perle

833AS User Guide

5500112-10

Copyrights

Mention of third party programs is for information purposes only constitutes neither and endorsement nor a recommendation. Perle Systems Limited assumes no responsibility with regard to the performance of these products.

IMPORTANT: Please review the Software License and Limited Warranty before using the software.

Important Safety Notice

This product is made to high safety standards. For safe operation all feature card slots are to be covered, and both power supplies are to be in place. Access should be gained only by authorized personnel that have been instructed about the proper procedures and precautions to follow when servicing the unit.

FCC/DOC Radio Frequency Interference Statement

Note This equipment has been tested and found to comply with the limits for a Class A Digital Device, pursuant to Part 15 of the FCC rules and to DOC Radio Interference Regulations, C.R.C., c1374. These limits are designed to provide reasonable protection against harmful interference when the equipment is used in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC/DOC compliance requires that all I/O cables used with Perle products be constructed using shielded and ferrite protected cable, metal-shelled connectors and conductive back-shells.

This equipment is approved in accordance with DIN IEC 380/VDE 0806/08.81. If this unit is installed as an office machine, the installation must conform with the above standard.

Equipment must be used with an appropriately approved power supply cordset.

Caution Changes or modifications to a Perle product not expressly approved by Perle Systems Limited may void the users authority to operate the equipment.

European Community (EC) Mark of Conformity

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Perle cannot accept responsibility for any failure to satisfy the protection requirements resulting from non-recommended modification of the product.

DEPARTMENT OF COMMUNICATIONS (DOC) REQUIREMENTS.

“NOTICE: The Canadian DOC label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user’s satisfaction.”

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

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

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

If you experience trouble with this equipment, please contact the Perle Technical Assistance Center at the following address for information about obtaining service;

Perle Systems Limited
60 Renfrew Drive
Markham, Ontario
L3R 0E1
1-800-33 PERLE

All repairs should only be performed by Perle Systems Limited or an authorized agent of Perle.

FEDERAL COMMUNICATIONS COMMISSION (FCC) REQUIREMENTS.

This product complies with Part 68 of the FCC rules. If requested, you must provide the telephone company with the FCC registration number, make and the model number of this device. This information can be found on the product label affixed to the back of the unit.

This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is part 68 compliant.

This equipment is not intended to be used on public coin phone service or be connected to party line service.

If this equipment malfunctions, it may cause harm to the telephone network. In such an event, the telephone company may request that you disconnect the equipment from the network until the problem is corrected. The may also notify you in advance that temporary discontinuance of service may be required. If advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modification to maintain uninterrupted service.

If you experienced trouble with this equipment, please contact the Perle Technical Assistance Center at the following address for information about obtaining service;

Perle Systems Limited

60 Renfrew Drive

Markham, Ontario

L3R 0E1

1-800-33 PERLE

All repairs should only be performed by Perle Systems Limited or an authorized agent of Perle.

When ordering service from the telephone company, you may need to provide the following information;

Port:	T1, ISDN 1.544 Mbps
Facility Interface Codes (FIC):	04DU9-BN 04DU9-DN 04DU9-1KN 04DU9-1SN 04DU9-1ZN
Service Order Code (SOC):	9.0N
USOC Jack:	RJ48C

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

For work to be performed in the certified territory of ____

(Telco's Name)

State of: ______________________

Country of: ______________________

I, ____, of ________________________________

(Name of Authorized Representative) (Business Name)

____, ______________________________

(Business Address) (Telephone Number)

being duly sworn, state:

I have responsibililty for the operation and maintenance of the terminal equipment to be connected to 1.544 Mbps digital services. The terminal equipment to be connected complies with part 68 of the commissions rules except for the encoded analog content and billing protection specifications. With respect to encoded analog content and billing protection:

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

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

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

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

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

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

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

( ) d. In lieu of the proceeding training requirements, the operator(s) maintainer(s) is (are) under the control of a supervisor trained in accordance with _______ above.

I agree to provide ____________________________________ with proper documentation to
(Telco's Name)
demonstrate compliance with the information as provided in the proceeding paragraph, if so requested.

_____________________________________ (Signature)

_____________________________________ (Title)

_____________________________________ (Date)

Subscribed and sworn to before me this ______ day of _________________, 19 ____.

____
Notary Public

My commission expires: ____________________

About this Book

The Perle 833AS User Guide is intended for users ranging from novice to experienced LAN Administrators. It is designed to help you install, configure and manage the 833AS.

Users

Novice

Novice Users can rely on the Guide to provide them with simple and easy to understand steps. The extensive indexing, cross-referencing, illustrations and full glossary are not only intended to help set up the 833AS, but also realize its full potential. Take advantage of the Quick Install Chapter to get an overview of what's ahead. Make sure you familiarize yourself with the Icons used to convey important information.

Experienced

To meet the different needs of more experienced users, the Guide provides a Quick Install Chapter. Brief and to the point, it gives a complete overview of the installation and configuration process.

Once you have successfully installed the 833AS, turn to Section 3: Management, to learn about the management features. If you still have any questions, turn to our extensive index for help.

How to Use This Guide

This Guide is divided into three sections: Installation, Configuration, and Management. Each section has a number of chapters that highlight a unique aspect of that section. The order of the sections and the chapters within comprise a series of steps that will lead to the successful installation and operation of the Perle 833AS.

Assumptions

This Guide assumes that Users have at least a basic knowledge of LAN Theory and terminology. It also presumes that some users will have extensive experience and may wish to customize their configuration. To meet this need, we have included a comprehensive discussion of features and parameters that can be customized along with simple instructions on how perform them.

While the Guide assumes LAN familiarity, we also assume that first time users want simple explanations that provide context. Further, we believe that our new users want to understand as much as they can, so we have provided a glossary to explain any new terminology.

Icons

You will find Icons throughout this guide. Use them to quickly locate useful and important information.

➲ *Procedure*: Indicates a series of steps that you need to perform in order to set up or configure the 833AS

⚠ *Warning*: Indicates vital information you need to know in order to protect your hardware or software.

ℹ *Information*: Provides important information that will make use of the 833AS easier.

What’s in the Guide

Installation

Chapter 1: *Quick Installation Overview:* Although intended for the experienced user, this chapter can assist the novice by previewing the steps ahead. Provides an overview of installation and configuration.

Chapter 2: *Site Preparation:* This chapter provides a complete description of the Electrical, Environmental and Cable Requirements of the 833AS.

Chapter 3: *Setting Up and Installing the Perle 833AS:* Familiarize yourself with the unit’s physical appearance as well as the basic functions. Make the LAN connections and verify its correct operation.

Chapter 4:Using the Perle 833AS Manager: This chapters describes the requirements, function and features of the Manager Software.

Configuration

Chapter 5: *Configuring the Perle 833AS:* Learn about Dial-In and Dial-Out access and how configuration can help you fully exploit the potential of the 833AS.

Chapter 6: *Configuring the Feature Cards:* Describes the unique characteristics and requirements of each Feature Card as well as card configuration.

Chapter 7: *Configuring the Protocols:* Learn about the various communication protocols supported and how to use them.

Chapter 8: *Configuring the User Database:* Learn how to custom define the user to your system. Describes the various ways of identifying users and limiting their access.

Chapter 9: *Configuring the Server:* Describes the parameters not related to *Feature Cards*, protocols or users. Provides information about Security, Groups, Servers, and more.

Management

Chapter 10: *Managing the Perle 833AS:* Intended for experienced users. Learn about Manager Statistics, Front Panel, and the Event Log. Also learn about upgrading your software.

Appendix 1: *Menu Descriptions*: Gives the user a quick overview of the Front Panel Menu Descriptions in table format.

Appendix 2: *AT Command Set:* Describes the commands that the Modem will respond to as well the parameters applicable to each.

Appendix 3: Specifications: A detailed description of the physical parameters of the 833AS as well as its performance capabilities.

Appendix 4: RADIUS Server Attributes

Glossary: This section provides a brief explanation of terms found in this Guide. While the explanations are not exhaustive, they are intended to provide context to their usage in the Guide.

