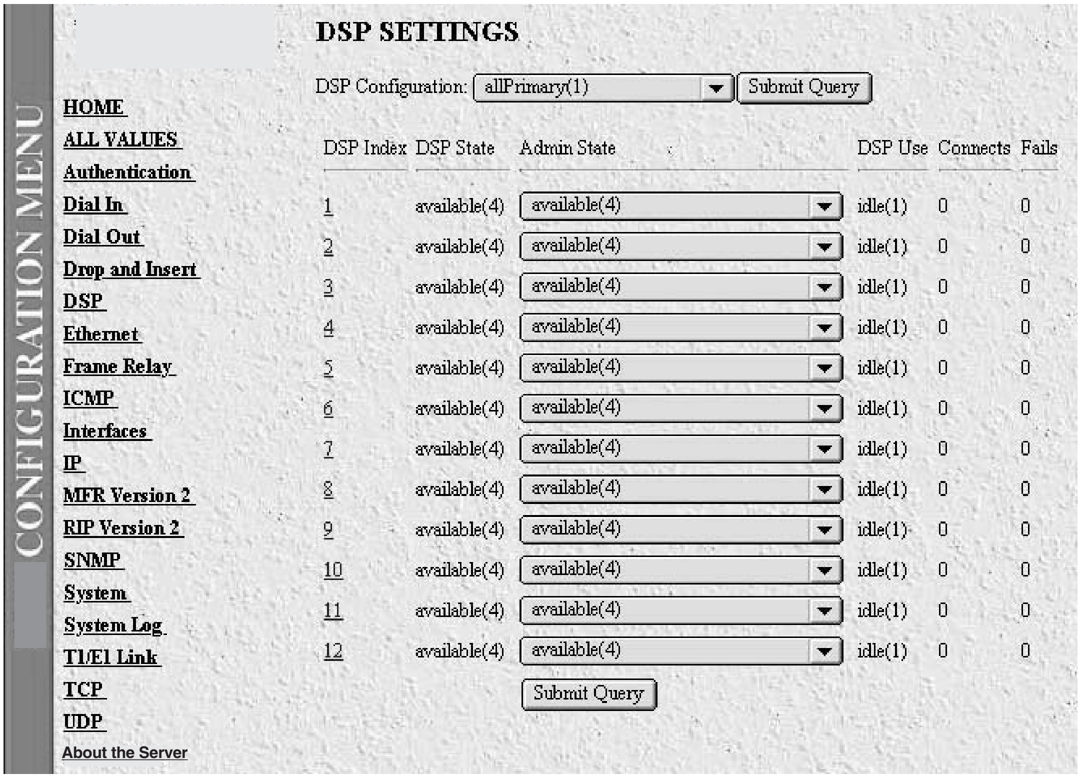
- **DSP Failed (dspFailed)**—Indicates the number of DSPs taken out of the DSP resource pool.

- **DSP Fail Mask (dspFailMask)**—A bit mask that identifies which DSPs 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 DSPs (see **Figure A-24**). The SNMP variables for this table are referenced through the **DSP Index (dspIndex)** variable.



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 |

**Figure A-24. DSP Settings.**

- **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 DSPs are attached to Line A.
**split(2) =** Half of the DSPs are attached to Line A and half of the DSPs 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 you 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.

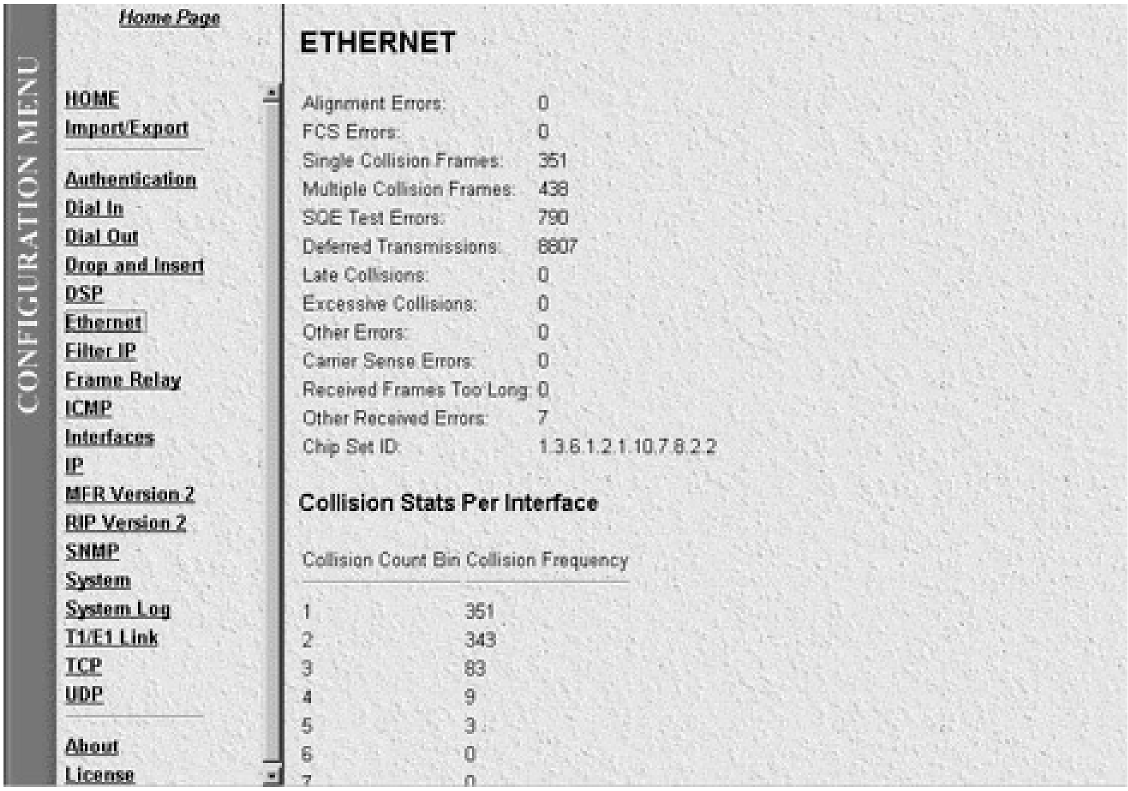
- **DSP Use (dspUse)**—This variable identifies the current stae that the DSP is in.  Select from:

  **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 processing on the WAN link.
  **signalling(6)** = The DSP is being used to process WAN-link signaling.

- **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 identifes that connection.

## A.8 Ethernet

The Server provides management and statistical information on the Ethernet interface.  You can find detailed information regarding the SNMP MIB II variables in RFC 1643,  Definitions of Managed Objects for the Ethernet-like Interface Types (see **page 3**).  Select Ethernet from the Configuration Menu to monitor Ethernet statistics.  Following **Figure A-25** are descriptions for each variable.



ETHERNET

| | |
|---|---|
| Alignment Errors: | 0 |
| FCS Errors: | 0 |
| Single Collision Frames: | 351 |
| Multiple Collision Frames: | 438 |
| SQE Test Errors: | 790 |
| Deferred Transmissions: | 6807 |
| Late Collisions: | 0 |
| Excessive Collisions: | 0 |
| Other Errors: | 0 |
| Carrier Sense Errors: | 0 |
| Received Frames Too Long: | 0 |
| Other Received Errors: | 7 |
| Chip Set ID: | 1.3.6.1.2.1.10.7.8.2.2 |

Collision Stats Per Interface

| Collision Count Bin | Collision Frequency |
|---|---|
| 1 | 351 |
| 2 | 343 |
| 3 | 83 |
| 4 | 9 |
| 5 | 3 |
| 6 | 0 |
| 7 | 0 |

**Figure A-25. Ethernet Main Screen.**

- **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.

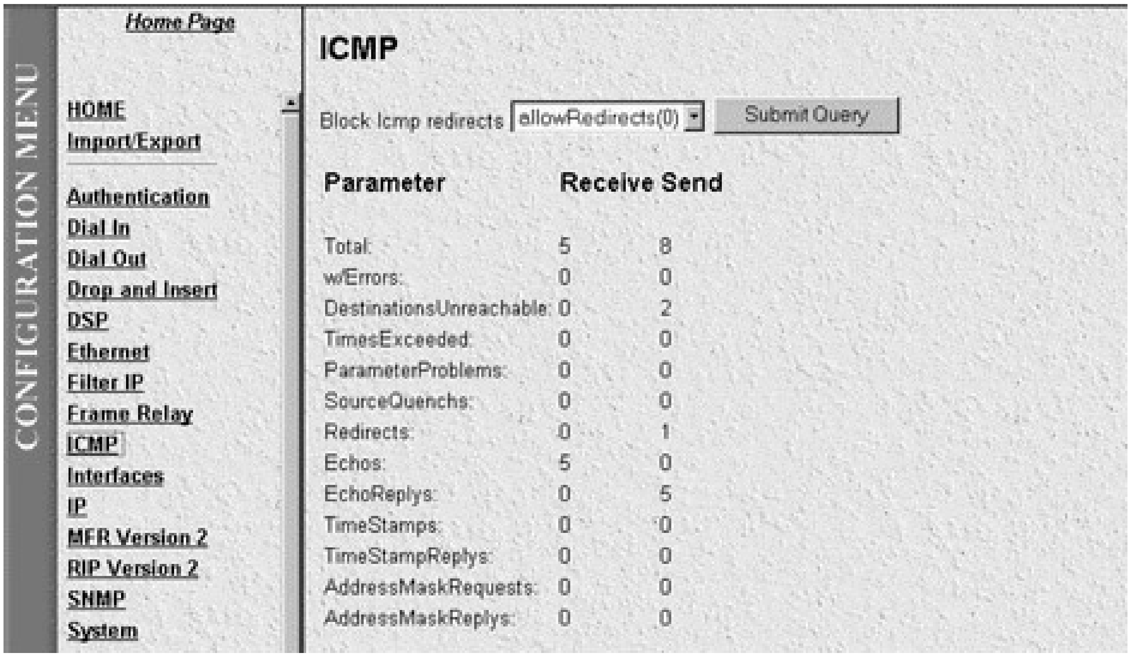
- **Other Errors (dot3StatsInternalMacTransmitErrors)**—The number of frames transmission failed due to an internal MAC sublayer transmit error.
- **Carrier Sense Errors (dot3StatsCarrierSenseErrors)**—The number of times that the carrier sense condition was lost or never asserted when attempting to 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 chipset 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 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.

## NOTE

**For Frame Relay applications, call Black Box Technical Support at 724-746-5500.**

## A.9 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 Server's 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 Server's ICMP parameters, select ICMP from the Server's Configuration Menu (see **Figure A-30**).



ICMP

Block Icmp redirects allowRedirects(0)

| Parameter | Receive | Send |
|---|---|---|
| Total: | 5 | 8 |
| w/Errors: | 0 | 0 |
| DestinationsUnreachable: | 0 | 2 |
| TimesExceeded: | 0 | 0 |
| ParameterProblems: | 0 | 0 |
| SourceQuenchs: | 0 | 0 |
| Redirects: | 0 | 1 |
| Echos: | 5 | 0 |
| EchoReplys: | 0 | 5 |
| TimeStamps: | 0 | 0 |
| TimeStampReplys: | 0 | 0 |
| AddressMaskRequests: | 0 | 0 |
| AddressMaskReplys: | 0 | 0 |

**Figure A-30. ICMP Main Screen.**

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

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

Example: **Parameter (InMibVariable, OutMibVariable)**

The numbers following the parameters can point out potential problems on the network. Both gateways (routers) and hosts may send ICMP messages.

### ICMP Receive/Send Messages

- **Received (icmpInMsgs)**—The number of ICMP messages the Server has received. This number also includes ICMP messages received/sent that have ICMP specific errors.

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

- **w/Errors (icmpInErrors, icmpOutErrors)**—The number of ICMP messages that the Server has received/sent but that 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 (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 that is reassembling a fragmented 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 prohibits further processing, the gatway or host will discard the packet and return an ICMP Parameter Problem message. One potential source of this problem may be incorrect or invalid arguments in an option. ICMP sends the Parameter 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 message 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 Server 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/sent. The ICMP Echo is used whenever you use 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 Server 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 Server 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 Time Protocol (NTP)—has been designed and implemented to perform this function. In normal conditions, this number will be zero.

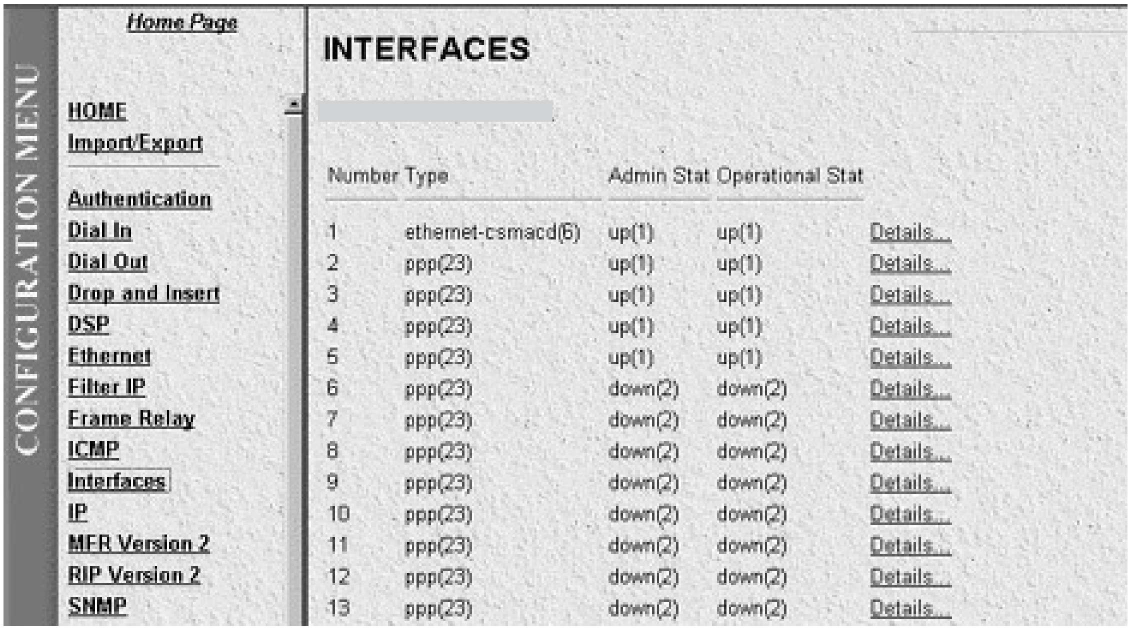
- **Time Stamp Replys (icmpInTimestampsReps) (icmpOutTimestampsReps)**—The number of ICMP Timestamp Reply messages received/sent. This message is part of a Time Stamp (see above) request. In normal conditions, this number will be zero.

- **Address Mask Requests (icmpInAddrMasks) (icmpOutAddrMasks)**—The number of ICMP Address Mask Request messages received/sent. This message is generally used for diskless workstations that 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.

## A.10 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 Server Interfaces page correspond directly to statistics listed in *RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II.* Some frames are 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 Server's Configuration Menu (see **Figure A-31**). Following **Figure A-31** are descriptions for each variable on this page.



INTERFACES

| Number | Type | Admin Stat | Operational Stat | |
|---|---|---|---|---|
| 1 | ethernet-csmacd(6) | up(1) | up(1) | Details... |
| 2 | ppp(23) | up(1) | up(1) | Details... |
| 3 | ppp(23) | up(1) | up(1) | Details... |
| 4 | ppp(23) | up(1) | up(1) | Details... |
| 5 | ppp(23) | up(1) | up(1) | Details... |
| 6 | ppp(23) | down(2) | down(2) | Details... |
| 7 | ppp(23) | down(2) | down(2) | Details... |
| 8 | ppp(23) | down(2) | down(2) | Details... |
| 9 | ppp(23) | down(2) | down(2) | Details... |
| 10 | ppp(23) | down(2) | down(2) | Details... |
| 11 | ppp(23) | down(2) | down(2) | Details... |
| 12 | ppp(23) | down(2) | down(2) | Details... |
| 13 | ppp(23) | down(2) | down(2) | Details... |

**Figure A-31. Interfaces Main Screen.**

- There are **(ifNumber)** total interfaces. This is 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) immediately "below" the network layer in the protocol stack. Valid interface options are:

  **other(1)**<br>
  **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 operational frames may be passed in this mode.

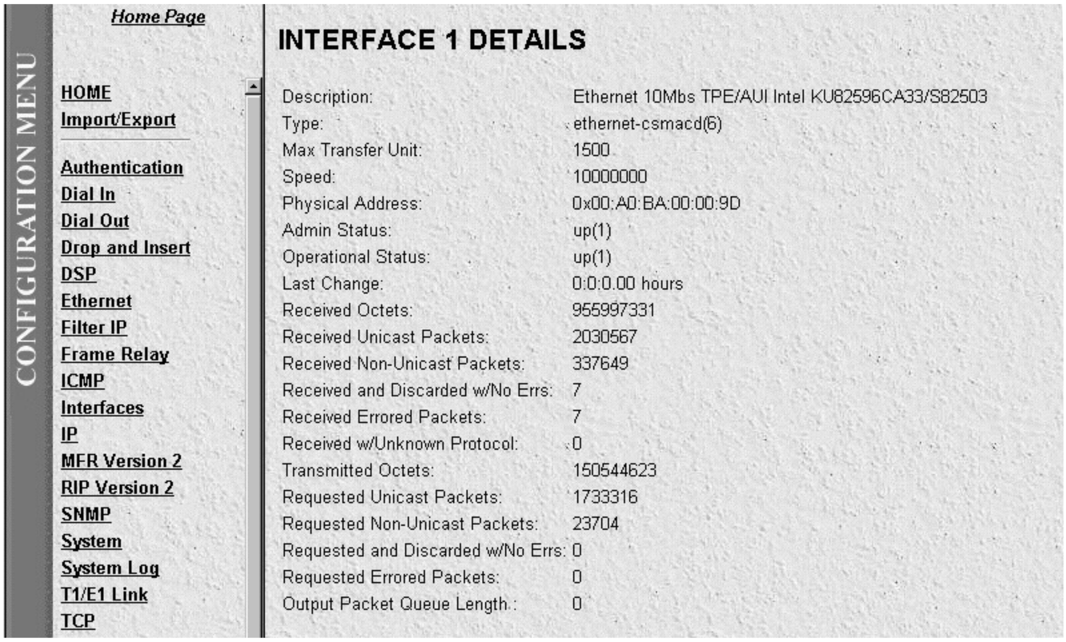
- **Operational Status**—The current operational state of the interface.