Contents

Section 2: Configuration.......... 71

Chapter 5: Configuring the Perle 833AS..........73

Chapter 6: Configuring the Feature Cards......85

Chapter 7: Configuring the Protocols............111

Chapter 8: Configuring the User Database...153

Chapter 9: Configuring the Server 173

Section 3: Management........................... 207

Chapter 10: Managing the Perle 833AS 209

Appendix 1: Menu Descriptions and Maps...235

Appendix 2: AT Command Set 251

Appendix 3: Specifications 283

Appendix 4: RADIUS Server Attributes..........295

Introduction

The Perle 833AS...Reliability and Flexibility

About the Features of the 833AS

Dial- In Access

The 833AS lets Remote Users access the LAN (Local Area Network) via the telephone network as if they are directly attached to it. Remote Users can then access file servers, Email, Mainframes, application servers, or any other server on your LAN. It can be teamed with a remote control package such as PC Anywhere or Carbon Copy to allow a user to use a locally attached PC remotely. It can even act as a Dial-In gateway to another network, such as the Internet.

Dial- Out Access

With Perle Dial-Out Client software, LAN attached PCs can use the PerleDSP Modem and lines as Dial-Out modems. To the PC application, the PerleDSP Modem and line attached to the 833AS look like a modem connected to the PC COM port. Most PC applications that require a modem are supported. With appropriate software, users can connect to a BBS, Internet provider, or any other service accessible by the telephone network. When used with Fax software such as WinFax Pro, users can send faxes from their PC.

T1/E1/PRI Support

Calls are brought into the 833AS by a T1/PRI (Primary Rate Interface) or E1/PRI line. North America and Japan use the T1 line while the E1 is used in Europe. This type of connection supports up to 30 simultaneous phone calls on a single line. Instead of many individual RJ11 phone lines, one or two physical connections can be used - reducing the number of cables, simplifying management, and reducing the cost in many cases.

ISDN PRI (Integrated Service Digital Network) is supported for both T1 and E1 to provide a clean, digital high speed link for remote access from conventional modems, ISDN Basic Rate Interface (BRI) cards or Terminal Adapters. T1 with Robbed Bit Signaling is supported for locations where this service is less expensive than ISDN. Depending on the support of your Telephone Company, you can even split a single T1 into Robbed Bit and ISDN, letting you supply both services to your users in the most cost effective manner. E1 with Channel Associated Signalling (R2 CAS) is available for the ITU and China variants.

Multiprotocol Support

There is direct support for IP (Internet Protocol), IPX (Internet Packet eXchange), Netbeui, and AppleTalk routing protocols in their native form. They do not require workarounds and special settings (such as Netbeui over IP) to be used. Logical Link Control (LLC) bridging is supported for use in IBM Mainframe and Midrange environments.

Multiple Dial In Client Support

Included with the 833AS are the Perle Remote Dial-In Clients for DOS and Windows 3.1. Microsoft Dial Up Networking Clients are supported for Windows 95, 98 and NT. For the Macintosh user, the 833AS is compatible with Apple Remote Access.

In addition to these standard clients, many other third party clients can be used with the 833AS.

Advanced User Security

The 833AS supports access protection by individual User ID and passwords. Optionally, an external RADIUS or Novell server can be used for centralized access management. Token authentication access systems such as Security Dynamics SecurID and Axent can work with the 833AS to meet high security requirements.

The internal database of the 833AS supports up to 2000 users, each with their own password.

Fixed Callback and Roaming Callback are supported to meet both security requirements and toll management.

Grouping

The 833AS's powerful grouping functions lets you:

- Allocate connections for specific departments or have a connection always available for the MIS (Management Information System) department.
- Set up a group of modems that are compatible with older Dial-In modems that require special settings.
- Split connections into Dial-In only and Dial-Out only lines.
- Set one group of users with a maximum Dial-In time of one hour, and another with unlimited access time.

LAN-to-LAN

The 833AS LAN-to-LAN feature lets you establish IP/IPX connections to remote Routers. These connections can be initialted by either the 833AS or the remote Router. The Virtual Connection feature can be used to provide cost effective connections between two LANs.

Expandable System

You can size the hardware of the 833AS to meet the needs of your business. The 833AS supports up to 4 line cards (T1/PRI or E1/PRI) or 2 dual cards (dual T1/PRI or E1/PRI) for up to 120 simultaneous phone calls. PerleDSP modem cards are available in fixed 12 or 18 modem version or with plug-in modem modules. The number of modems on a plug-in card can be 12, 18, 24, or 30. The maximum number of modems in a unit is 120.

Flexible Modem Support

The 833AS modems support all the standard modem modulations, including 56Kflex and V. 90. Class 2 Fax support allows the use of the modems for Fax Dial-Out when used with Fax Software such as WinFax Pro. The modem initialization string can be customized for each modem to meet special requirements.

Manager

The 833AS Manager is a Windows based application used to configure and manage the 833AS. You can connect to the 833AS by a LAN or Dial In connection, using either IP or IPX. You do not require a serial connected PC to set up or manage the 833AS. The configuration process is entirely GUI based - no editing of complex configuration files is needed. The Manager also displays the operational status of the 833AS. Key statistics are provided for all interfaces to enable monitoring of normal operation and assist in network troubleshooting if necessary.

High Performance Architecture

The 833AS was designed for high performance, even when handling the maximum number of incoming calls. At its heart is a high speed PowerPC RISC (Reduced Instruction Set Computer) CPU, which is optimized for communications. The T1/PRI, E1/PRI and PerleDSP Modem Feature Cards each contain their own PowerPC processors. They improve performance by offloading the character oriented processing from the main engine.

There are two independent data busses within the 833AS. The PCI (Peripheral Component Interconnect) data bus transfers data at 132 Mbytes per second. All Feature Cards operate as PCI bus masters, freeing the System card from data transfers and ensuring that the bus is used to its maximum potential. Data transfer between the T1/PRI, E1/PRI cards and the PerleDSP Modem cards is done via a separate telephony bus.

High Reliability Design

There are no moving storage devices such as floppy or hard drives in the 833AS. All program storage is on Flash ROMs (Read Only Memory). Instead of using PC type connector technology, cards are interconnected via high reliability CompactPCI industrial connectors.

The 833AS is fitted with a dual redundant power supply. If a power supply problem occurs in one supply, the other supply will maintain the power.

Section 1: Installation

Chapter 1: Quick Installation Overview

About Installation

This chapter provides an overview of how to install, setup, and configure the 833AS.

These are the major steps:

- Preparing the Site for the 833AS
- Setting up and Installing the 833AS Hardware
- Setting up the 833AS LAN Connection
- Configuring the 833AS
- Attaching the 833AS to the Telephone Network
- Verifying Correct Operation of the 833AS

Preparing the Site

For detailed instructions, see “Chapter 2: Site Preparation” .

Before installing, prepare the site for the 833AS by:

- Arranging the installation of telephone services by the carrier.
- Locating the 833AS in an area where:
  - There is sufficient clearances in the front and rear of the unit for ventilation.
  - Power cords and cables are out of traffic areas.
  - The Front Panel is easily visible and accessible.
- Identifying the Windows 3.1/95/98/NT PC that will be used for installation of the Manager. This PC must be attached to the LAN.
- Extending all telephony and LAN wiring to the location where the 833AS will be installed.

Setting up and Installing the 833AS Hardware

For detailed instructions, see "Chapter 3: Setting Up and Installing" on page 25.

To Install the 833AS Hardware:

1. Unpack the 833AS.
2. Set up the 833AS. See "Unpacking the 833AS" on page 26.
3. Set the Voltage Selector Switch. See "Voltage Selector Switch" on page 30.
4. If the unit is to be rack mounted, install the Rack Mount Kit and place the unit in the rack.
5. Connect and plug in the power cords.

It is not recommended that you attach the LAN or the telephone network wiring at this time. If the 833AS is powered up with a configuration that does not match the carriers' requirements, errors could be generated at the Central Office. Some carriers will disable or disconnect the service if excessive errors are encountered. Also, if you are in a Token Ring LAN environment and the speed setting is incorrect, beaconing could occur, disrupting the service of others on the LAN.

6. Power on the 833AS.

Setting up the LAN Connection

For more details, see "Set up the basic parameters" on page 41.

➲ To Set up the 833AS LAN connection:

1. Set the basic configuration from the Front Panel.

   Some parameters may have to be set from the Front Panel to allow the Manager to connect to the 833AS. Depending on the LAN type and network protocol used by the Manager (IP or IPX), this step may not be required. See "Set up the basic parameters" on page 41.

2. Power off the 833AS.
3. Attach the LAN cable to the appropriate connector, based on your LAN type and media type. See "Attaching the LAN Cable" on page 45.
4. Power on the 833AS.
5. Verify that the 833AS can see LAN network traffic. See "Verifying that the 833AS can see LAN Traffic" on page 25.

Configuring the 833AS

For detailed instructions, refer to Section 2: Configuration

You configure the 833AS with the 833AS Manager. The Manager Software must be installed on a Windows 3.1/95/98/NT PC that is LAN attached. The PC must also have IP or IPX network software installed and set up. This network software is built in to Windows 95, 98 and NT. Perle includes IP software on the installation disks for Windows 3.1 environments.

Attaching to the Telephone Network

See “Attaching to the Telephone Network” on page 51.

Now that the 833AS is configured, the telephone cables can be attached to the unit. Depending on which telephone network is being used, the 833AS may be either directly attached (DSX-1 mode) or require a CSU (Channel Service Unit).

To attach the telephone line:

1. Power down the 833AS.
2. Attach the cable from the phone network or CSU to the appropriate interface on the 833AS.
3. Power up the 833AS.
4. Verify that the 833AS can operate correctly with the telephone line.

Verifying Correct Operation

For details, see “Verifying Connection” on page 47.

At this point, installation is complete. Now you can verify that remote users can dial into the 833AS and access the services. Also, you can install Perle Dial-Out software on LAN PCs and verify that the Dial-Out is functioning correctly.

If you are using Perle Remote Client software, please see the *Perle Remote User’s Guide* for details on software installation and operation.

If you are using Perle Dial-Out software, please see the *Perle Dial-Out User’s Guide* for details on software installation and operation.

Chapter 2: Site Preparation

About Site Preparation

In this chapter you will read about:

- Site Preparation Overview
- Electrical Requirements
- Environmental Requirements
- Cabling Planning and Requirements
- Telephony Cabling

Site Preparation Overview

The following is a checklist of recommended tasks that should be completed before installing the 833AS. Some may not apply to your installation, or you may wish to add new items.

Identify and contact the following individuals:

✎__ Network supplier.

✎__ Remote Installation Planner.

✎__ Cabling supplier.

then,

✎__ Analyze the site's electrical requirements. See “Electrical Requirements” on page 12.

✎__ Analyze the site's environmental requirements. See “Environmental Requirements” on page 13.

✎__ Determine the future location of the 833AS that will meet the placement needs of the unit. See “Placement” on page 13.

Determine your cabling needs for:

✎__ LAN cabling. See “LAN Cabling” on page 14.

✎__ Telephone network cabling. See “Telephony Cabling” on page 20.

then,

✎__ Order the Telephone network facilities. See “T1 Telephony Planning” on page 21 and “E1 Telephony Planning” on page 23.

✎__ Order the CSU, if required.

✎__ Order the required cabling. See “Cable Planning and Requirements” on page 14.

✎__ Ensure that the electrical outlets have been installed and are properly grounded.

Electrical Requirements

Electrical Specification	Voltage Selector Switch	
	115	230
Voltage	100 - 125 VAC	200 - 240 VAC
Phases	1	1
Current	2 A (Maximum)	1 A (Maximum)
Power	250 W (Maximum)	250 W (Maximum)

The 833AS should not share electrical circuits with equipment that can cause electrical noise and interference.

For the Redundant power supply, two separate outlets that meet the above specifications are required. Each outlet must be capable of carrying the full electrical load.

For your safety, you must connect equipment only to a properly wired and grounded outlet. An improperly wired outlet can place hazardous voltage on the accessible metal parts of the unit.

It is strongly recommended that you use an Uninterruptable Power Supply (UPS) to power your CSU (Channel Service Unit). This will prevent setting Central Site alarms in the event of power fluctuations or outages. If you are using the built in

CSU feature of the T1 card, it is recommended that you use a UPS to power the 833AS.

Environmental Requirements

The 833AS is designed to operate in a normal office environment. The following condition must be met and maintained.

Condition	Temperature Range	Relative Humidity
Operating	10° - 30° C 50° - 80° F	20% - 80%

Placement

The 833AS is designed for either 19" rack mount or table top placement.

Locate the 833AS in an area where:

- Power cords and cables are out of traffic areas.
- The front panel is accessible.

⚠ *Sufficient clearances must be maintained in front of and behind the unit to allow proper air flow to the internal fans.*

For rack mounting, the 833AS requires 5 rack mount spaces (i.e. the 833AS height is 5U). It is not necessary to leave empty spaces above or below the unit in the rack.

⚠ *Mounting of the equipment in the rack shall be such that a hazardous condition does not occur due to uneven mechanical loading. Heavier equipment should be located at the bottom of the rack, and the rack should be loaded such that the bottom slots are used first (fill from the bottom up).*

Circuits supplying power to the rack must be sufficient to safely supply power to all equipment within the rack based on the equipment nameplate rating. Power distribution to all equipment in the rack must have proper grounding. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. power strips).

Cable Planning and Requirements

LAN Cabling

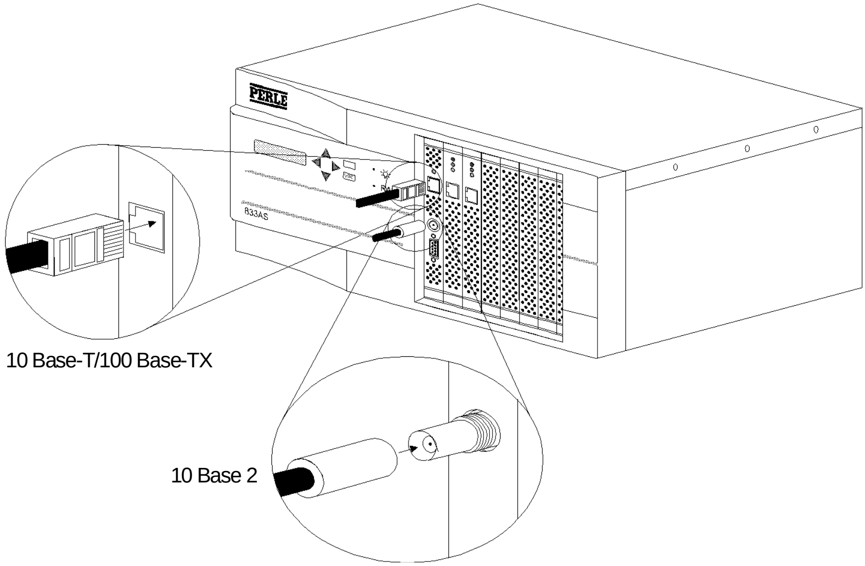
The 833AS has a 10/100 Mbps Ethernet LAN interface built in. You can optionally add a Token Ring Feature card for support of 4/16 Mbps Token Ring LAN. Only one LAN interface is supported at a time – if you have a Token Ring Feature card installed, the Ethernet interface is disabled. Cabling required will be dependent on these factors:

- The type of LAN.
- The type of hub (Ethernet) or Media Access Unit (Token Ring).
- The type of cabling used in the existing LAN network.

Ethernet

The Ethernet interface is located on the System card. The following physical interfaces are available:

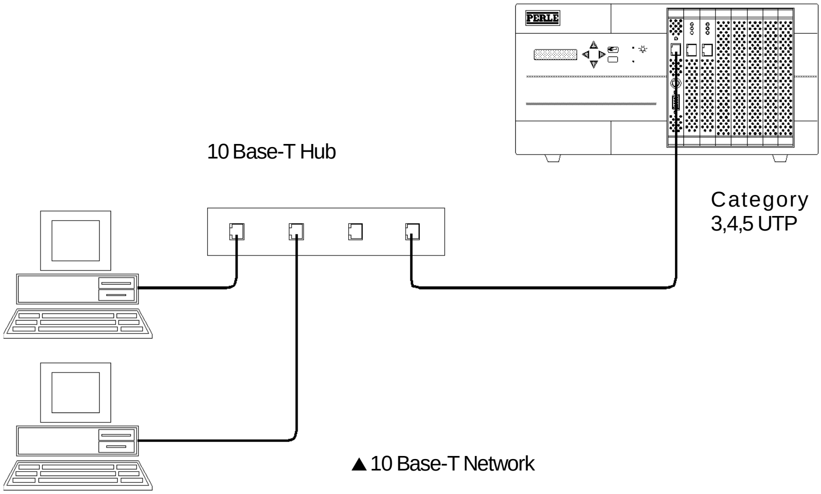
- 10Base -T/100Base-TX - uses an RJ-45 connector
- 10Base2 - uses a BNC connector



▲ Ethernet/LAN Cable Connection

10Base-T: (Note: Emission standards require ferrite protected cables).