  **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**. This page shows the status of all DSPs. 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.



INTERFACE 1 DETAILS

| | |
|---|---|
| Description: | Ethernet 10Mbs TPE/AUI Intel KU82596CA33/S82503 |
| Type: | ethernet-csmacd(6) |
| Max Transfer Unit: | 1500 |
| Speed: | 10000000 |
| Physical Address: | 0x00:A0:BA:00:00:9D |
| Admin Status: | up(1) |
| Operational Status: | up(1) |
| Last Change: | 0:0:0.00 hours |
| Received Octets: | 955997331 |
| Received Unicast Packets: | 2030567 |
| Received Non-Unicast Packets: | 337649 |
| Received and Discarded w/No Errs: | 7 |
| Received Errored Packets: | 7 |
| Received w/Unknown Protocol: | 0 |
| Transmitted Octets: | 150544623 |
| Requested Unicast Packets: | 1733316 |
| Requested Non-Unicast Packets: | 23704 |
| Requested and Discarded w/No Errs: | 0 |
| Requested Errored Packets: | 0 |
| Output Packet Queue Length : | 0 |

**Figure A-32. Interface Details.**

- **Description (ifDescr)**—A text string containing 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 that 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 that 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 Server:

1. Select the desired Admin Stat mode.
2. Select Submit 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 (subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.

- **Received and Discarded w/No Errs (ifInDiscards)**—The number of inbound packets that 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 that were discarded because of an unknown or unsupported protocol.

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

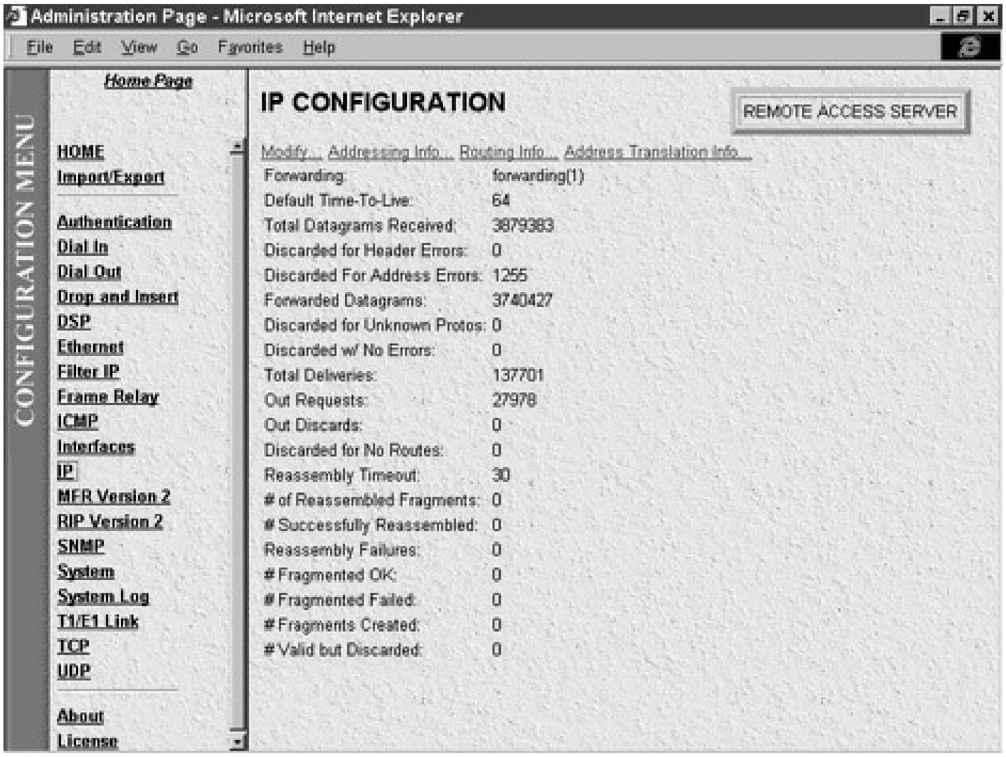
- **Requested Unicast Packets (ifOutUcastPkts)**—The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

- **Requested Non-Unicast Packets (ifOutNUcastPkts)**—The total number of packets that higher level protocols requested be transmitted to a non-unicast (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 that 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).

## A.11 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 Server's Configuration Menu (see **Figure A-33**). Following **Figure A-33** are descriptions for each variable on this screen.



IP CONFIGURATION

Forwarding: forwarding(1)
Default Time-To-Live: 64
Total Datagrams Received: 3879383
Discarded for Header Errors: 0
Discarded For Address Errors: 1255
Forwarded Datagrams: 3740427
Discarded for Unknown Protos: 0
Discarded w/ No Errors: 0
Total Deliveries: 137701
Out Requests: 27978
Out Discards: 0
Discarded for No Routes: 0
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

**Figure A-33. IP Configuration Main Screen.**

- **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

**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 (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E).
- **Forwarded Datagrams (ipForwDatagrams)**—The number of input datagrams for which the Remote Access Server 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.
- **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 (for example, 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 that local IP user-protocols (including ICMP) supplied to IP in requests for transmission.

## NOTE

**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 (for example, for lack of buffer space).

## NOTE

**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.

## NOTES

**This counter includes any packets counted in ipForwDatagrams that meet this "no-route" criterion.**

**This includes any datagrams that a host cannot route because all of its default gateways are down.**

- **Reassembly Timeout (ipReasmTimeout)**—The maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
- **# of Reassembled Fragments (ipReasmReqds)**—The number of IP fragments received that 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).

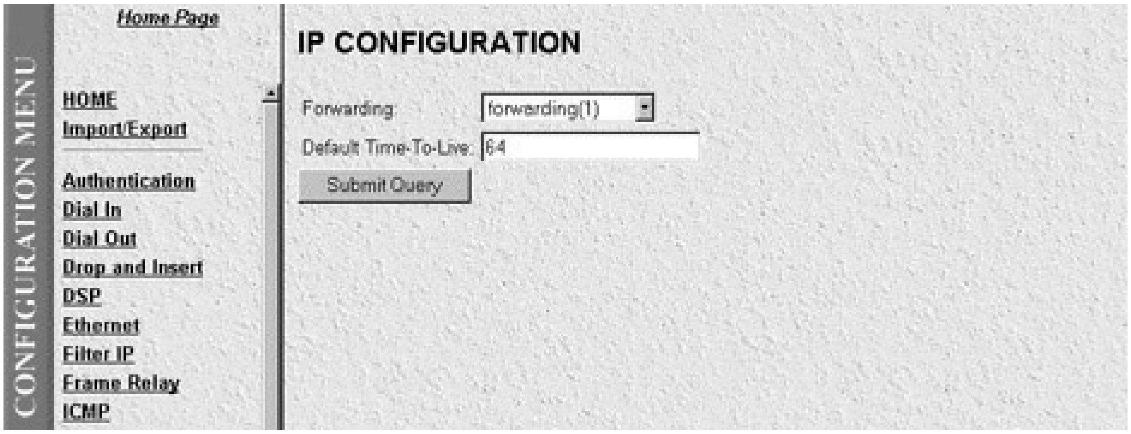
## NOTE

**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, for example, 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 that 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.

### A.11.1 IP Configuration (Modify Forwarding and Time-To-Live)

IP Forwarding and Time-To-Live (**Figure A-34**) 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.



IP CONFIGURATION

Forwarding: forwarding(1)

Default Time-To-Live: 64

**Figure A-34. IP Configuration—Modify Forwarding and Time-to-Live.**

- **Forwarding (ipForwarding)**—The indication of whether the Server is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, the Remote Access Server.

## NOTE

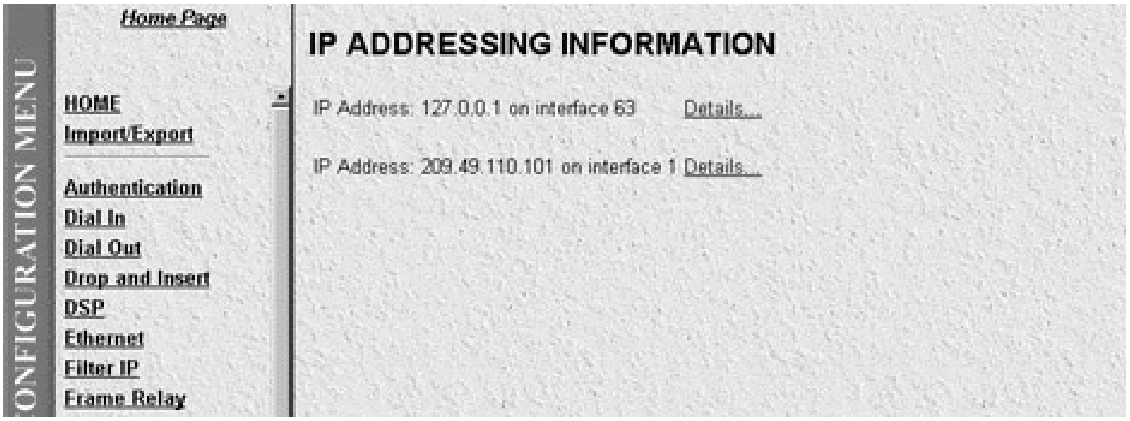
**For some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a "badValue" response if a management station attempts to change this object to an inappropriate value.**

| | |
|---|---|
| **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.

### A.11.2 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**). To reach this page, select Addressing Info… from the main IP Configuration screen.



IP ADDRESSING INFORMATION

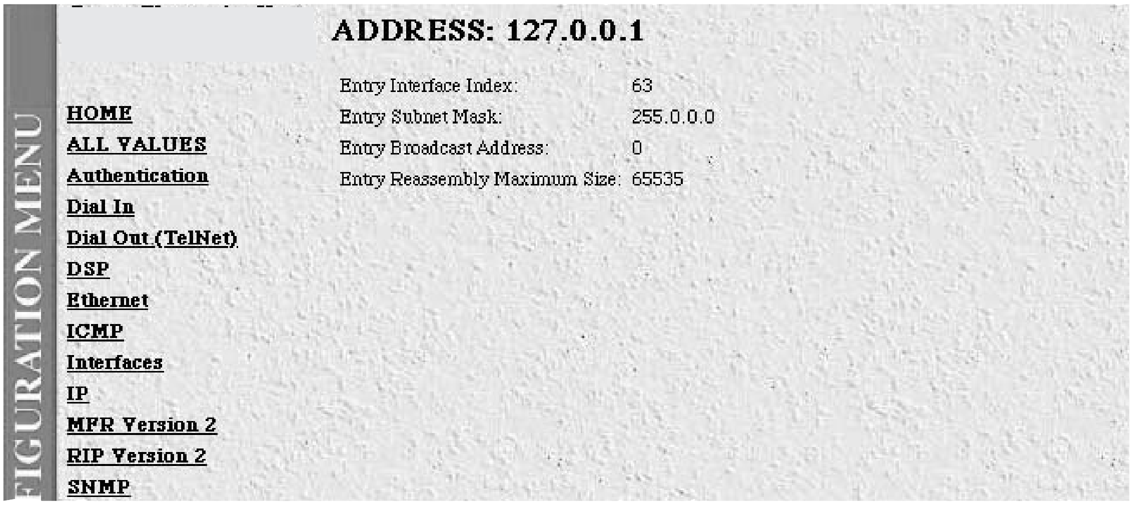
IP Address: 127.0.0.1 on interface 63 Details...

IP Address: 209.49.110.101 on interface 1 Details...

**Figure A-35. IP Configuration—Addressing Information.**

### A.11.3 IP Configuration (Addressing Information Details)

This screen shows IP Address Table entries for each defined network interface (See **Figure A-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.



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 |

**Figure A-36. IP Configuration—Addressing Informantion Details.**

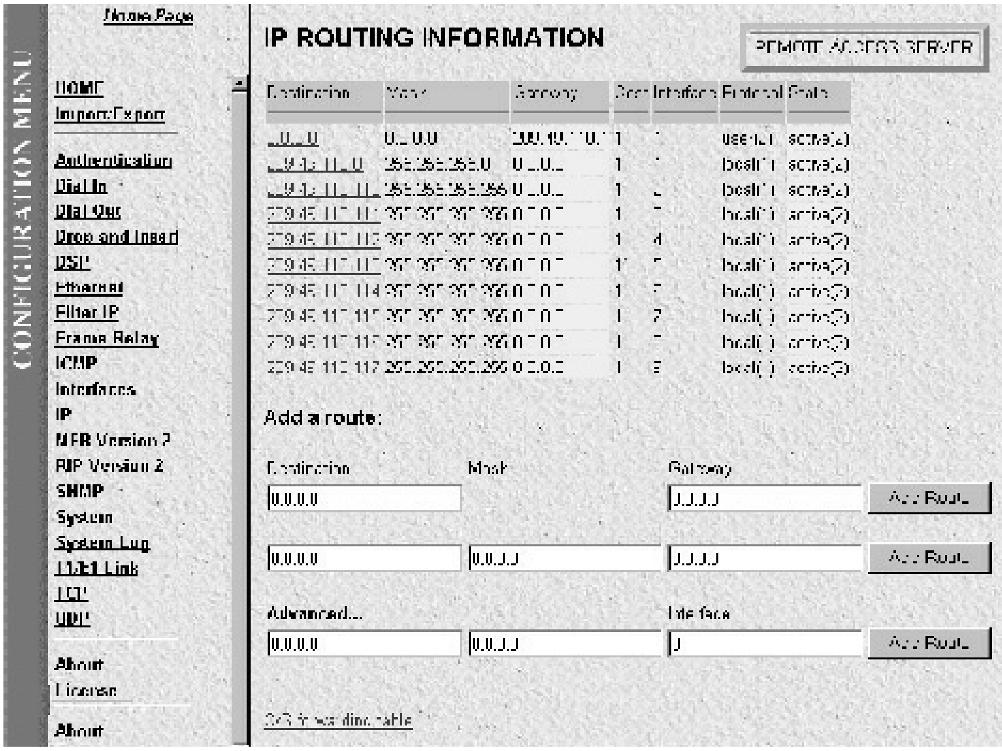
- **Entry Interface Index (ipAdEntIfIndex)**—The index value that uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
- **Entry Subnet Mask (ipAdEntNetMask)**—The 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 that this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

### A.11.4 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.



IP ROUTING INFORMATION

| Destination | Mask | Gateway | Cost | Interface | Protocol | State |
|---|---|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | [illegible] | 1 | [illegible] | [illegible] | active(2) |
| [illegible] | 255.255.255.0 | 0.0.0.0 | 1 | [illegible] | local(2) | active(2) |
| [illegible] | 255.255.255.255 | 0.0.0.0 | 1 | [illegible] | local(2) | active(2) |
| [illegible] | 255.255.255.255 | 0.0.0.0 | 1 | [illegible] | local(2) | active(2) |
| [illegible] | 255.255.255.255 | 0.0.0.0 | 1 | 4 | local(2) | active(2) |
| [illegible] | 255.255.255.255 | 0.0.0.0 | 1 | [illegible] | local(2) | active(2) |
| [illegible] 114 | 255.255.255.255 | 0.0.0.0 | 1 | [illegible] | local(2) | active(2) |
| [illegible] | 255.255.255.255 | 0.0.0.0 | 1 | 7 | local(2) | active(2) |
| [illegible] | 255.255.255.255 | 0.0.0.0 | 1 | [illegible] | local(2) | active(2) |
| [illegible] 117 | 255.255.255.255 | 0.0.0.0 | 1 | [illegible] | local(2) | active(2) |

Add a route:

Destination: 0.0.0.0 Mask: Gateway: 0.0.0.0

Destination: 0.0.0.0 Mask: 0.0.0.0 Gateway: 0.0.0.0

Advanced... 0.0.0.0 0.0.0.0 Interface: 0

IP forwarding table

**Figure A-37. IP Configuration—Routing Information.**

- **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 depends on the table-access mechanisms defined by the network management protocol in use.