- Uses 22 to 26 AWG unshielded twisted pair (UTP) cable.
- Terminated with RJ-45 plugs.
- Cables are straight wired – pin 1 of one end of the cable is wired to pin 1 on the other end.
- Category 3, 4 and 5 UTP cable is acceptable.
- For best results, Category 4 and 5 cable is recommended.
- Cables are attached to a 10Base-T hub in a star configuration.
- Maximum length from 833AS to hub is 100m (328 ft.).



▲ 10 Base-T Network

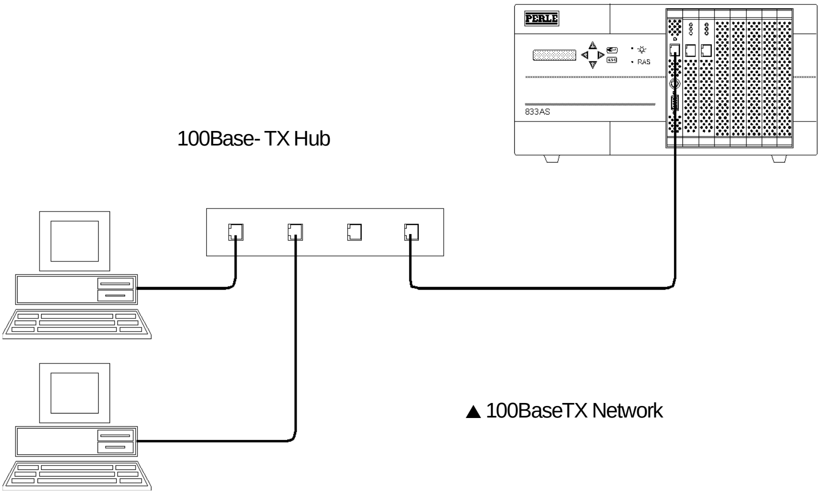
100Base-TX: (Note: Emission standards require ferrite protected cables).

- Uses Category 5 unshielded twisted pair (UTP) or Type 1 shielded twisted pair (STP) cable.
- Terminated with RJ-45 plugs.
- Cables are straight wired – pin 1 of one end of the cable is wired to pin 1 on the other end.
- If you are using STP cable, make sure that *all* cables and connection points are shielded.
- Cables are attached to a 100Base-TX hub in a star configuration.
- Maximum length from 833AS to hub is 100m (328 ft.).

There are other cabling types that are available for Ethernet:

- 10Base5 (AUI).
- 100Base-T4.
- 100Base-FX.

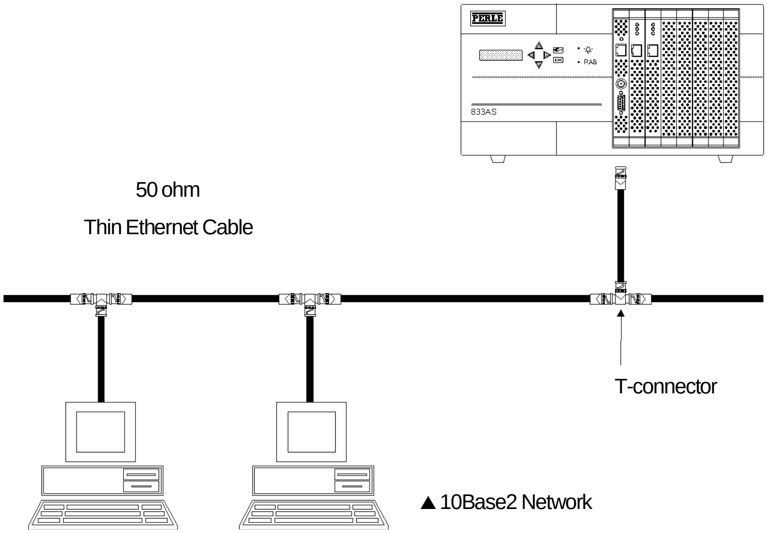
If you are using any of these types of cabling, you will require an adapter. See your network equipment supplier to obtain this adapter.



▲ 100BaseTX Network

10Base2: (Note: Emission standards require ferrite protected cables).

- Also known as Thin Ethernet.
- Uses 50 ohm Thin Ethernet coaxial cable.
- Terminated with BNC connectors.
- Devices are chained to each other using "T" connectors. All devices chained together comprise a segment.
- "T" connectors must be plugged directly into the Ethernet device.
- The maximum length of one segment is 185m (607 ft.).
- No more than 30 connections are allowed in one segment.
- The first and last device on a segment must be terminated on one side of their "T" connectors with a 50 ohm resistor.
- The minimum distance between "T" connectors is .5m (1.6 ft.).

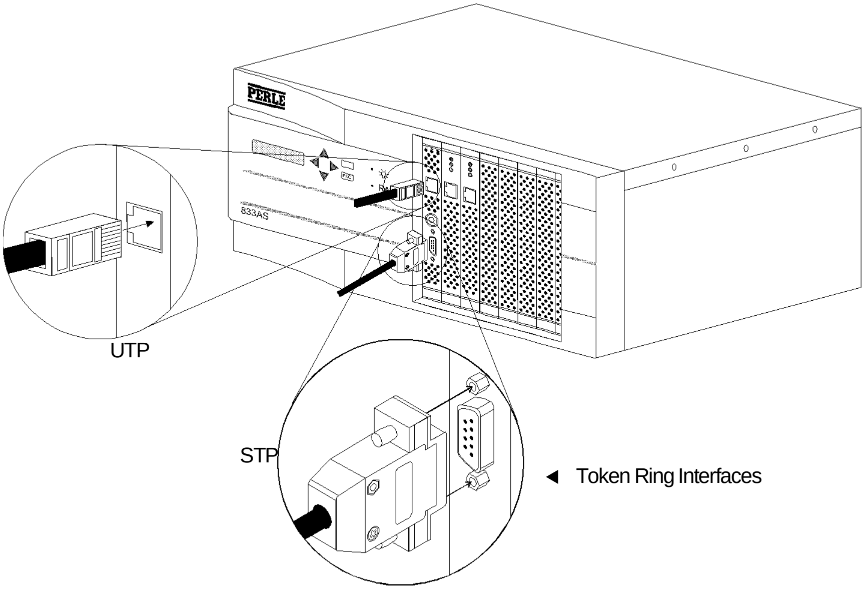


▲ 10Base2 Network

Token Ring

The Token Ring feature card has the following physical interfaces:

- STP (Shielded Twisted Pair).
- UTP (Unshielded Twisted Pair).

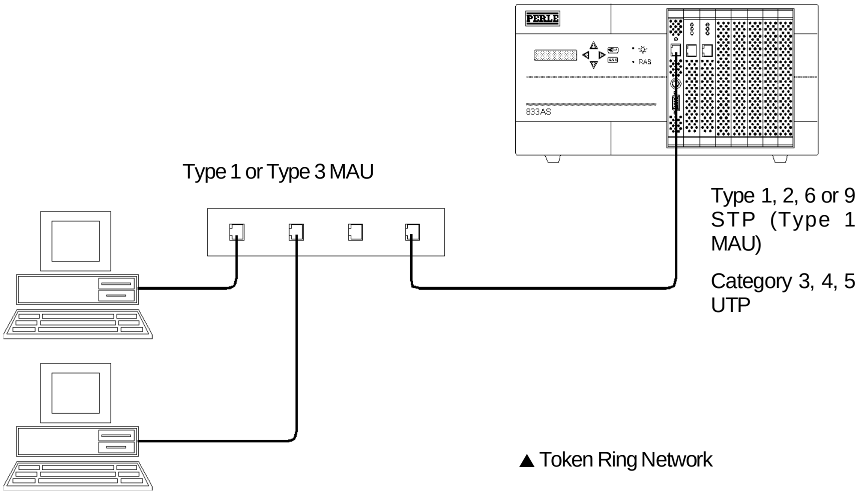


STP

- Uses STP wiring, Types 1, 2, 6, and 9.
- Terminated with IBM style universal data connectors.
- Cables are attached to a Media Access Unit (MAU) in a star configuration.

UTP

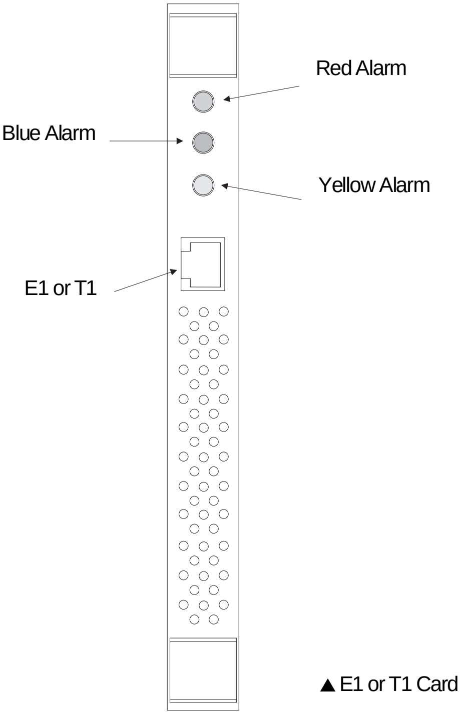
- Uses UTP wiring, Category 3, 4 or 5.
- Terminated with RJ-45 plugs.
- Cables are attached to a MAU in a star configuration.



▲ Token Ring Network

Telephony Cabling

The connection to the T1 or E1 network is made via an RJ-48 connector. Standard UTP telephone cable is used for the connection.



▲ E1 or T1 Card

Network equipment attaches to a T1/E1 line via a CSU. This unit provides line coding and conditioning functions as well as performing line diagnostics under the control of the carrier. The T1/PRI feature card has a CSU built in. However, an external CSU can be used by operating the card in DSX-1 mode.

An external CSU isolates the line from the 833AS and keeps the line from causing Central Site alarms to be activated if the 833AS is powered off. In some countries that use T1 and all countries using E1, an external CSU is mandatory. In many cases, the CSU is provided by the carrier.

If you are using the T1 built in CSU, you should first contact your carrier for approval before installation. Otherwise, the T1/PRI service could be temporarily discontinued if Central Site alarms occur.

The carrier brings the T1/E1 service to a "Demarcation Point" (also known as Demark or Demarc), and assumes responsibility for wiring and equipment up to the Demarc. You are responsible for the wiring from the Demarc to the 833AS. Depending on the carrier, the Demarc may either be brought to the 833AS or it may terminate some considerable distance from the unit. You will need to work with the carrier in advance to determine where the T1/E1 service will be brought, and if necessary, arrange for the wiring from the Demarc to the 833AS.

T1 Telephony Planning

When you order your T1 line, you will need to specify certain options. This process of specifying these options is referred to as "provisioning" the line.

Overview

A T1 line is a digital transmission link with a capacity of 1.544 Mbps. By using Time Division Multiplexing the line is split into 24 channels with one call occupying one channel. From the user perspective, each channel looks like an individual phone line with its own phone number.

The T1 line can operate as a channelized T1 line, or as an Primary Rate Interface (PRI) ISDN line. A channelized T1 line treats all calls as analog voice calls and modems are used to transfer digital data. A PRI ISDN line treats all calls as digital calls so either ISDN digital calls or ISDN voice calls can be handled. If an ISDN voice call is used, a modem is used to transfer the digital data.

When a call is made on one of the T1 channels, it is signaled on the T1 line. This signaling emulates the dial and answer sequence of a standard telephone. There are a number of different signaling schemes in use and you configure the 833AS to match the scheme that is used by the carrier. For a PRI ISDN connection, one T1 channel is dedicated solely for signaling.

Provisioning

Provisioning a T1 connection for the 833AS will require the determination of the following types of parameters:

Line parameters

- Coding (AMI, B8ZS, or JBZS)
- Framing (D4 or ESF)
- Facilities Data Link (ANSI, AT&T or none)
- Line Build Out

Mode of operation

- T1 (robbed bit signaling), PRI (ISDN) or Mixed T1/PRI.

Signaling Type

- If T1, type of robbed bit signaling used.
- Does not apply to ISDN.

Switch Type, if PRI

- US NI-2
- AT&T 4ESS
- AT&T 5ESS
- Northern Telecom DMS 100
- Northern Telecom DMS 250
- Japan INSNet 1500

Channel assignment

- Unused channels, if any.
- If mixed T1/PRI, which channels use T1 signaling, and which channels use ISDN signaling.

These parameters will be dependent on the carrier's requirements. Your carrier will usually determine these values, and you will enter these values in the 833AS T1 configuration. For more details, see “T1 Parameters” on page 96.

A typical line provisioning for North American T1 would include:

- Coding - B8ZS
- Framing - ESF
- FDL mode - None (with external CSU)
- T1 Signaling - E & M Wink Start
- All channels used.

A typical line provisioning for North American PRI would include:

- Coding - B8ZS
- Framing - ESF
- FDL mode - None (with external CSU)
- Switch Type - Northern Telecom DMS-100
- All channels used.

E1 Telephony Planning

When you order your E1 line, you will need to specify certain options. This process of specifying these options is referred to as "provisioning" the line.

Overview

An E1 telephone line supports up to 30 telephone calls on a single physical line. By using Time Division Multiplexing the line is split into channels with one call occupying one channel. From the user perspective, each call carrying channel (known as the bearer channel) looks like an individual phone line with its own phone number. The E1/PRI line can operate as an ISDN Primary Rate Interface or as an R2 Channel Associated Signalling (CAS) Interface.

Provisioning

Provisioning an E1 connection for the 833AS will require the determination of the following types of parameters:

Line Parameters

- Coding (HDB3)
- Framing (CRC4 or no CRC4)
- Line Build Out

ISDN Parameters

- Switch Type

Channel Assignment

- Unused channels, if any.

These parameters will be dependent on the carrier's requirements. Your carrier will usually determine these values, and then you set these values in the 833AS E1 configuration. For more details on these parameters, see “E1 Parameters” on page 104.

A typical line provisioning for E1/PRI would include:

- Framing - CRC4
- Switch Type - EuroISDN ETSI NET5
- All channels used.

Chapter 3: Setting Up and Installing

About Setting Up and Installing

In this chapter you will read about:

- Unpacking the 833AS
- Familiarize Yourself with the Unit
- Assembling the Hardware
- Factory Default Mode
- Setting up the 833AS LAN connection
- Attaching the LAN Cable
- Verifying that the 833AS can see LAN Traffic
- Configuring the 833AS

What's in the box?

The 833AS shipping carton contains the following:

- 833AS
- Rack Mount Kit
- Power Cord
- Documentation Packet
- Diskette Packets

Rack Mount Kit

The Rack Mount Kit allows you to mount the 833AS into a standard 19" equipment rack.

Power Cords

The appropriate power cords for your location are provided.

Documentation Package

The Documentation Package contains the following documents:

- Perle 833AS User Guide
- Perle Remote User’s Guide
- Perle Dial-Out User’s Guide

Software Package

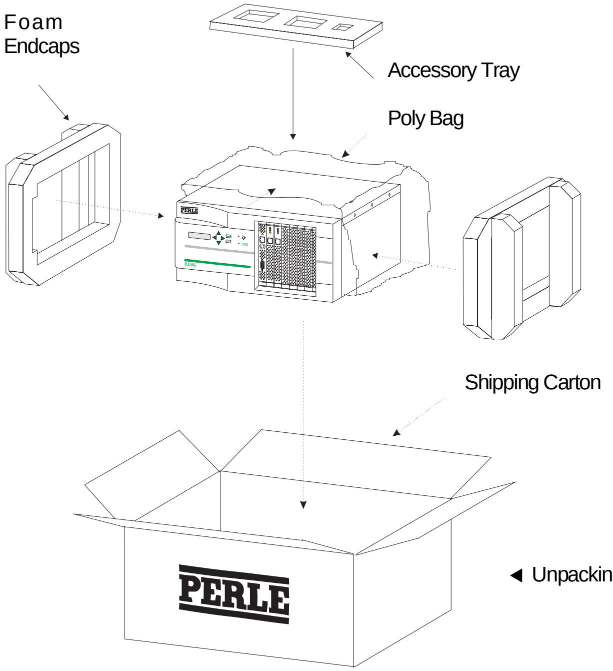
The Software Package contains the following:

- 833AS Manager Diskette Set
- Perle Remote Client (CD-ROM)
- Perle Dial-Out Client Diskette (CD-ROM)

Unpacking the 833AS

To Unpack the 833AS:

➲ **1.** Open the shipping carton.