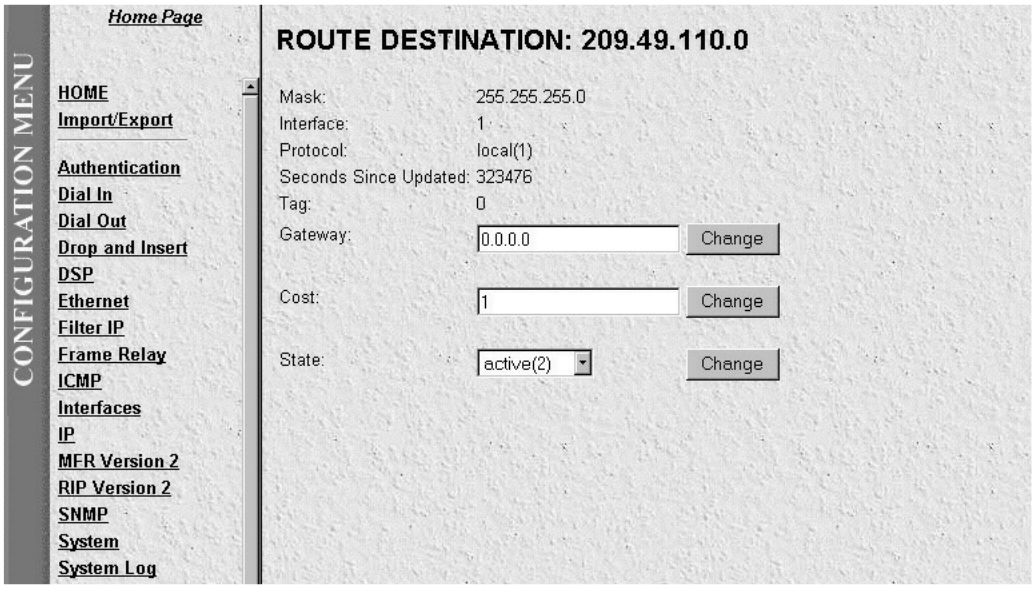
- **Mask (ipRouteMask)**—Indicates the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the corresponding 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 that 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 that 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.

### A.11.5 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 Destination column in the previous routing information screen.



ROUTE DESTINATION: 209.49.110.0

Mask: 255.255.255.0
Interface: 1
Protocol: local(1)
Seconds Since Updated: 323476
Tag: 0
Gateway: 0.0.0.0
Cost: 1
State: active(2)

Figure A-38. IP Configuration—Routing Information, Destination.

- **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 depends 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 corresponding 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 that 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—for example, manually configured entries

  **netmgmt(3)**—set via a network management protocol

  **icmp(4)**—obtained via ICMP,—for example, 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)**

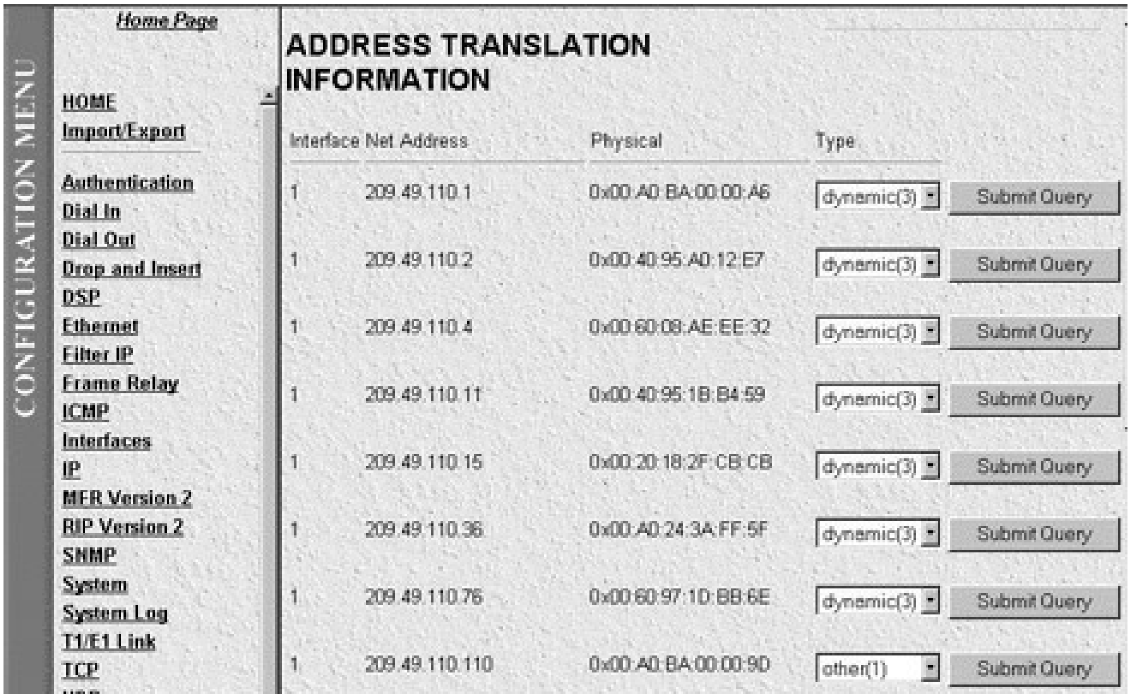
- **Seconds Since Updated (ipRouteAge)**—The number of seconds since this route was last updated or otherwise determined to be correct. Note that no semantics of “too old” can be implied except through knowledge of the routing protocol by which the route was learned.
- **Info (ipRouteInfo)**—A reference to MIB definitions specific to the particular routing protocol that 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 synactically 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 that 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) invalidates 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

### A.11.6 IP Configuration (Address Translation Information)

The IP address translation table contains the IpAddress-to-physical-address equivalences (see **Figure A-39**). Some interfaces do not use translation tables for determining address equivalences (for example, DDN-X.25 has an algorithmic method). If all interfaces are of this type, then the Address Translation table is empty (it has zero entries).



ADDRESS TRANSLATION INFORMATION

| Interface | Net Address | Physical | Type |
|---|---|---|---|
| 1 | 209.49.110.1 | 0x00:A0:BA:00:00:A6 | dynamic(3) |
| 1 | 209.49.110.2 | 0x00:40:95:A0:12:E7 | dynamic(3) |
| 1 | 209.49.110.4 | 0x00:60:08:AE:EE:32 | dynamic(3) |
| 1 | 209.49.110.11 | 0x00:40:95:1B:B4:59 | dynamic(3) |
| 1 | 209.49.110.15 | 0x00:20:18:2F:CB:CB | dynamic(3) |
| 1 | 209.49.110.36 | 0x00:A0:24:3A:FF:5F | dynamic(3) |
| 1 | 209.49.110.76 | 0x00:60:97:1D:BB:6E | dynamic(3) |
| 1 | 209.49.110.110 | 0x00:A0:BA:00:00:9D | other(1) |

**Figure A-39. IP Configuration—Address Translation Information.**

- **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) invalidates 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

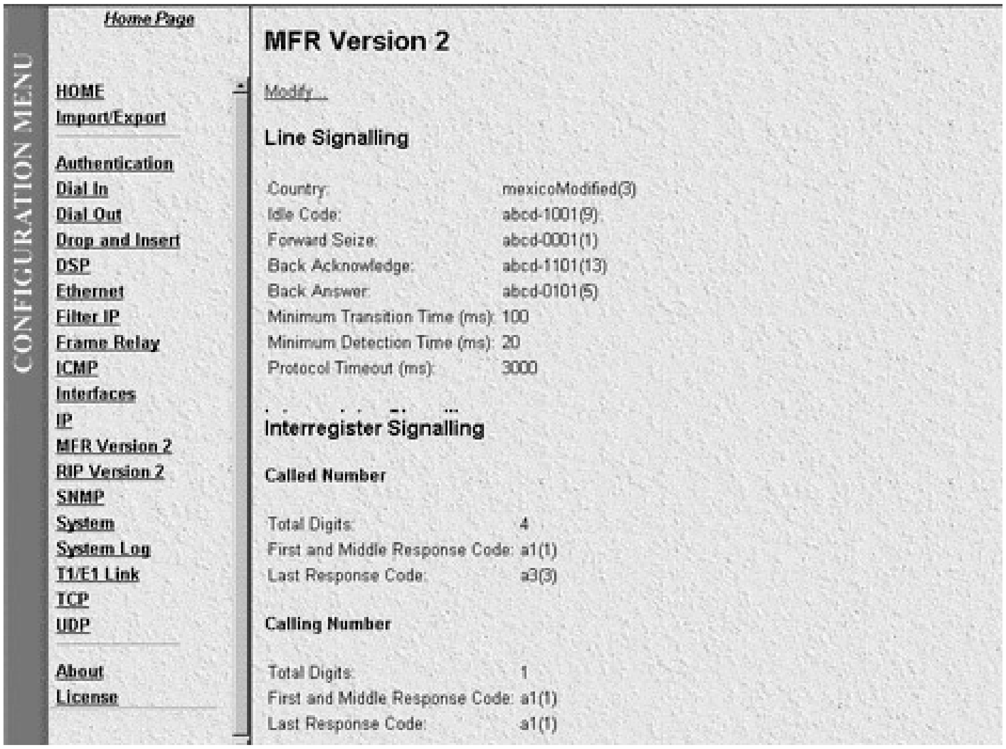
currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object.

| | |
|---|---|
| **other(1)** | none of the following |
| **invalid(2)** | an invalidated mapping |
| **dynamic(3)** | |
| **static(4)** | |

## A.12 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 Server, refer to Recommendations Q.40–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 Server's Configuration Menu (see **Figure A-40**). Following **Figure A-40** are descriptions for each object on this page.



MFR Version 2

Line Signalling

Country: mexicoModified(3)
Idle Code: abcd-1001(9)
Forward Seize: abcd-0001(1)
Back Acknowledge: abcd-1101(13)
Back Answer: abcd-0101(5)
Minimum Transition Time (ms): 100
Minimum Detection Time (ms): 20
Protocol Timeout (ms): 3000

Interregister Signalling

Called Number

Total Digits: 4
First and Middle Response Code: a1(1)
Last Response Code: a3(3)

Calling Number

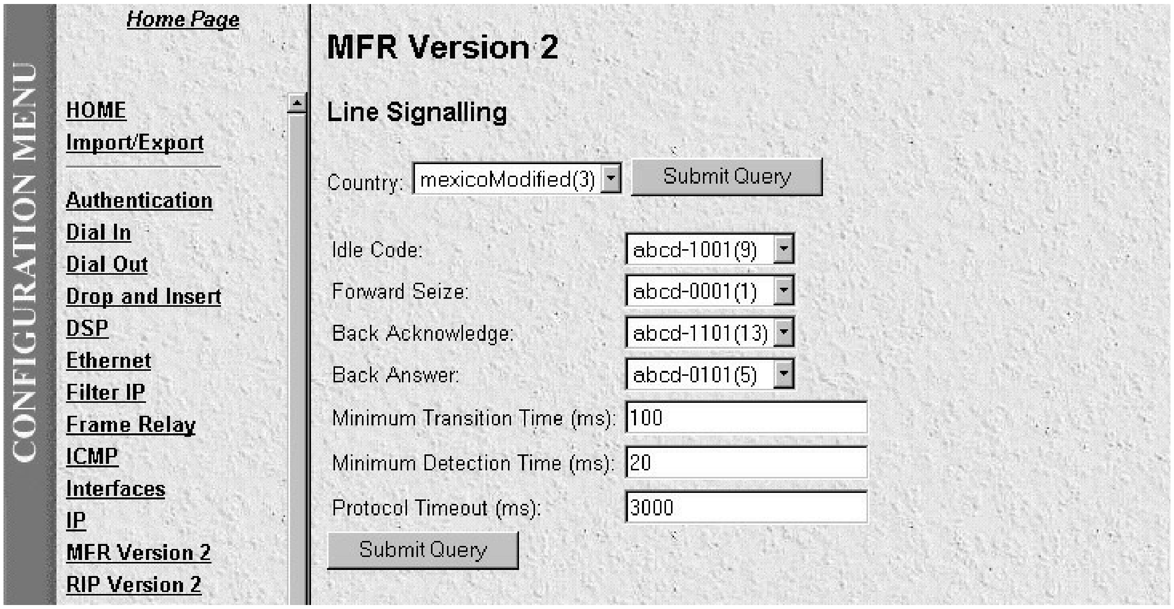
Total Digits: 1
First and Middle Response Code: a1(1)
Last Response Code: a1(1)

**Figure A-40. MFR Version 2.**

The objects on this screen will be discussed in the next section.

### A.11.1 MFR Version 2 (Modify Line Signalling)

From this screen you can modify Line Signalling parameters (see **Figure A-41**). 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.



MFR Version 2

Line Signalling

Country: mexicoModified(3)

Idle Code: abcd-1001(9)

Forward Seize: abcd-0001(1)

Back Acknowledge: abcd-1101(13)

Back Answer: abcd-0101(5)

Minimum Transition Time (ms): 100

Minimum Detection Time (ms): 20

Protocol Timeout (ms): 3000

**Figure A-41. MFR Version 2—Modify Line Signalling.**

*Line Signalling*

The Line Signalling parameters are link-by-link digital signals that use two signalling channels in each direction per circuit. Set the Server 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),**

**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-1111(15)**

- **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),**
**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-1111(15)**

- **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),**
**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-1111(15)**

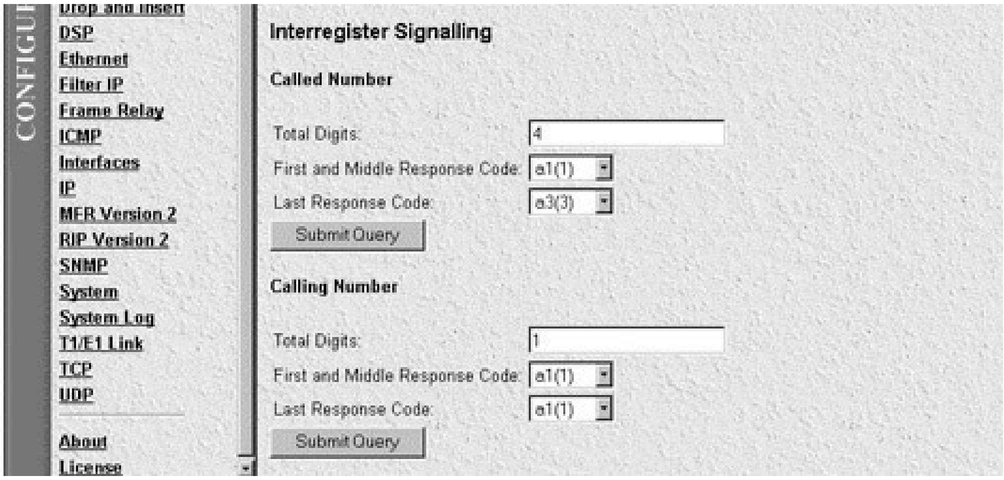
- **Back Answer (lineSigBackAnswer)**—Code to indicate a call has been completed.

  **abcd-0000(0),**
  **abcd-0000(0),**
  **abcd-0001(1),**
  **abcd-0010(2),**
  **abcd-0011(3),**
  **abcd-0100(4),**
  **abcd-0101(5),**
  **abcd-0110(6),**
  **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-1111(15)**

- **Minimum Transition Time (lineSigMinTransTime)**—The minimum transition time in milliseconds.
- **Minimum Detection Time (lineSigMinDetectTime)**—The minimum detect time in milliseconds.
- **Protocol Timeout (lineSigProtoTimeout)**—The time for a protocol timeout in milliseconds.

### A.11.2 MFR Version 2 (Modify Interregister Signalling)

From this screen you can modify Line Signalling parameters (see **Figure A-42**). 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.



Interregister Signalling

Called Number

Total Digits: 4

First and Middle Response Code: a1(1)

Last Response Code: a3(3)

Submit Query

Calling Number

Total Digits: 1

First and Middle Response Code: a1(1)

Last Response Code: a1(1)

Submit Query

**Figure A-42. MFR Version 2—Modify Line Signalling.**

*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 Server 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)**

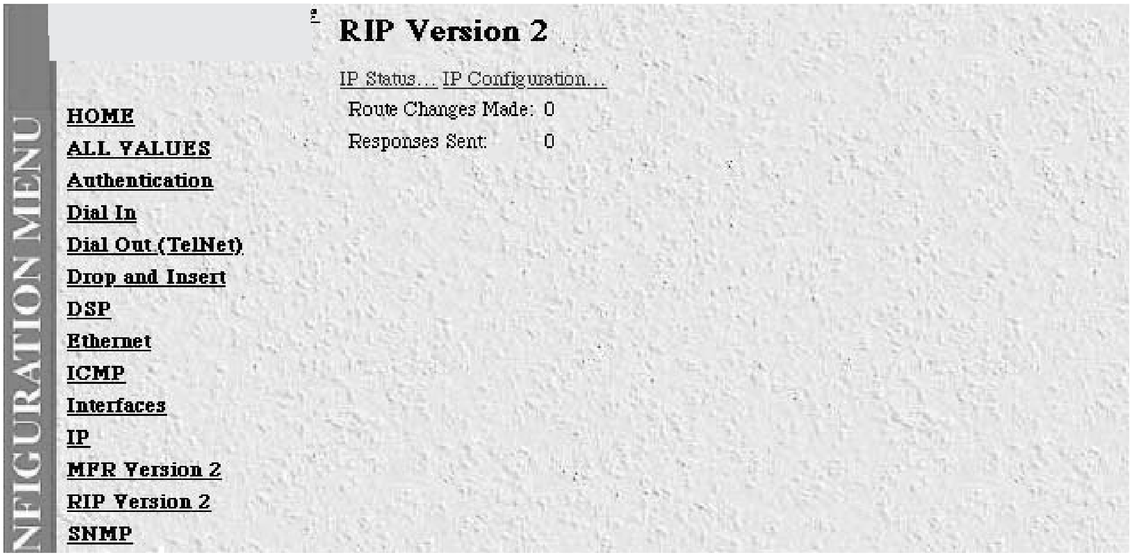
- **Last Response Code (InterRegCallingNum Last)—**The code specifying what is done after the last digit is sent for the calling number.

  **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)**

## A.13 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. 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 Server Configuration Menu (see **Figure 3-43**). Following **Figure A-43** are descriptions for each variable on this screen.



RIP Version 2

IP Status... IP Configuration...

Route Changes Made: 0

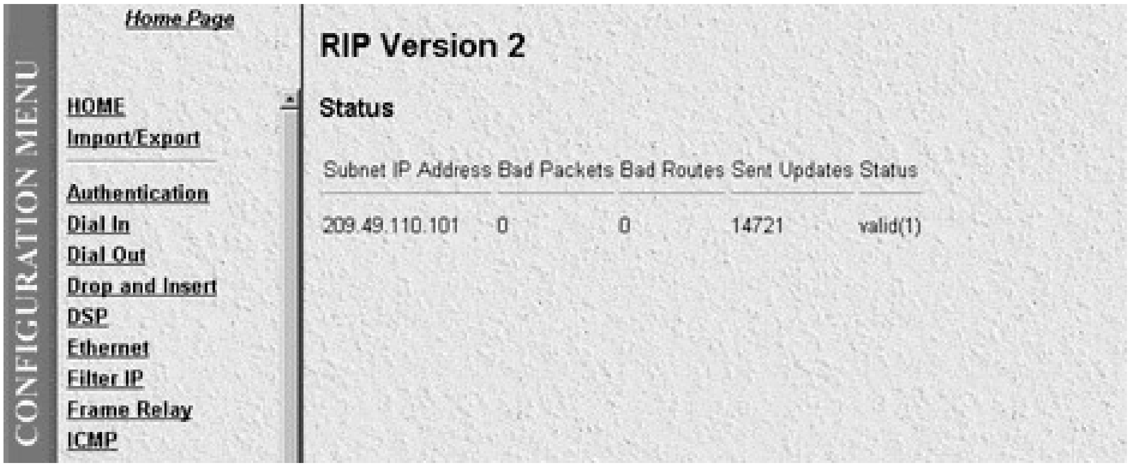
Responses Sent: 0

**Figure A-43. RIP Version 2 Main Screen.**

- **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.

### A.13.1 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**).



RIP Version 2

Status

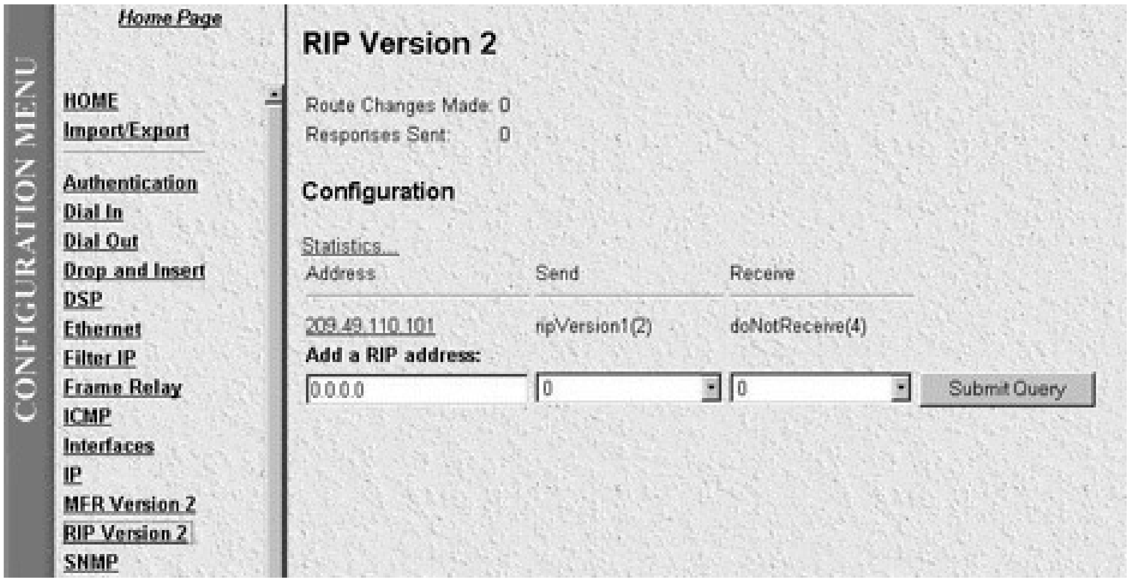
| Subnet IP Address | Bad Packets | Bad Routes | Sent Updates | Status |
|---|---|---|---|---|
| 209.49.110.101 | 0 | 0 | 14721 | valid(1) |

**Figure A-44. RIP Version 2—IP Status.**

- **Subnet IP Address (rip2IfStatAddress)**—The IP Address of this system on the indicated subnet. For unnumbered interfaces, it’s 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 that were subsequently discarded for any reason (for example, a version 0 packet, or an unknown command type).
- **Bad Routes (rip2IfStatRcvBadRoutes)**—The number of routes, in valid RIP packets, that were ignored for any reason (for example, 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.

### A.13.2 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**).



RIP Version 2

Route Changes Made: 0
Responses Sent: 0

Configuration

Statistics...

| Address | Send | Receive |
|---|---|---|
| 209.49.110.101 | ripVersion1(2) | doNotReceive(4) |

Add a RIP address:

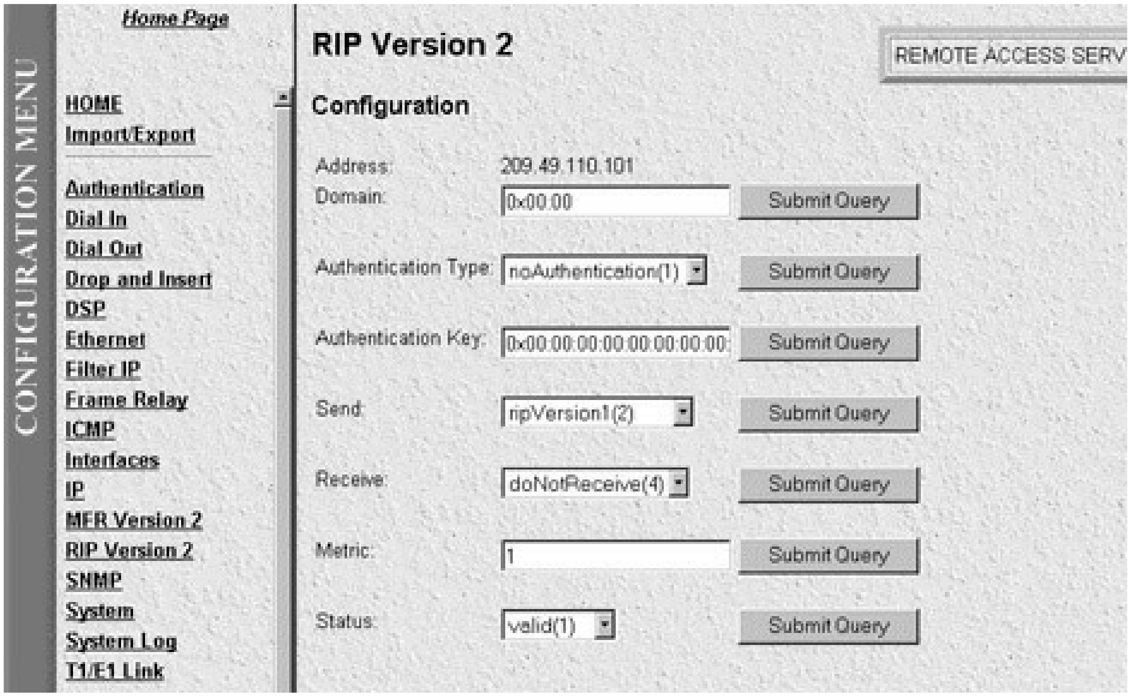
| | | |
|---|---|---|
| 0.0.0.0 | 0 | 0 |

**Figure A-45. RIP Version 2—IP Configuration.**

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 shown on this this screen will be described in the following section, RIP **Version 2** (IP Configuration Details).

### A.13.3 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**). This section describes each of the objects.



RIP Version 2

Configuration

Address: 209.49.110.101
Domain: 0x00:00
Authentication Type: noAuthentication(1)
Authentication Key: 0x00:00:00:00:00:00:00:00:
Send: ripVersion1(2)
Receive: doNotReceive(4)
Metric: 1
Status: valid(1)

**Figure A-46. RIP Version 2—Configuration Details.**

- **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.

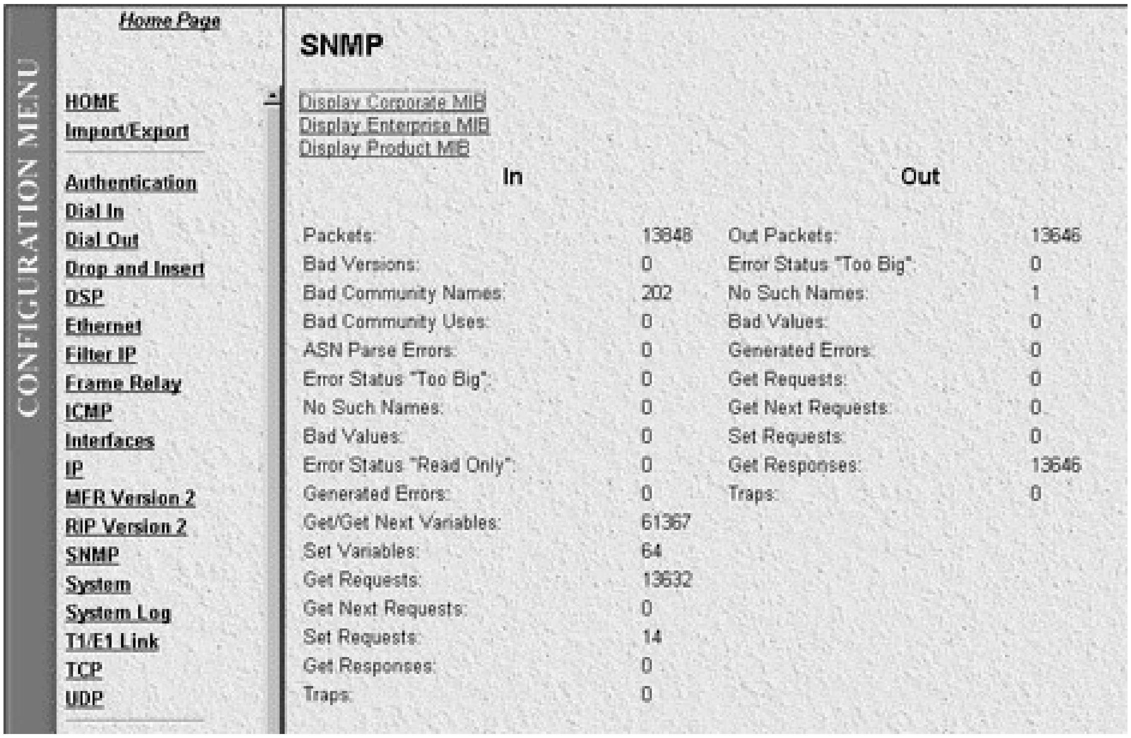
  **rip1 (1),**
  **rip2 (2),**
  **rip1OrRip2 (3),**
  **doNotRecieve (4)**

- **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),**

## A.14 SNMP

The Server provides management and statistical information on SNMP. Detailed information on the SNMP MIB variables may be downloaded from the RFC. Select SNMP from the Server's Configuration Menu to monitor SNMP statistics. Following **Figure A-47** are descriptions for each variable on this page.



SNMP

| In | | Out | |
|---|---|---|---|
| Packets: | 13848 | Out Packets: | 13646 |
| Bad Versions: | 0 | Error Status "Too Big": | 0 |
| Bad Community Names: | 202 | No Such Names: | 1 |
| Bad Community Uses: | 0 | Bad Values: | 0 |
| ASN Parse Errors: | 0 | Generated Errors: | 0 |
| Error Status "Too Big": | 0 | Get Requests: | 0 |
| No Such Names: | 0 | Get Next Requests: | 0 |
| Bad Values: | 0 | Set Requests: | 0 |
| Error Status "Read Only": | 0 | Get Responses: | 13646 |
| Generated Errors: | 0 | Traps: | 0 |
| Get/Get Next Variables: | 61367 | | |
| Set Variables: | 64 | | |
| Get Requests: | 13632 | | |
| Get Next Requests: | 0 | | |
| Set Requests: | 14 | | |
| Get Responses: | 0 | | |
| Traps: | 0 | | |

**Figure A-47. SNMP In or Out.**

- **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." Note

that it is a protocol error to generate an SNMP PDU that contains the value "readOnly" in the error-status field, as such this object is provided to detect incorrect implementations of the SNMP.

- **Generated Errors (snmpInGenErrs)**—The total number of SNMP PDUs that 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 that 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 that have been accepted and processed by the SNMP protocol entity.
- **Get Next Requests (snmpInGetNexts)**—The total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP protocol entity.
- **Set Requests (snmpInSetRequests)**—The total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity.
- **Get Responses (snmpInGetResponses)**—The total number of SNMP Get-Response PDUs that have been accepted and processed by the SNMP protocol entity.
- **Traps (snmpInTraps)**—The total number of SNMP Trap PDUs that have been accepted and processed by the SNMP protocol entity.

*Out*

- **Out Packets (snmpOutPkts)**—The total number of SNMP Messages that were passed from the SNMP protocol entity to the transport service.
- **Error Status "Too Big" (snmpOutTooBigs)**—The total number of SNMP PDUs that 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 that 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 that 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 that 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 that have been generated by the SNMP protocol entity.
- **Get Next Requests (snmpOutGetNexts)**—The total number of SNMP Get-Next PDUs that have been generated by the SNMP protocol entity.
- **Set Requests (snmpOutSetRequests)**—The total number of SNMP Set-Request PDUs that have been generated by the SNMP protocol entity.
- **Get Responses (snmpOutGetResponses)**—The total number of SNMP Get-Response PDUs that have

been generated by the SNMP protocol entity.

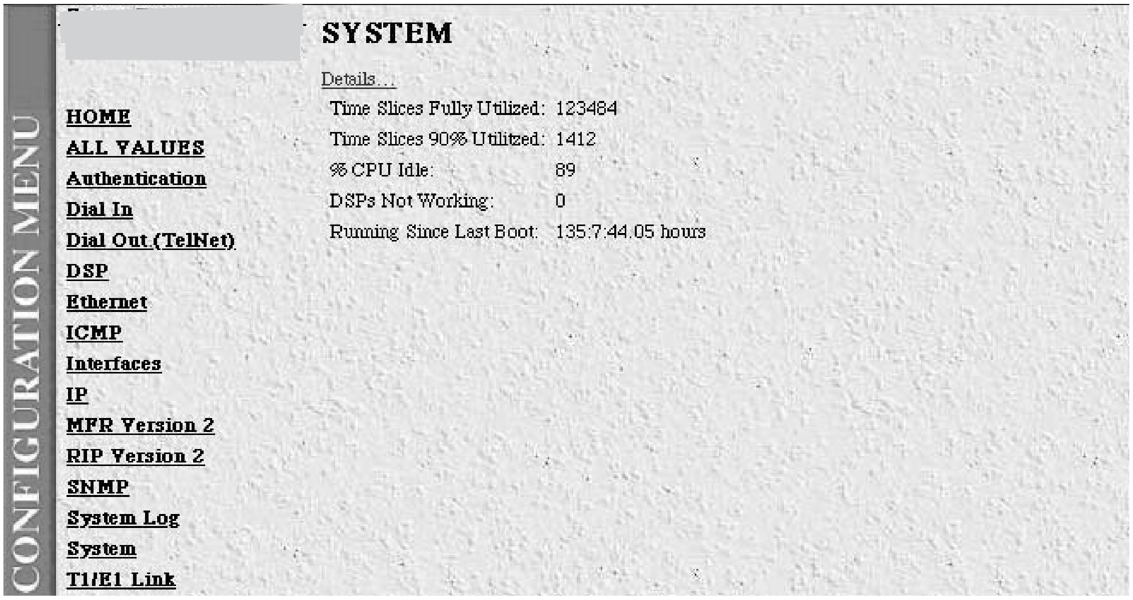
- **Traps (snmpOutTraps)**—The total number of SNMP Trap PDUs that have been generated by the SNMP protocol entity.
- **Authentication Failure Traps (snmpEnableAuthenTraps)**—Indicates whether the SNMP agent process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information, so it lets you disable all authentication-failure traps. We strongly recommend that you store this object in non-volatile memory, so that it remains constant between re-initializations of the network-management system.

  **enable (1);**
  **disable (2)**

## A.15 System

The System Section contains general setup information about the Server. System parameters may be read-only and read/write parameters. These parameters are 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 Server's Configuration Menu (see **Figure A-48**). Following **Figure A-48** are descriptions for each variable on this screen.



[redacted] SYSTEM

Details...

```
Time Slices Fully Utilized:  123484
Time Slices 90% Utilized:    1412
% CPU Idle:                  89
DSPs Not Working:            0
Running Since Last Boot:     135:7:44.05 hours
```

**Figure A-48. System Main Screen.**

- **Total Active Calls (diActive)**—This number, ranging from 0 to 60 (this number can be no more than 46 for two T1/PRIs running PRI, and 60 for an E1/PRI) displays the total number of calls being processed (connecting, dead, authenticating, etc.) in a Server at the time the HOME page was brought up.