◀ Unpacking the 833AS

2. Remove Accessory Tray containing the Power Cords.

3. Remove the Documentation and Diskette packets from the side cavity between the unit and outer carton.

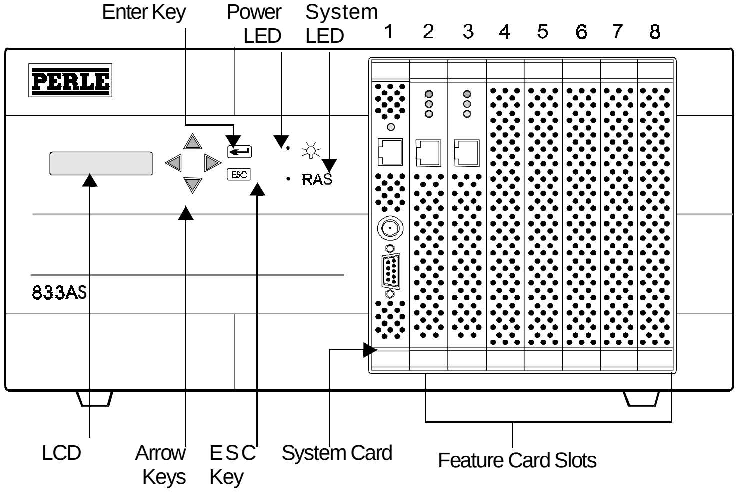
4. Lift the 833AS out of the shipping carton.

5. Remove the packing material.

Familiarize Yourself with the Unit

833AS Views

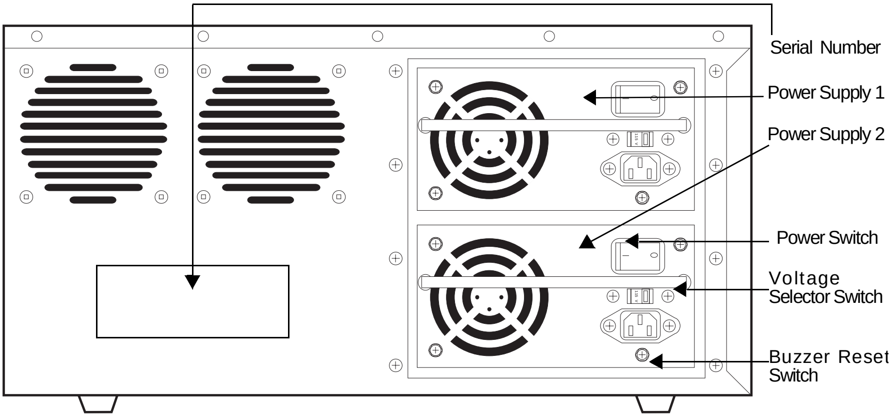
The diagrams below show the major hardware components of the 833AS.



▲ Front Panel

Note: We've displayed slot numbers in this diagram to help you identify slot positions on your 833AS.

Slots 2 thorough 8 are occupied by the Feature Cards you ordered and may be different than those shown in this diagram.



▲ Back Panel with Dual Redundant Power Supply

833AS Chassis Description

Operator Panel LCD

The operator panel has a 2 line by 16 character LCD that displays status for the 833AS.

Operator Panel Keypad

Use the keypad to navigate the LCD menus and enter data. The keys are:

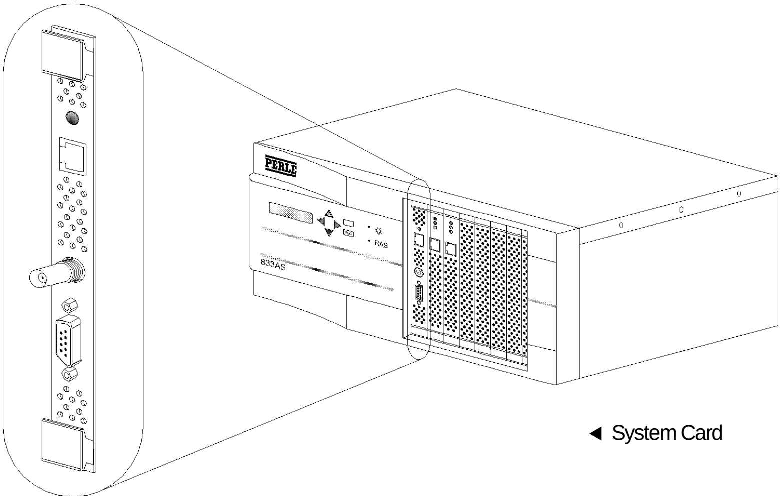
Menu	Description
▲	Up
▼	Down
◀	Left
▶	Right
Enter ↵	Start selected function or confirm entered data.
Esc	Escape. Returns to the previous submenu or cancels the current command.

Operator Panel LEDs

Menu	Description
Power	Indicates that the 833AS is powered up.
System Active	Blinks continuously when the 833AS is operational. Blinking will start after System initialization is complete.

System Card

The System card is the main processing card for the 833AS. It is always located in Slot 1.



◄ System Card

The System card includes a 10/100 Mbps Ethernet interface that supports 10Base-T and 100Base-TX (RJ-45 connector) and 10Base2 (BNC connector) type Ethernet. The Link LED flashes when the Ethernet interface is connected to the LAN and data is being transmitted or received.

The Service port is a serial port that is for service use only.

On the circuit board of the System card, there are expansion sockets for additional RAM. Your 833AS contains the RAM required for your application.

Feature Card Slots

Slots 2 through 8 are for Feature Cards. The following Feature Cards are available:

- Token Ring LAN Feature Card
- T1/PRI Feature Card
- Dual T1/PRI Feature Card
- E1/PRI Feature Card
- Dual E1/PRI Feature Card
- PerleDSP 12 Modem Feature Card
- PerleDSP 18 Modem Feature Card

The Feature Cards can be installed in any available slot. Your Feature Cards may have been installed prior to delivery.

Serial Number Label

This label contains the serial number for the unit.

Dual Redundant Power Supply

The Dual Redundant power supply consists of two separate power supplies within a common case. Both supplies are powered up and active during normal operation. If one supply fails, the 833AS will operate on the second supply.

Power Switch

The Redundant power supply has a power switch for each power supply. Use the power switches to turn power for the 833AS on and off. When power is on, one or more LEDs on the front of the unit will be lit.

For the 833AS to be turned off, both power switches must be in the off position.

Voltage Selector Switch

The Redundant power supply has a voltage selector switch for each power supply. Use the voltage selector switches to adjust the 833AS for the electrical service available at your site. The selected setting is visible on the switch. This switch has two positions:

- 115 for 100 - 125 VAC
- 230 for 200 - 240 VAC

Both switches must be in the correct position, or you may damage your unit.

Buzzer Reset Switch

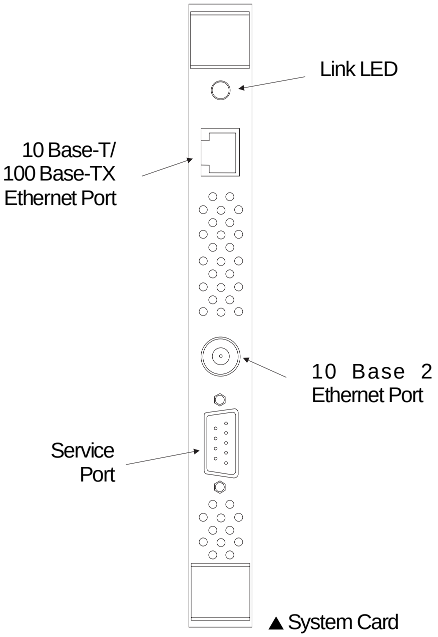
A warning buzzer will sound if one of the power supplies is not providing power. This could be due to a supply failure, or because the power was not switched on for that supply.

Press the Buzzer Reset Switch to turn off the warning buzzer.