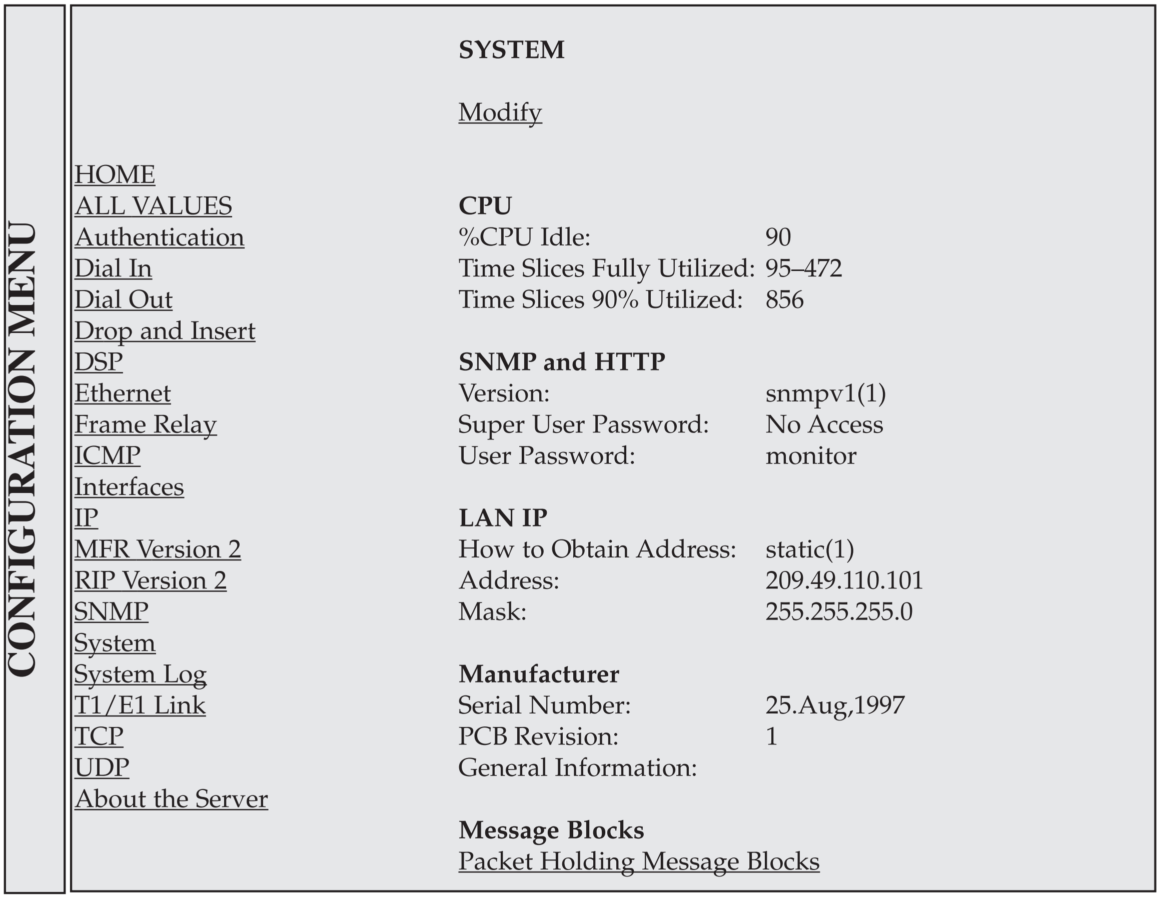
- **Time Slices Fully Utilized (boxCPUCritical)**—Each second is divided into 100 time slices. If a time slice passes in which all the CPU power was used to handle the system, then this count is incremented by one.
- **Time Slices 90% Utilized (boxCPUWarning)**—Each second is divided into 100 time slices. If a time slice passes 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 that is not being used by the Server. 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 DSPs in the Server 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 Server will automatically remove the non-working DSP from the resource pool. One symptom of a DSP failure is the Server isn't handling as many calls as it should. A DSP may be taken out of service if it fails to respond to the Server 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 Server has been running since the it was last reset. It displays the number of hours and rolls over after 1,193 hours (497 days).

### A.15.1 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-49**). To reach this screen, select Details from the main System Details screen.

## NOTE

**You can modify SNMP, HTTP, and LAN IP parameters by selecting Modify from the top of this screen.**



**SYSTEM**

**CPU**
%CPU Idle: 90
Time Slices Fully Utilized: 95–472
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**

**Figure A-49. System Details (CPU, SNMP and HTTP, LAN IP, Manufacturer, 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 used.
- **Time Slices Fully Utilized (boxCPUcritical)**—This value represents a count of how many times the CPU was fully used (expressed in 1/100th seconds).
- **Time Slices 90% Utilized (boxCPUWarning)**—This value represents a count of how many times the CPU approached full use (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 #) is a revision of Simple Network Management Protocol (not just a new MIB) that 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 Server.

## NOTE

**This software release of the Server, Rev. 1.3, uses only disable(0), static(1), and 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 (for example, Server T1 to T1 usage only)

**static(1)**—LAN IP address is obtained from the RS-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 Internet address. It is used primarily by diskless nodes, when they first initialize, to find their Internet addresses.

**bootp(3)**—Not implemented in this version.

**dhcp(4)**—Not implemented in this version.

- **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.

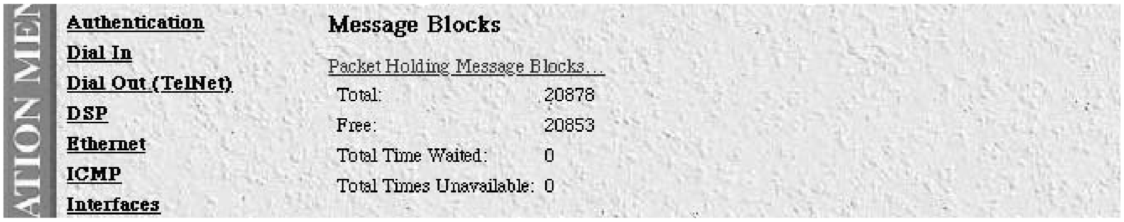
*Manufacturer*

This section describes Server-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 Server 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 Server message block usage (see **Figure A-50**).



Message Blocks

Packet Holding Message Blocks...

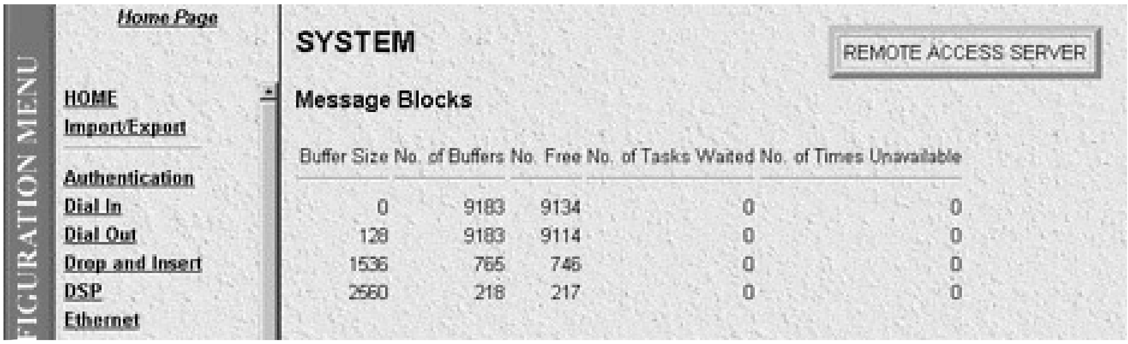
| | |
|---|---|
| Total: | 20878 |
| Free: | 20853 |
| Total Time Waited: | 0 |
| Total Times Unavailable: | 0 |

**Figure A-50. Message Blocks.**

- **Packet Holding Message Blocks**—The buffer usage of Server message blocks based upon message block sizes.
- **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 Server system manages the I960 processor utilization by allocating message blocks for data transfers. This section shows buffer usage of Server message blocks based upon message block sizes (See **Figure A-51**).



SYSTEM

Message Blocks

| Buffer Size | No. of Buffers | No. Free | No. of Tasks Waited | No. of Times Unavailable |
|---|---|---|---|---|
| 0 | 9183 | 9134 | 0 | 0 |
| 128 | 9183 | 9114 | 0 | 0 |
| 1536 | 765 | 746 | 0 | 0 |
| 2560 | 218 | 217 | 0 | 0 |

**Figure A-51. Packet Holding Message Blocks.**

- **Buffer Size(boxbuffersize)**—The size in bytes of the buffer.
- **No. of Buffers (boxbuffercount)**—The number of buffers this size that are currently free for use.
- **No. Free (boxbuffersfree)**—The number of buffers this size that are currently free for use.
- **No. of Tasks Waited (boxCountBufferTaskWait)**—The number of times a task has waited for this buffer size.

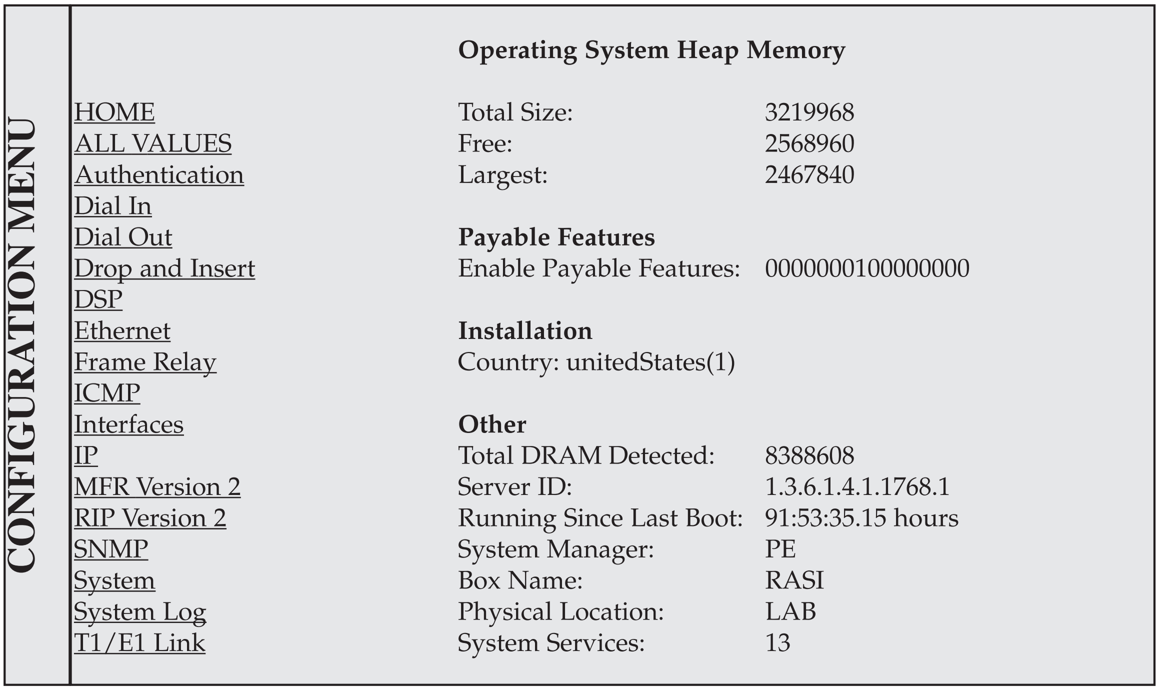
- **No. of Times Unavailable (boxCountBufferUnavailable)**—The number of times one of these buffers was unavailable.

### A.15.2 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-52**). To reach this screen, scroll down from the previous screen.

## NOTE

**You can modify Payable Features, Installation, and Other parameters by selecting Modify from the top of this screen).**



**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
Server ID: 1.3.6.1.4.1.1768.1
Running Since Last Boot: 91:53:35.15 hours
System Manager: PE
Box Name: RASI
Physical Location: LAB
System Services: 13

**Figure A-52. System Details (Operating System Heap Memory, Payable Features, Installation, Other).**

*Operating System Heap Memory*

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. It changes the way the box operates based on local laws.

  **other(0),**<br>
  **unitedStates(1),**<br>
  **australia(2),**<br>
  **canada(3),**<br>
  **europeanUnion(4),**<br>
  **france(5),**<br>
  **germany(6)**

*Other*

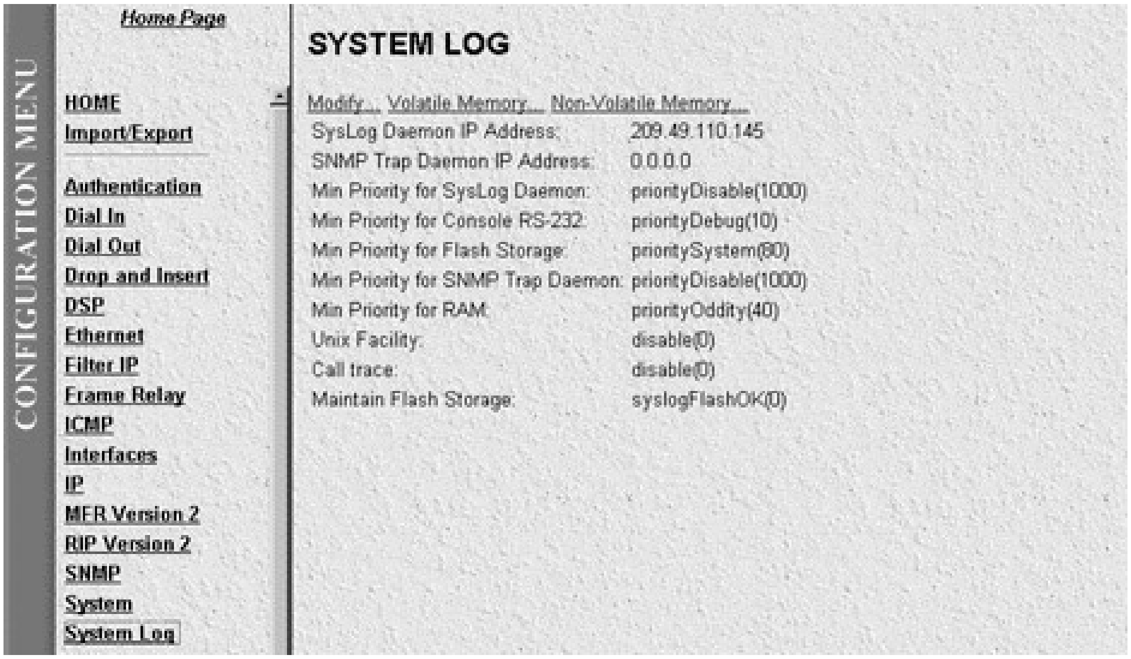
- **Total DRAM Detected(boxDetectedMemory)**—The total number of bytes of DRAM detected by the CPU.
- **Model 2800 ID(sysObjectID)**—This SNMP variable represents the “kind of box” being managed as defined by specification RFC1213.MIB.
- **Running Since Last Boot(sysUpTime)**—This SNMP variable represents 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. (Refer to RFC1213.MIB.)
- **Physical Location(sysLocation)**—The physical location of this node (for example, “telephone closet, 3rd floor”). (Refer to RFC1213.MIB.)
- **System Services(sysServices)**—A value which indicates the set of services that this entity primarily offers. (Refer to RFC1213.MIB.)

You may modify SNMP and HTTP, LAN IP, Payable Features, Installation, and Other parameters of the Server simply by selecting Modify at the top of the System Details Screen.

## A.16 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 Enterprise MIB object identifiers.

To reach the System Log Section, select System Log from the Server Configuration Menu (see **Figure A-53**). Following **Figure A-53** are descriptions for each variable on this screen.



SYSTEM LOG

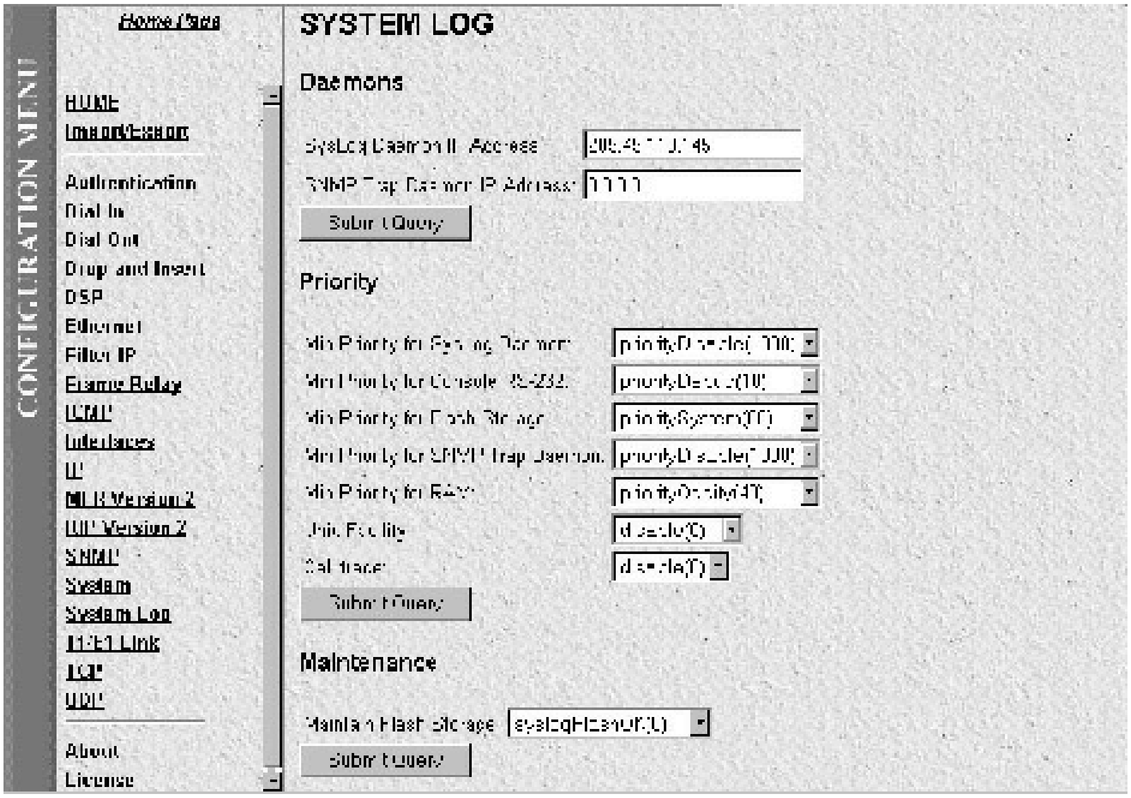
```
SysLog Daemon IP Address:          209.49.110.145
SNMP Trap Daemon IP Address:       0.0.0.0
Min Priority for SysLog Daemon:    priorityDisable(1000)
Min Priority for Console RS-232:   priorityDebug(10)
Min Priority for Flash Storage:    prioritySystem(80)
Min Priority for SNMP Trap Daemon: priorityDisable(1000)
Min Priority for RAM:              priorityOddity(40)
Unix Facility:                     disable(0)
Call trace:                        disable(0)
Maintain Flash Storage:            syslogFlashOK(0)
```

**Figure A-53. System Log Main Screen.**

The objects contained on this screen are read-write values. They are described in the next section.