Feature Cards

Each T1/PRI, Dual T1/PRI, E1/PRI, Dual E1/PRI and PerleDSP Modem card contains high performance RISC processors. They improve performance by offloading character oriented processing from the System card. Since each Feature Card contains the necessary processing power, 833AS system performance will remain high as the unit expands. Feature Cards operate as PCI bus masters, freeing the System card from data transfers and ensuring that the bus is used to its maximum potential.

System Card Physical Description



▲ System Card

Link LED

- Flashes to indicate that the card detects activity on the Ethernet.

10Base-T/100Base-TX Connector

- RJ-45 Female Connector.
- Used to connect to either a 10Base-T or 100Base-TX LAN.

10Base2 Connector

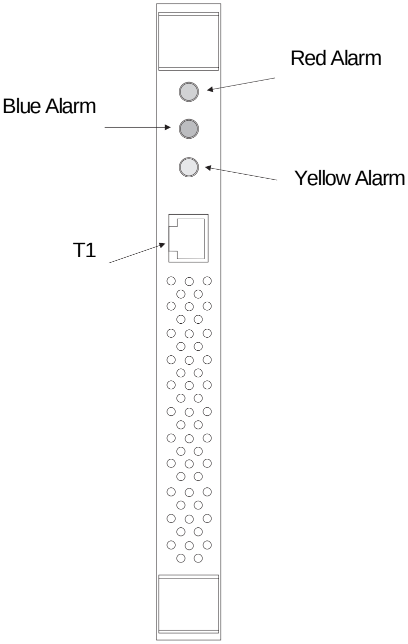
- BNC.
- Used to connect to a 10Base2 LAN.

Service port

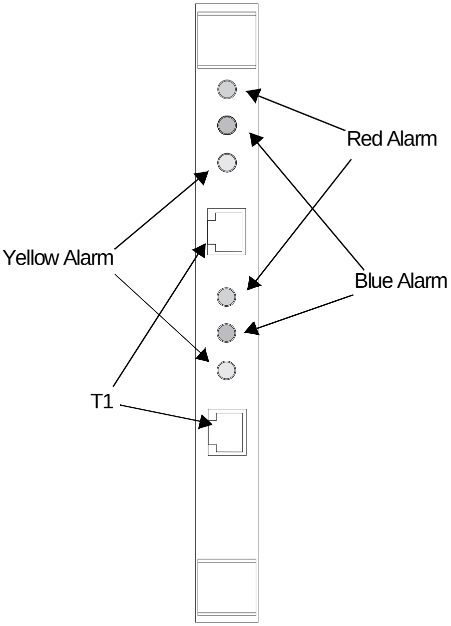
- DB9.
- For Service use only – not for Customer use.

You should connect the card to the Ethernet LAN using either the RJ-45 or BNC interface, but not both.

T1/PRI or Dual T1/PRI Card Physical Description



▲ T1 Card



▲ Dual T1 Card

Red Alarm LED

Lights if the T1/PRI card locally detects a line failure. An example of a detected line failure is loss of line synchronization for 2.5 seconds.

Blue Alarm LED

Lights if the T1/PRI card has seen two consecutive T1 frames with less than three zeros in the data bit stream. This is also known as the AIS (Alarm Indication Signal)

Yellow Alarm LED

Lights if the T1/PRI card receives a yellow alarm signal from the Central Office. This signal is transmitted if the remote link believes that it has lost contact with the 833AS.

T1 Connector

RJ-48C Female Connector wired as a 4 wire PRI.

Pin 1 = Receive (Tip)

Pin 2 = Receive (Ring)

Pin 3 = Grounded

Pin 4 = Transmit (Tip)

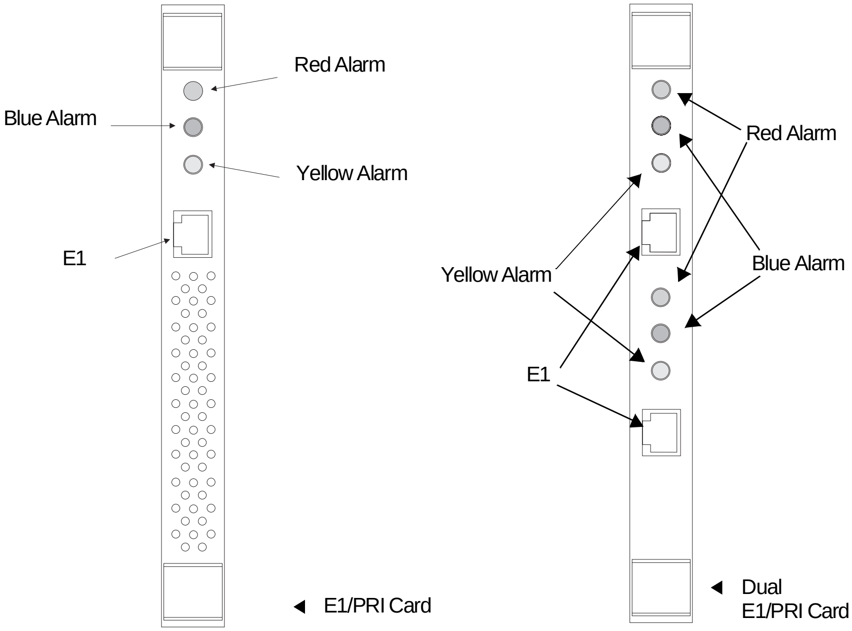
Pin 5 = Transmit (Ring)

Pin 6 = Grounded

Pin 7 = OPEN

Pin 8 = OPEN

E1/PRI Card or Dual E1/PRI Card Physical Description



Red Alarm LED

Lights if the E1/PRI card locally detects a line failure. An example of a detected line failure is loss of synchronization for 2.5 seconds.

Blue Alarm LED

Lights if the E1/PRI card has seen two consecutive E1 frames with less than three zeros in the data bit stream. This is also known as the AIS (Alarm Indication Signal).

Yellow Alarm LED

Lights if the E1/PRI card receives a yellow alarm signal from the Central Office. This signal is transmitted if the remote link believes that it has lost contact with the 833AS.

E1 Connector

- RJ-48C Female Connector wired as a 4 wire PRI.
- 120 ohms

Pin 1 = Receive (Tip)

Pin 2 = Receive (Ring)

Pin 3 = Grounded

Pin 4 = Transmit (Tip)

Pin 5 = Transmit (Ring)

Pin 6 = Grounded

Pin 7 = OPEN

Pin 8 = OPEN

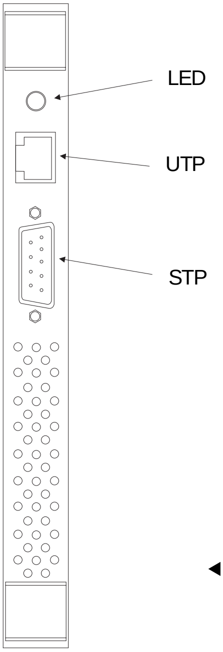
Alarms

The Perle 833AS has a straightforward "Fault Indication Plan" as recommended by ITU/CCITT 0.162. Each E1 interface on the 833AS has three LEDs (RED, GREEN. YELLOW) which are used to display the following status and error conditions:

■	Loss of Signal or Syncs	- RED continuous ON
■	Alarm indication signal	- RED Flashing
■	Loss and recovery of frame alignment	- GREEN continuous ON
■	Loss and recovery of multiframe alignment	- GREEN flashing
■	Distant Alarm	- YELLOW continuous ON
■	Distant Multiframe Alarm	- YELLOW Flashing

In addition to displaying the above alarm conditions, the 833AS will generatethe "Distant alarm" and the "Multiframe Distant alarm" to the Telelphone company when these conditions are detected by the 833AS.

Token Ring Card Physical Description



◄ Token Ring Card

Link LED

Flashes to indicate that the card detects activity on the Token Ring LAN.

Shielded Twisted Pair (STP) Interface

- DB9 connector.
- Used to connect to a Media Access Unit utilizing IBM style universal connectors.

Unsheildded Twisted Pair (UTP) Interface

- RJ-45 Female Connector.
- Used to connect to a Media Access Unit using UTP wiring.

You should connect the card to the Token Ring LAN using either the STP or UTP interface, but not both.

PerleDSP Modem Card

There are no connectors or LEDs on this card. All monitoring is done via the Front Panel and Manager.