### A.16.1 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-54**).



SYSTEM LOG

Daemons

SysLog Daemon IP Address: 205.[illegible]

SNMP Trap Daemon IP Address: 1.1.1.1

Submit Query

Priority

Min Priority for SysLog Daemon: priorityDisable(1000)

Min Priority for Console RS-232: priorityDebug(10)

Min Priority for Flash Storage: prioritySystem(80)

Min Priority for SNMP Trap Daemon: priorityDisable(1000)

Min Priority for RAM: priorityOddity(40)

Unix Facility: disable(0)

Call trace: disable(0)

Submit Query

Maintenance

Maintain Flash Storage: syslogFlashOK(0)

Submit Query

**Figure A-54. System Log (Modify Daemon, Priority, Maintenance).**

*Daemons*

- **SysLog Daemon IP Address(syslogDaemonIP)**—The IP address of a host system that 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 that 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 that 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 that 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 that 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 that 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 that will log every single function call and return. If a box fails, 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 that 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)**

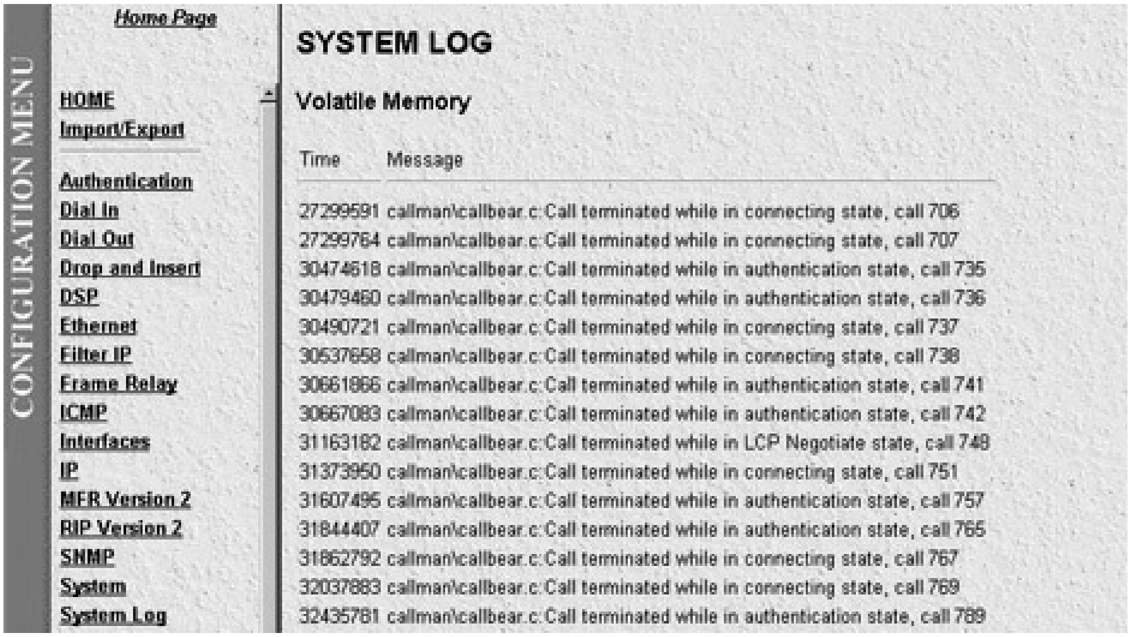
*Maintenance*

- **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)**

### A.16.2 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-55**).



SYSTEM LOG

Volatile Memory

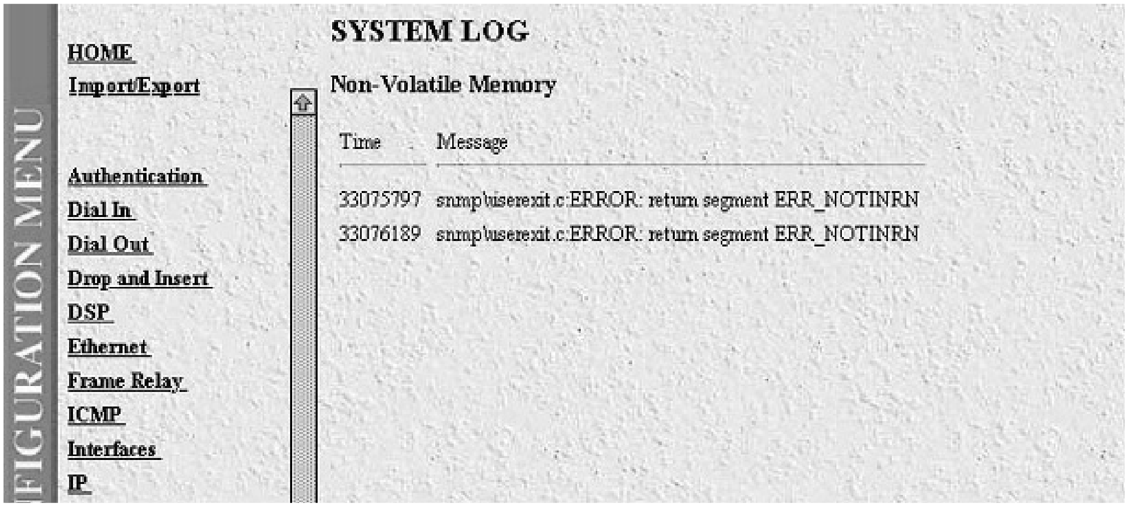
```
Time     Message
27299591 callman\callbear.c:Call terminated while in connecting state, call 706
27299764 callman\callbear.c:Call terminated while in connecting state, call 707
30474618 callman\callbear.c:Call terminated while in authentication state, call 735
30479460 callman\callbear.c:Call terminated while in authentication state, call 736
30490721 callman\callbear.c:Call terminated while in connecting state, call 737
30537658 callman\callbear.c:Call terminated while in connecting state, call 738
30661866 callman\callbear.c:Call terminated while in authentication state, call 741
30667083 callman\callbear.c:Call terminated while in authentication state, call 742
31163182 callman\callbear.c:Call terminated while in LCP Negotiate state, call 748
31373950 callman\callbear.c:Call terminated while in connecting state, call 751
31607496 callman\callbear.c:Call terminated while in authentication state, call 757
31844407 callman\callbear.c:Call terminated while in authentication state, call 765
31862792 callman\callbear.c:Call terminated while in connecting state, call 767
32037883 callman\callbear.c:Call terminated while in connecting state, call 769
32435781 callman\callbear.c:Call terminated while in authentication state, call 789
```

**Figure A-55. System Log—Volatile Memory.**

- **Time (slTick)**—The time stamp in 100-ms intervals of the stored message.
- **Message (slMessage)**—Stored system-log message.

### A.16.3 System Log (Non-Volatile Memory)

The System Log - Non-Volatile screen shows non-volatile RAM messages for each 100-ms time stamp. To reach this screen, select Non-Volatile Memory from the main System Log screen (see **Figure A-56**).



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
```

**Figure A-56. System Log—Non-Volatile Memory.**

- **Time (slfTick)**—The time stamp in 100-ms intervals of the stored message.
- **Message (slfMessage)**—Stored system log message.

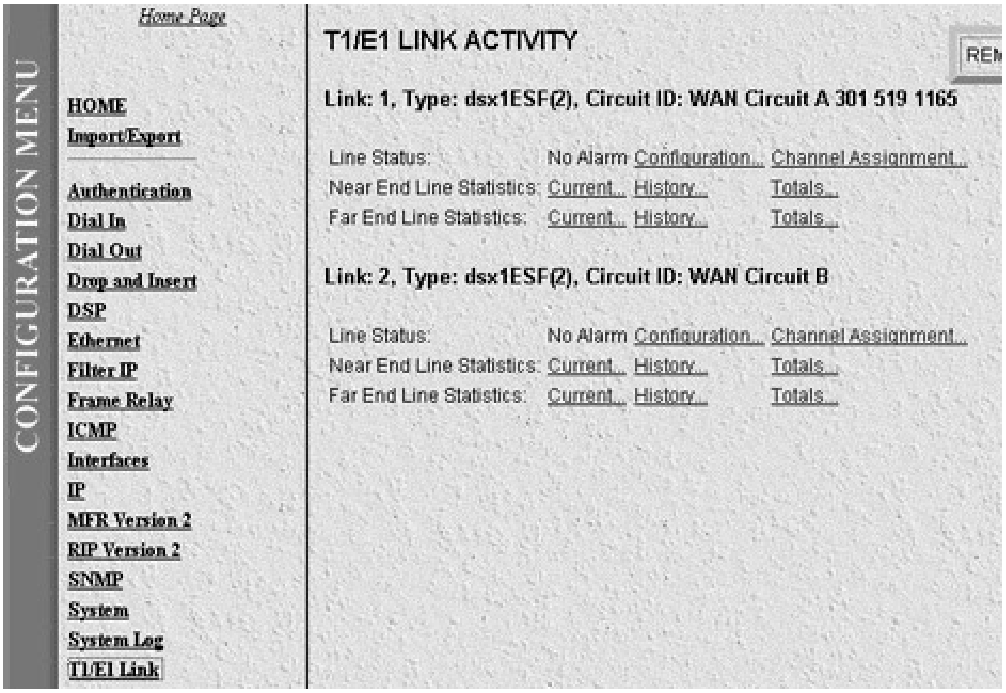
## A.17 T1/E1 Link

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 and 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 of the 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 Server Configuration Menu (see **Figure A-57**). Following **Figure A-57** are descriptions for each variable on this page.



T1/E1 LINK ACTIVITY

Link: 1, Type: dsx1ESF(2), Circuit ID: WAN Circuit A 301 519 1165

| | | | |
|---|---|---|---|
| Line Status: | No Alarm | Configuration... | Channel Assignment... |
| Near End Line Statistics: | Current... | History... | Totals... |
| Far End Line Statistics: | Current... | History... | Totals... |

Link: 2, Type: dsx1ESF(2), Circuit ID: WAN Circuit B

| | | | |
|---|---|---|---|
| Line Status: | No Alarm | Configuration... | Channel Assignment... |
| Near End Line Statistics: | Current... | History... | Totals... |
| Far End Line Statistics: | Current... | History... | Totals... |

**Figure A-57. T1/E1 Link Activity Main Screen.**

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 (for example, equipment side) with even numbers and outside interfaces (for example, 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, without CRC
  **dsx1E1-CRC-MF**—Based on CCITT/ITU G.704 with TS16 multiframing, with CRC

- **Circuit ID (dsx1CircuitIdentifier)**—This variable contains the transmission vendor's circuit identifier, for the purpose of facilitating troubleshooting.

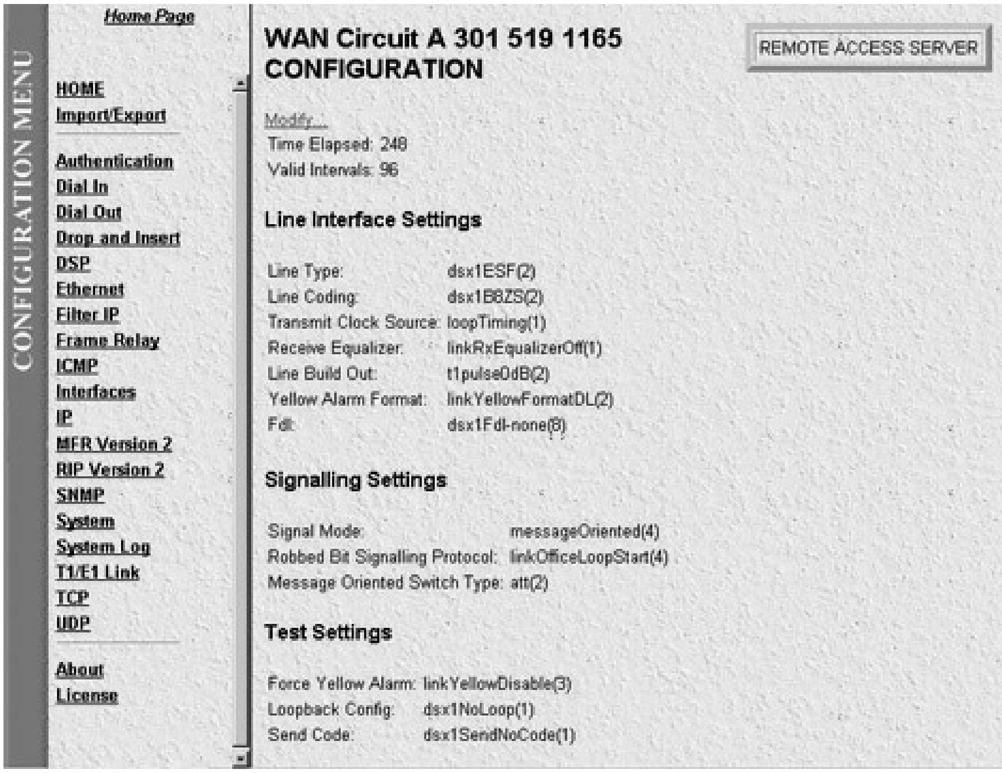
- **Line Status (dsx1LineStatus)**—This variable indicates the Line Status of the interface. It contains loopback, failure, received "alarm" and transmitted "alarm" information.

  The dsx1LineStatus is a bitmap 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 | **Adsx1NoAlarm** | 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 (D4 Superframe or Extended Superframe), number of time intervals passed, and kind of line coding (B8ZS or AMI). **Figure A-58** shows the Circuit Configuration Screen for a typical ESF connection. Following **Figure A-58** are descriptions for each variable on this page.



WAN Circuit A 301 519 1165
CONFIGURATION

Time Elapsed: 248
Valid Intervals: 96

Line Interface Settings

| | |
|---|---|
| Line Type: | dsx1ESF(2) |
| Line Coding: | dsx1B8ZS(2) |
| Transmit Clock Source: | loopTiming(1) |
| Receive Equalizer: | linkRxEqualizerOff(1) |
| Line Build Out: | t1pulse0dB(2) |
| Yellow Alarm Format: | linkYellowFormatDL(2) |
| Fdl: | dsx1Fdl-none(8) |

Signalling Settings

| | |
|---|---|
| Signal Mode: | messageOriented(4) |
| Robbed Bit Signalling Protocol: | linkOfficeLoopStart(4) |
| Message Oriented Switch Type: | att(2) |

Test Settings

| | |
|---|---|
| Force Yellow Alarm: | linkYellowDisable(3) |
| Loopback Config: | dsx1NoLoop(1) |
| Send Code: | dsx1SendNoCode(1) |

**Figure A-58. Circuit Activity.**

- **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 since the interface has been online.
- **Line Type (dsx1LineType) Type (dsx1LineType)**—This variable indicates the variety of DS1 Lines 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, without CRC |
| **dsx1E1-CRC-MF(7)** | Based on CCITT/ITU G.704 with TS16 multiframing, with 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. The AT&T specification of at least one pulse every 8 bit periods is literally implemented by forcing a pulse in bit 8 of each channel. Thus, only seven bits per channel, or 1.344 Mbps, is available for data.

**dsx1B8ZS (2)**—A specified pattern of normal bits and bipolar violations 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)**—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 that 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 will always return this as its 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 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 manufacturer of the switch 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 a 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 Servers.

  **linkGroundStart(1),**
  **linkLoopStart(2),**
  **linkOfficeGroundStart(3),**
  **linkOfficeLoopStart(4),**
  **linkMFR2(5)**

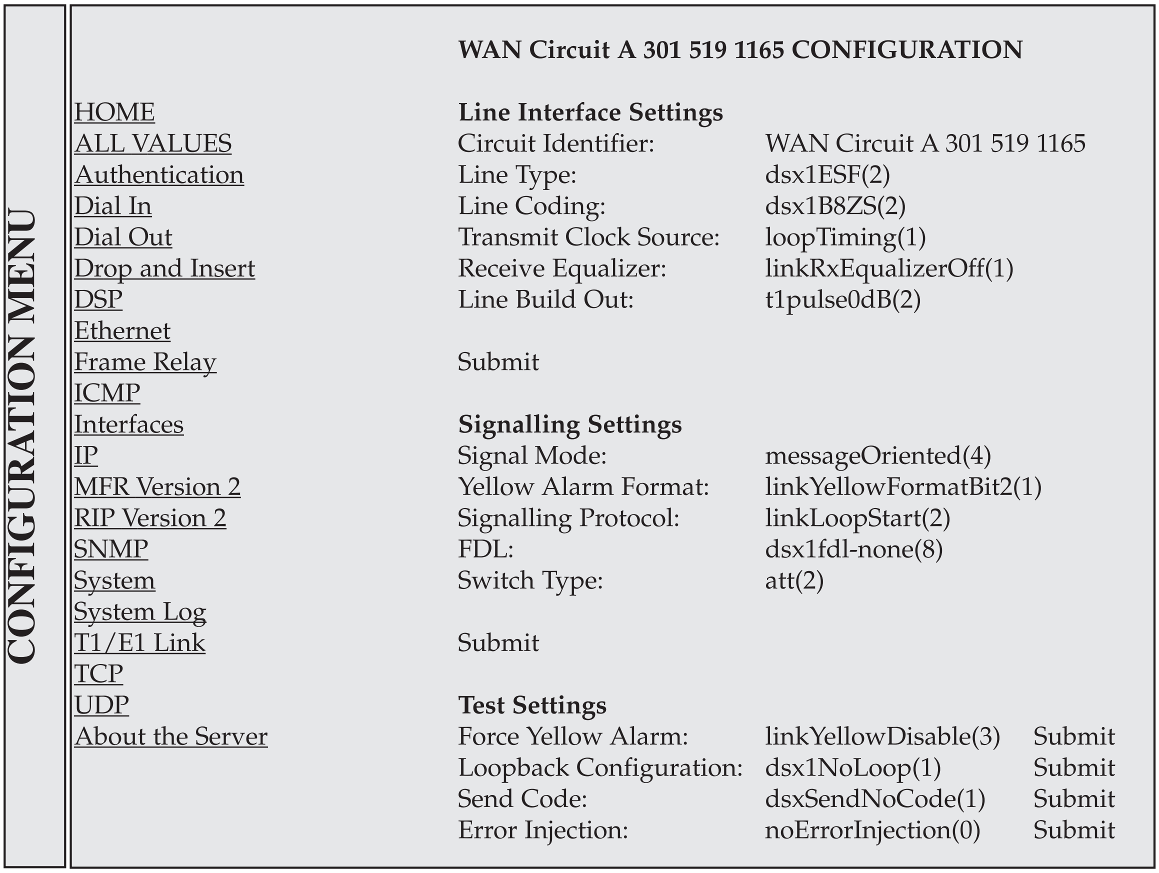
- **Line Build Out (linkLineBuildOut)**—This variable is used in T1 applications to adjust the T1 pulse shape at the cross-connect point. Select the enumeration that best represents the amount of cable between the unit and the cross-connect point.

  **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 can modify Line Interface Settings, Signalling Settings, and Test Settings, and change the T1/E1 Pulse shapes. **Figure A-59** shows Line Interface Settings and Signalling 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) | |

Submit

**Signalling Settings**

| | | |
|---|---|---|
| Signal Mode: | messageOriented(4) | |
| Yellow Alarm Format: | linkYellowFormatBit2(1) | |
| Signalling Protocol: | linkLoopStart(2) | |
| FDL: | dsx1fdl-none(8) | |
| Switch Type: | att(2) | |

Submit

**Test Settings**

| | | |
|---|---|---|
| Force Yellow Alarm: | linkYellowDisable(3) | Submit |
| Loopback Configuration: | dsx1NoLoop(1) | Submit |
| Send Code: | dsxSendNoCode(1) | Submit |
| Error Injection: | noErrorInjection(0) | Submit |

**Figure A-59. Line Status (Modify Line Interface, Signalling, and Test Settings.**

*Line Interface Settings*

- **Circuit ID (dsx1CircuitIdentifier)**—This variable contains the transmission vendor's circuit identifier, to facilitate 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)**<br>
  **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, without CRC
**dsx1E1-CRC-MF(7)**—Based on CCITT/ITU G.704 with TS16 multiframing, with 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)**—In Jammed Bit Zero Suppression, the AT&T specification of at least one pulse every 8 bit periods is literally implemented by forcing a pulse in bit 8 of each channel. Thus, only seven bits per channel, or 1.344 Mbps, is available for data.
  **dsx1B8ZS (2)**—A specified pattern of normal bits and bipolar violations is 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 that 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 Servers.

**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 manufacturer of the switch 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 a 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 will always return this as its 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:

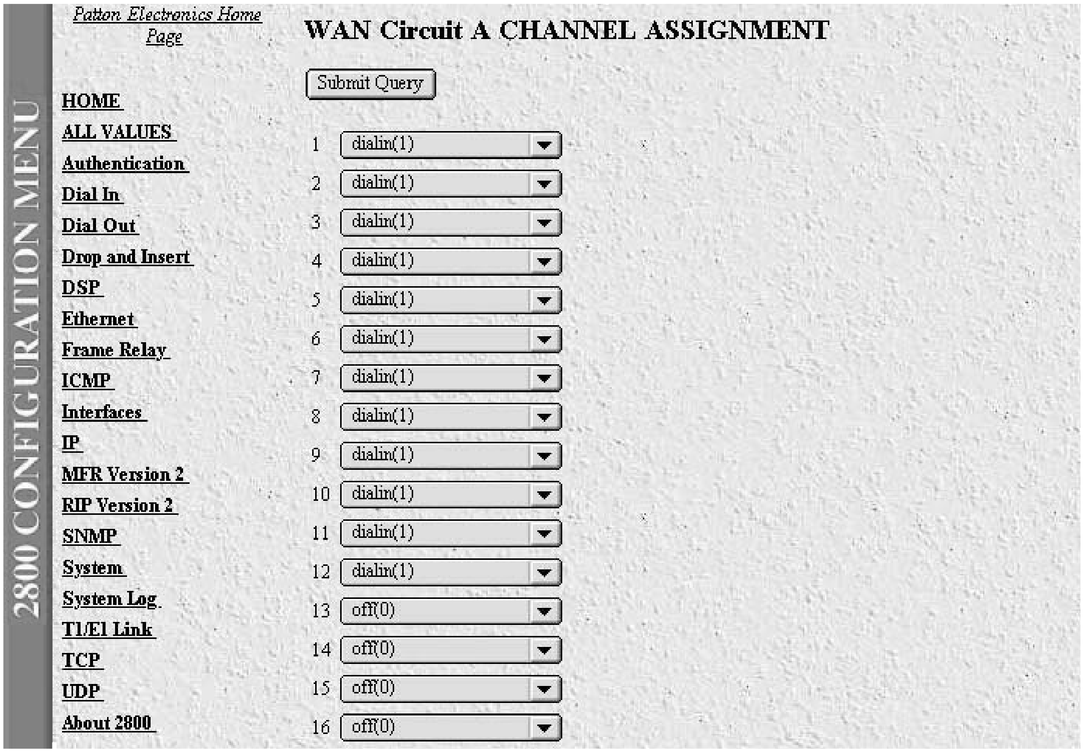
  **dsx1SendNoCode**—Sending looped or normal data
  **dsx1SendLineCode**—Sending a request for a line loopback
  **dsx1SendPayloadCode**—Sending a request for a payload loopback
  **dsx1SendResetCode**—Sending a loopback termination request
  **dsx1SendQRS**—Sending a Quasi-Random Signal (QRS) test pattern
  **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 ASSIGNMENT)

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-60**).



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) |
| 15 | off(0) |
| 16 | off(0) |

**Figure A-60. Slot/Channel Assignments.**

- **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)**

## A.18 Near End Line Statistics

### A.18.1 CURRENT

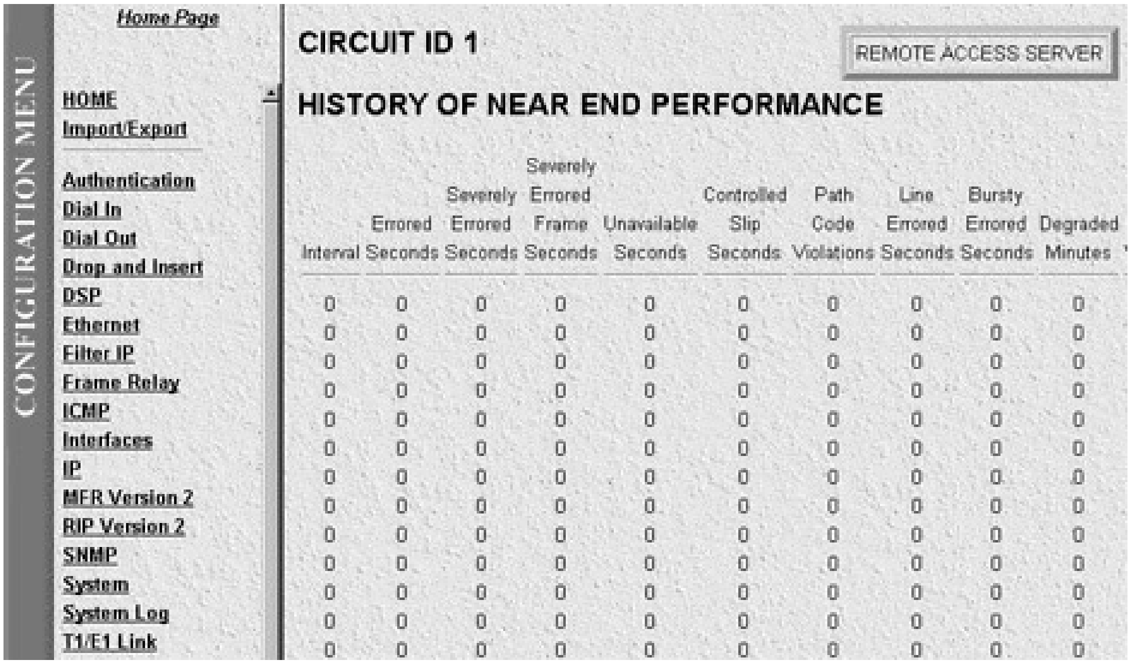
Select Near End Line Statistics—Current to show line statistics for the current 15-minute interval (see **Figure A-62**).

- **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.

### A.18.2 HISTORY

Select Near End Line Statistics—History to show line statistics for earlier, completed 15-minute intervals (see **Figure A-61**.



CIRCUIT ID 1

HISTORY OF NEAR END PERFORMANCE

| | | | Severely | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Severely | Errored | | Controlled | Path | Line | Bursty | |
| | Errored | Errored | Frame | Unavailable | Slip | Code | Errored | Errored | Degraded |
| Interval | Seconds | Seconds | Seconds | Seconds | Seconds | Violations | Seconds | Seconds | Minutes |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Figure A-61. Near End Performance—Historical Activity.**

- **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-minute interval (assuming that all 96 intervals are valid).

  Choose Details to view historical information for any previous 15-minute interval T1/E1 link.

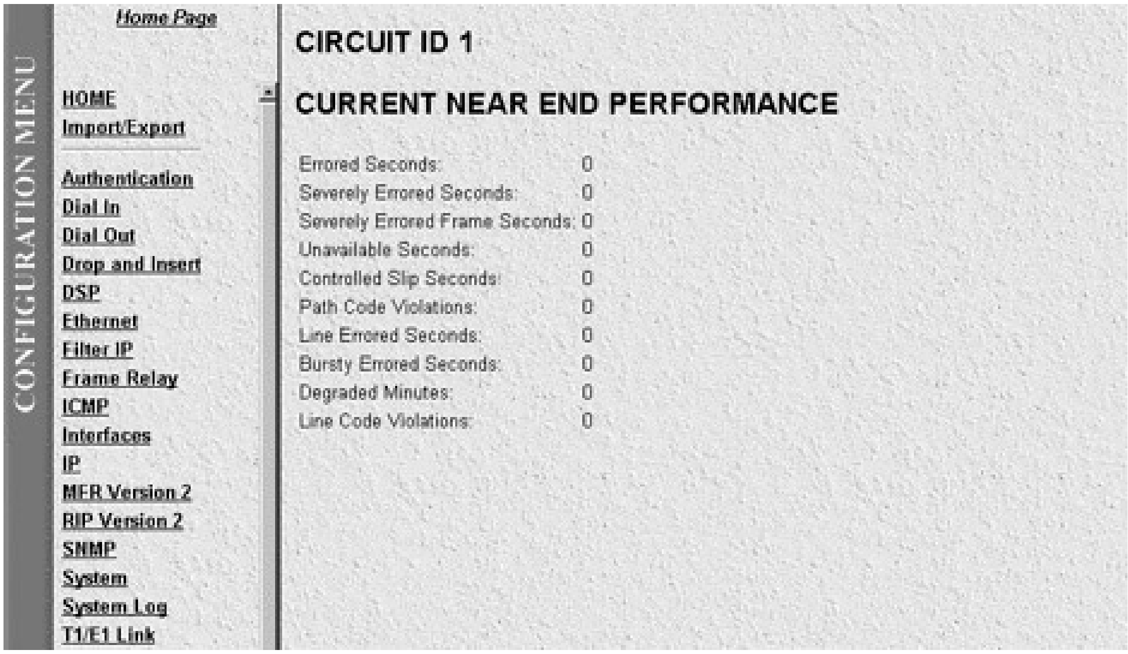
***Near End Line Statistics (History Details)***

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**).

- **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.

### A.18.3 Totals

Select Near End Line Statistics—Totals to show sums of error statistics collected over the previous 24-hour interval (see **Figure A-62**).



CIRCUIT ID 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 |

**Figure A-62. Near End Performance—Totals.**

- **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.

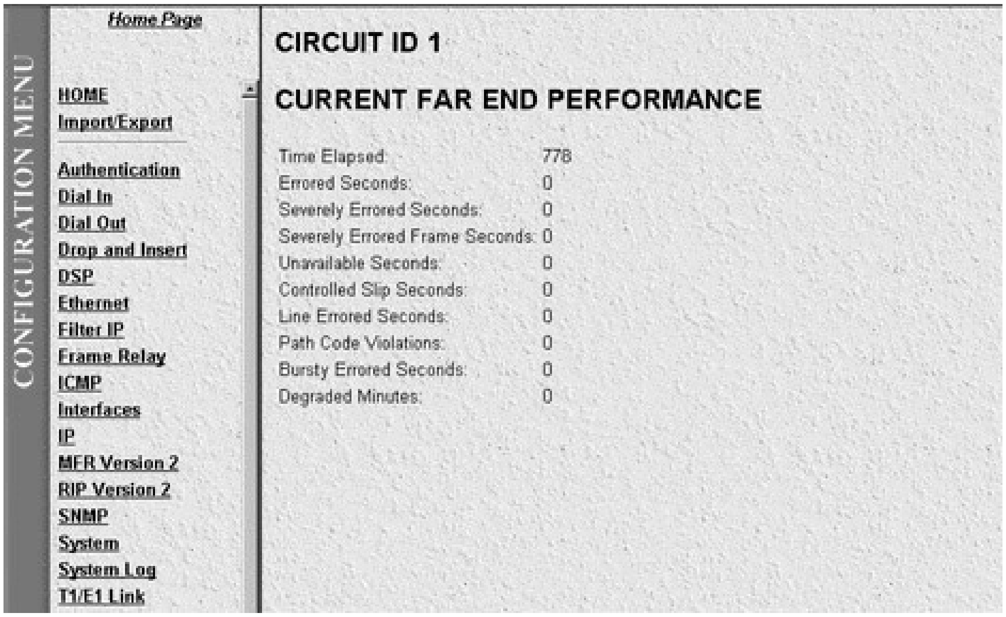
- **Degraded Minutes (dsx1TotalDMs)**—The number of Degraded Minutes (DMs) encountered by a DS1 interface in the previous 24-hour interval.

- **Line Code Violations (dsx1TotalLCVs)**—The number of Line Code Violations (LCVs) encountered by a DS1 interface in the current 15-minute interval.

## A.19 Far End Line Statistics

### A.19.1 CURRENT

Select Far End Line Statistics—Current to show far-end statistics for the current 15-minute interval (see **Figure A-63**).



CIRCUIT ID 1

CURRENT FAR END PERFORMANCE

| | |
|---|---|
| Time Elapsed: | 778 |
| Errored Seconds: | 0 |
| Severely Errored Seconds: | 0 |
| Severely Errored Frame Seconds: | 0 |
| Unavailable Seconds: | 0 |
| Controlled Slip Seconds: | 0 |
| Line Errored Seconds: | 0 |
| Path Code Violations: | 0 |
| Bursty Errored Seconds: | 0 |
| Degraded Minutes: | 0 |

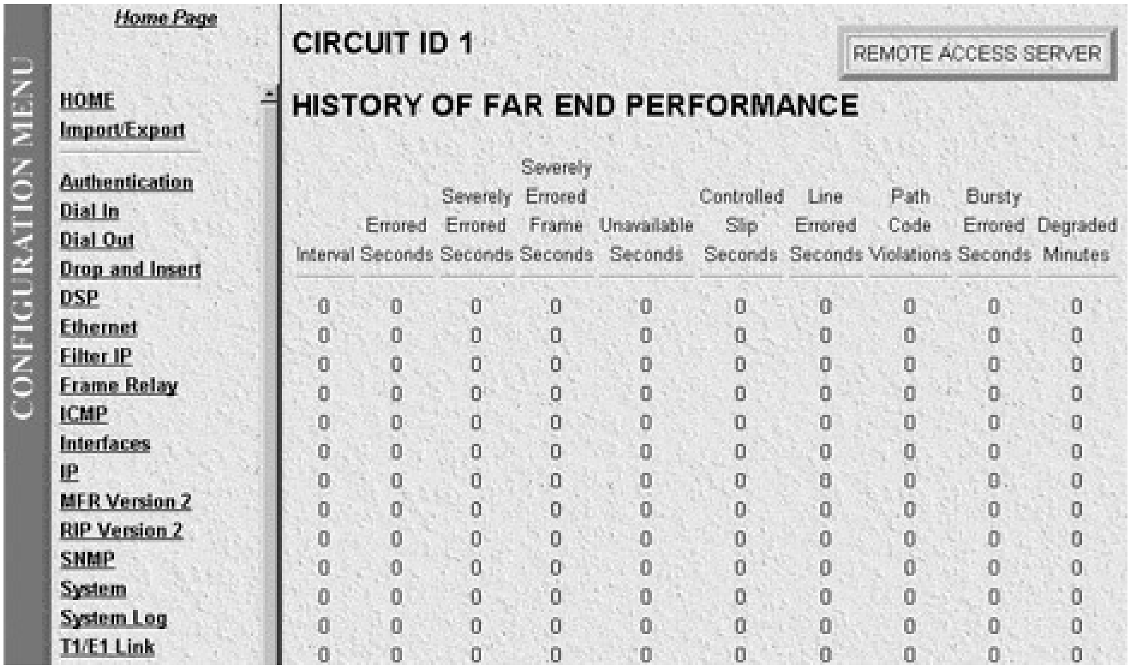
**Figure A-63. Far End Performance—Current.**

- **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.

### A.19.2 History

Select **Far End Line Statistics—History** to show far-end statistics for earlier, completed 15-minute intervals (see **Figure A-64**).



CIRCUIT ID 1

HISTORY OF FAR END PERFORMANCE

| Interval | Errored Seconds | Severely Errored Seconds | Severely Errored Frame Seconds | Unavailable Seconds | Controlled Slip Seconds | Line Errored Seconds | Path Code Violations | Bursty Errored Seconds | Degraded Minutes |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

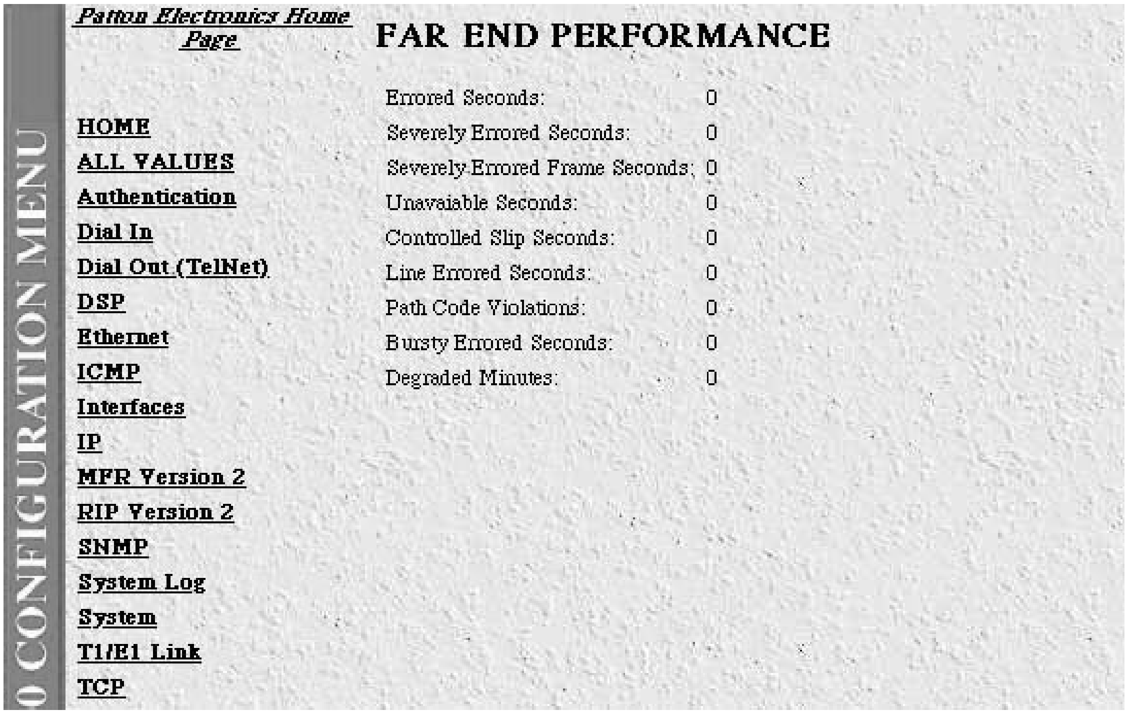
**Figure A-64. Far End Performance—History.**

- **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-minute 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-65**).



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 |

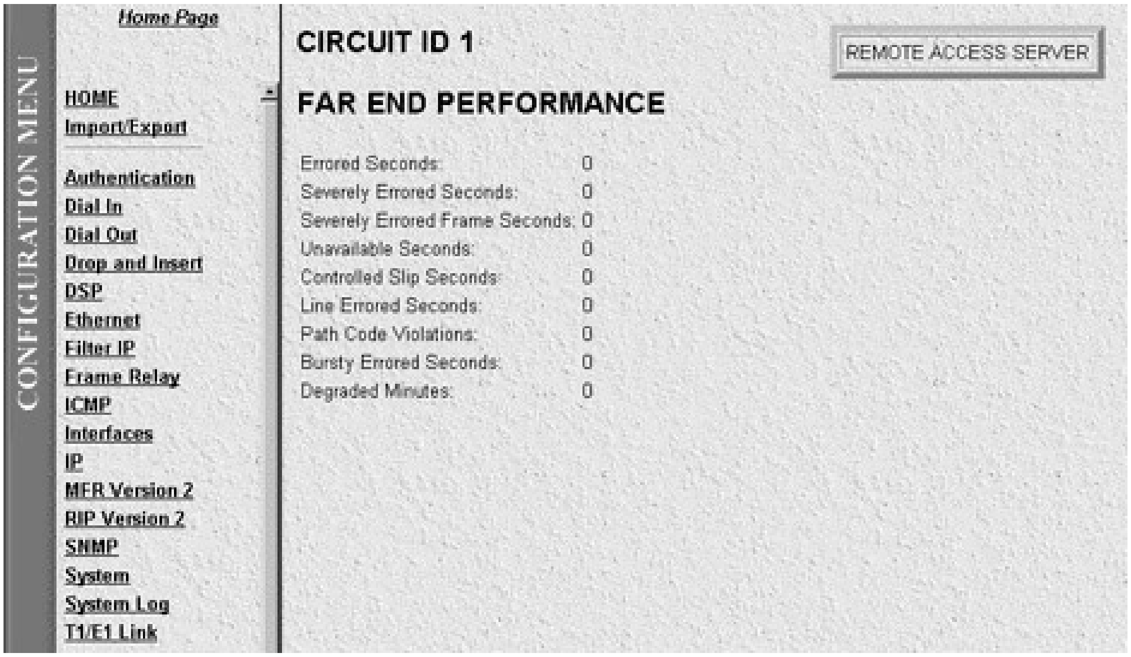
**Figure A-65. Far End Performance—History Details.**

- **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 Errored Seconds (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.

### A.18.3 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-66**).



CIRCUIT ID 1

FAR END PERFORMANCE

```
Errored Seconds:                  0
Severely Errored Seconds:         0
Severely Errored Frame Seconds:   0
Unavailable Seconds:              0
Controlled Slip Seconds:          0
Line Errored Seconds:             0
Path Code Violations:             0
Bursty Errored Seconds:           0
Degraded Minutes:                 0
```

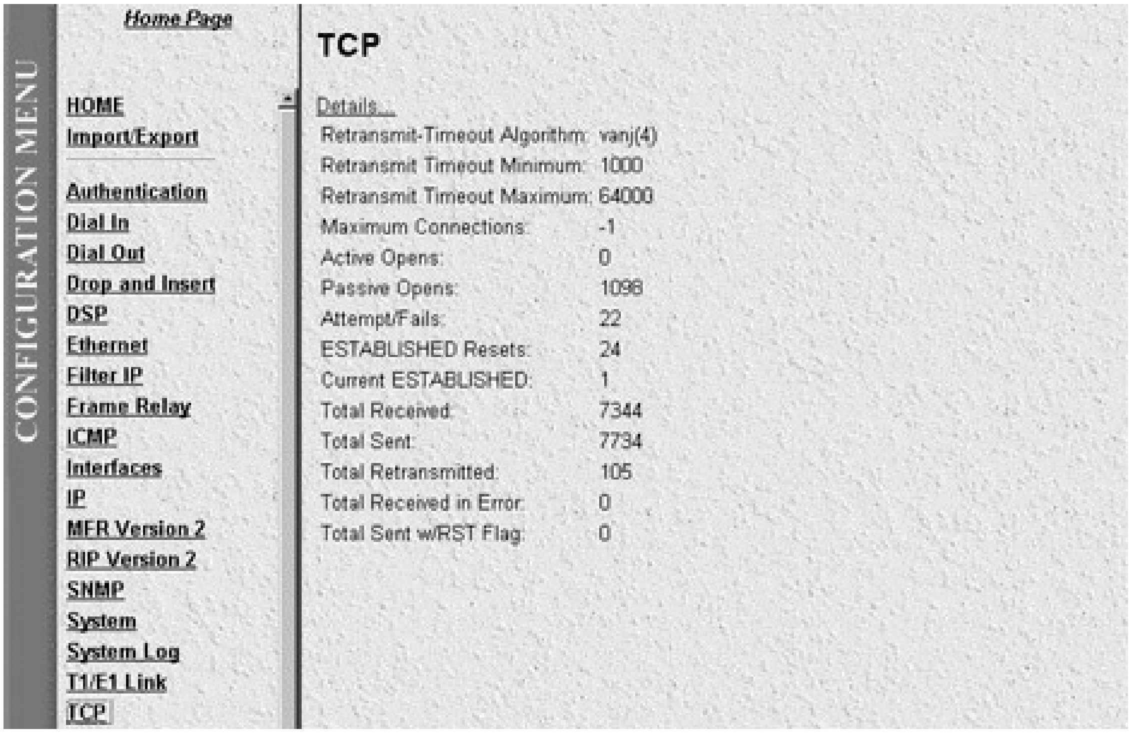
**Figure A-66. Far End Performance—Totals.**

- **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 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.

## A.20 TCP

Transmission Control Protocol (TCP) is the most widely used protocol among the TCP/IP suite. The Server 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 Server Configuration Menu to monitor TCP statistics. Following **Figure A-67** are descriptions for each object on this page.



TCP

Details...

| | |
|---|---|
| Retransmit-Timeout Algorithm: | vanj(4) |
| Retransmit Timeout Minimum: | 1000 |
| Retransmit Timeout Maximum: | 64000 |
| Maximum Connections: | -1 |
| Active Opens: | 0 |
| Passive Opens: | 1098 |
| Attempt/Fails: | 22 |
| ESTABLISHED Resets: | 24 |
| Current ESTABLISHED: | 1 |
| Total Received: | 7344 |
| Total Sent: | 7734 |
| Total Retransmitted: | 105 |
| Total Received in Error: | 0 |
| Total Sent w/RST Flag: | 0 |

**Figure A-67. TCP Main Screen.**

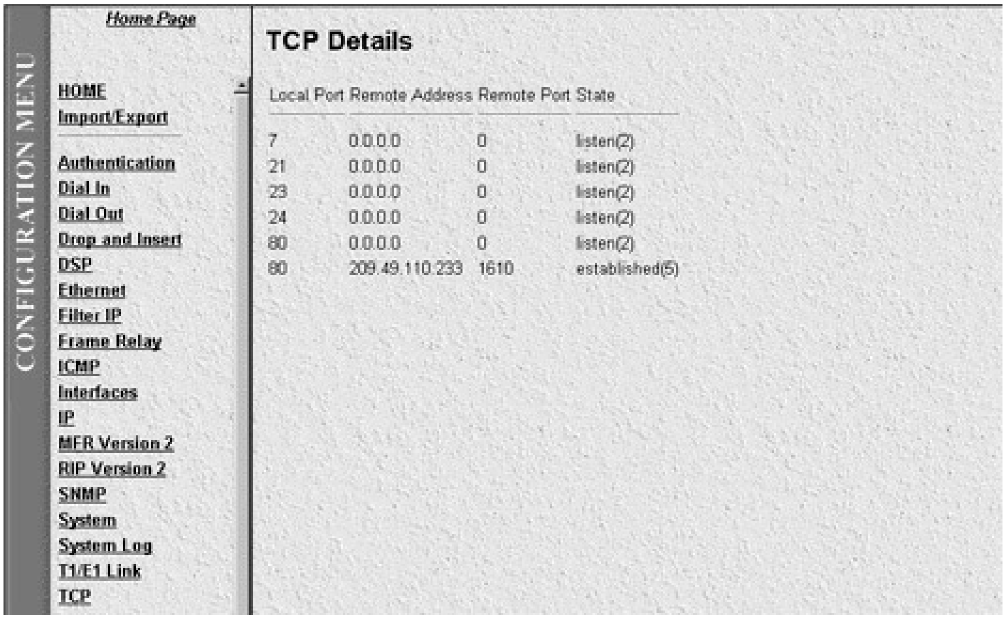
- **Retransmit-Timeout Algorithm (tcpRtoAlgorithm)**—The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
- **Retransmit-Timeout Minimum (tcpRtoMin)**—The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. 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 retransmitted. 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 (for example, bad TCP checksums).
- **Total Sent w/RST Flag (tcpOutRsts)**—The number of TCP segments sent containing the RST flag.

## A.20 TCP (Details)

From this screen you can view port details for remote and localTCP connections (see **Figure A-68**). 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.



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 | 209.49.110.233 | 1610 | established(5) |

**Figure A-68. TCP Details.**

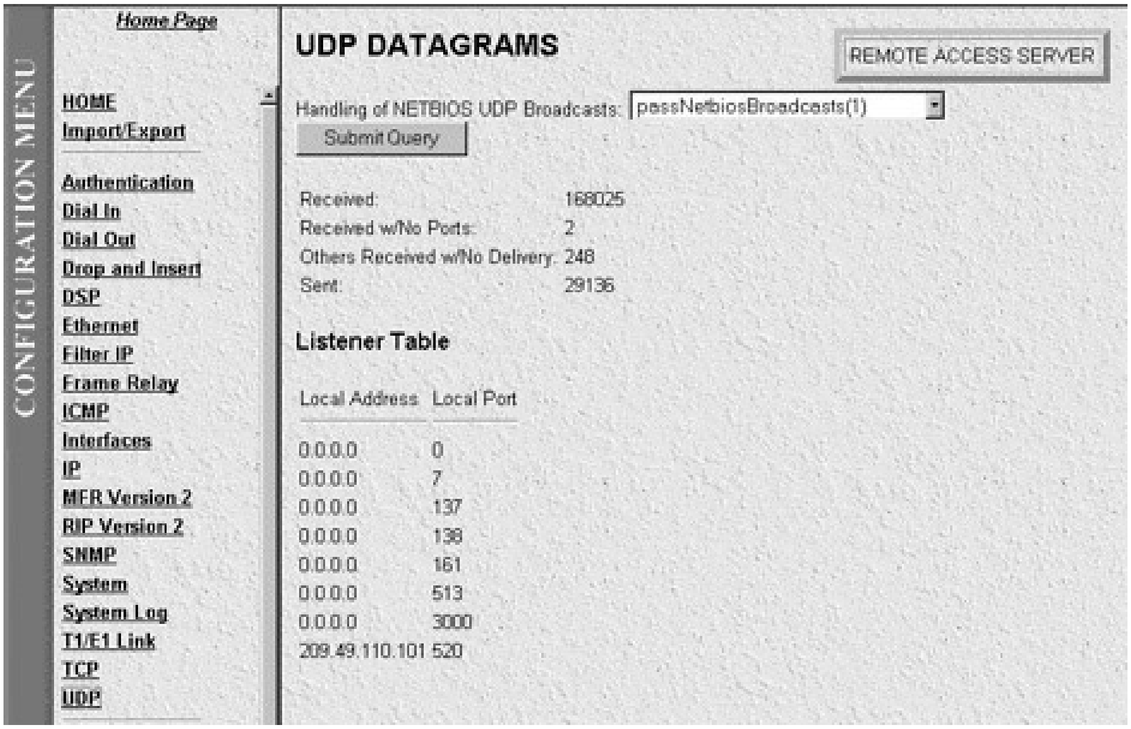
- **Local Port (tcpConnLocalPort)**—The local port number for this TCP connection.
- **Remote Address (tcpConnRemAddress)**—The remote IP address for this TCP connection.
- **Remote Port (tcpConnRemPort)**—The remote port number for this TCP connection.
- **State (tcpConnState)**—The state of this TCP 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, an 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)**

## A.21 UDP

User Datagram Protocol (UDP) is supported by the Remote Access Server. 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 Server Configuration Menu (see **Figure A-69**). Following **Figure A-69** are descriptions for each object on the screen.



UDP DATAGRAMS

Handling of NETBIOS UDP Broadcasts: passNetbiosBroadcasts(1)

| | |
|---|---|
| Received: | 168025 |
| Received w/No Ports: | 2 |
| Others Received w/No Delivery: | 248 |
| Sent: | 29136 |

Listener Table

| Local Address | Local Port |
|---|---|
| 0.0.0.0 | 0 |
| 0.0.0.0 | 7 |
| 0.0.0.0 | 137 |
| 0.0.0.0 | 138 |
| 0.0.0.0 | 161 |
| 0.0.0.0 | 513 |
| 0.0.0.0 | 3000 |
| 209.49.110.101 | 520 |

**Figure A-69. UDP Datagrams Main Screen.**

- **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.

BLACK BOX®
NETWORK SERVICES

*1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746*