Assembling the Hardware

Setting the Voltage Selector Switch

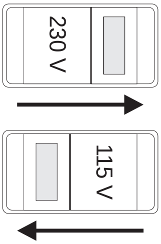
To set the voltage selector switch on the back of the 833AS:

1. Ensure that the 833AS is powered off. The Front Panel LED should be off.
2. Ensure that all power cords are disconnected from the electrical outlet.

If the voltage selector switch is set incorrectly, it may cause permanent damage to the unit and void any warranty. The 833AS must always be powered off and all power cords disconnected before adjusting the voltage selector switch. This setting must be done for both supplies.

3. Set the Voltage Selector Switch on each supply to the correct voltage as follows:
   - 115V for inputs of 100-125 VAC
   - 230V for inputs of 200-240 VAC

The following diagram shows the voltage selector switch in both the 115V and 230V positions.



◀ Voltage Selector Switch

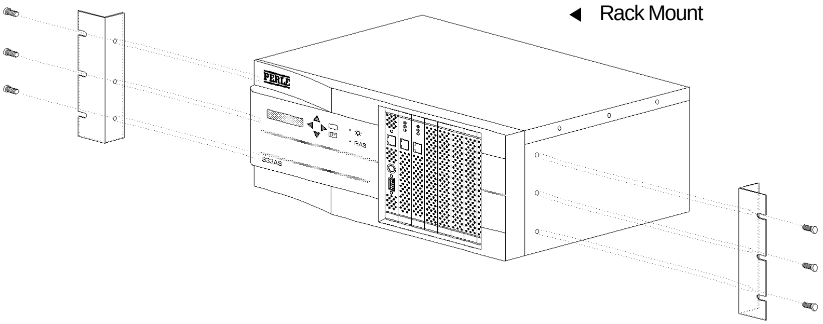
Connect the Power Cords

For each supply, connect one end of the supplied power cord into the 833AS power connection and the other end into a properly grounded electrical outlet.

For safety, this equipment is designed to be electrically grounded. The 833AS must be connected to a three wire grounded outlet only. The power cords supplied include a third (grounding) pin. If you are unable to insert the plug into an outlet, contact an electrician to replace the outlet with a properly grounded outlet.

Attaching the Rack Mount

The Rack Mount Kit provided can be used if you wish to install the 833AS in a standard 19" equipment rack. Use the screws included in the Rack Mount Kit to attach the Rack Mount brackets to the 833AS.



You require 6 Rack Mount screws (3 per side) to mount the 833AS in the Rack. Do not install the 833AS in the Rack with fewer screws. For rack mounting, the 833AS requires 5 rack mount spaces (i.e. the 833AS height is 5U). It is not necessary to leave empty spaces above or below the unit in the rack.

⚠ *Sufficient clearances must be maintained in front of and behind the unit to allow proper air flow to the internal fans.*

Mounting of the equipment in the rack shall be such that a hazardous condition does not occur due to uneven mechanical loading. Heavier equipment should be located at the bottom of the rack, and the rack should be loaded such that the bottom slots are used first (fill from the bottom up).

Circuits supplying power to the rack must be sufficient to safely supply power to all equipment within the rack based on the equipment nameplate rating. Power distribution to all equipment in the rack must have proper grounding. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. power strips).

Factory Default Mode

The operating Firmware and configuration for the 833AS is downloaded from the Manager to the Server. Before this occurs, the 833AS is in **Factory Default** mode, or simply **Factory** mode. In Factory mode, you use the Front Panel to configure any parameters needed to connect with the Manager. You then use the Manager to attach to the Server and download the Firmware and configuration. Factory mode also provides statuses on the Front Panel to help diagnose communication problems with the Manager. Front Panel operation in this mode is detailed in “Factory Default Mode” on page 247.

Once the 833AS has Firmware and is fully configured, the unit is in Normal mode. The unit can be restored to Factory mode from the Manager (“Configure Menu” on page 64) or Front Panel (“Control” on page 236).

Setting up the 833AS LAN Connection

This step includes the minimal configuration needed to enable the 833AS Manager to communicate with the 833AS. During installation, the Manager uses a LAN connection to talk to the 833AS. Once fully configured, you can manage the 833AS across the LAN, or from a Dial-In connection.

The Manager communicates with the 833AS by either IP or IPX protocols. There is no difference in the Manager's capability in either environment. You may choose whatever protocol is most appropriate for your network or set up the 833AS to support both IPX and IP.

The 833AS has a built in 10/100 Mbps Ethernet adapter. There is a 4/16 Mbps Token Ring Feature Card available to allow the 833AS to operate in a Token Ring environment. Only one adapter is operational at a time. If the Token Ring adapter is installed, the Ethernet adapter is disabled.

IPX Connection to the Manager

No configuration is required for the Manager to communicate with a 833AS using IPX. By listening to the traffic on the LAN, the 833AS learns about all the networks that it can reach. It automatically discovers the IPX network numbers for the networks and all supported frame types on the network.

IP Connection to the Manager

IP networks require devices to be configured with unique addresses. Depending on network topology, other parameters may have to be set. Most organizations have a department or individual responsible for IP address management. Consult with them to get the correct values.

The Manager can communicate to an 833AS through one or more routers. If the routers pass IP broadcast messages, you need only set the IP parameters listed below in the Server. The Manager can then discover the Servers using IP broadcasts. However, if the routers do not pass IP broadcasts, you will need to explicitly define the 833AS in the Manager as detailed in "IP Connection Through Routers" on page 60.

The 833AS requires the following IP parameters be established:

IP Address

This address uniquely identifies the unit to the IP network. The 833AS supports a number of ways of acquiring this IP address.

- You can configure an IP address from the Front Panel.
- If you are managing your network IP addresses on either a BOOTP (Boot Protocol) or RARP (Reverse Address Resolution Protocol) server, you can set the IP address there. The 833AS attempts to acquire the IP address from a BOOTP or RARP server by default. You will need the MAC address of the 833AS to do this. This address can be obtained from the Front Panel.

IP Subnet Mask

An IP network can be partitioned into subnetworks, or subnets. For IP networks on a single LAN segment, there are likely no subnets defined. If you have a larger IP network with IP routers, you likely have subnets defined.

If your IP network has not been partitioned, the IP subnet mask will default to the correct value. If you have set up subnets in your IP network, set the mask as instructed by your IP Network Administrator.

IP Gateway Address

If the IP network path to the Manager passes through an IP gateway or router, enter the IP address of the gateway that is on the same LAN segment as the 833AS.

Set up the basic parameters

The LAN cable should not be connected to the 833AS at this time. Power up the 833AS by turning on the power switch at the rear. If your 833AS has redundant power supplies, power up both supplies. The power LED should be lit.

The Front Panel will display:

```
Perle 833AS
```

After 5 seconds, the display will change to:

```
No Manager
```

This indicates that the 833AS is not communicating with a Manager.

Using the Front Panel

When the 833AS is received from the factory there is no configuration within the unit. The Front Panel is in "Factory mode", and lets you:

- Set the parameters needed for communication with the Manager
- Monitor the 833AS's operation on the network to verify correct configuration and provides information to diagnose network problems.

You navigate through the Front Panel screens as follows:

Left ◀ , Right ▶ Keys

Selects a menu.

Up ▲ , Down ▼ Keys

View entries within a menu.

Enter ↵ Key

If an item can be edited, enables the item to be edited.

ESC

Return to the previous screen.

When editing a field, the keys behave as follows:

Left ◀ , Right ▶ Keys

Selects a menu. Position the cursor to the correct editing position.

Up ▲ , Down ▼ Keys

View selections within a menu or change values at the cursor position.

Enter ↵ Key

Accept changes and exit edit mode.

ESC Key

Discard changes and exit edit mode.

To configure the basic parameters:

Press ▶

```
Perle 833AS
```

Press ▼

```
IP Address
```

If you wish to configure an IP address, enter the value here.

Do not enter an address if you are:

- Using an IPX connection with the Manager.
- Using an address server to acquire the IP address.

To enter an IP address, press **Enter** to go to Edit mode.

```
IP Address
000.000.000.000
```

Use ◀ ▶ to select the digit to change. Use ▲ ▼ to change the digit. When complete, press **Enter** to accept the new address and exit Edit mode. If you wish to discard your changes, press **Esc**.

Press ▼

```
IP Subnet Mask
255.255.255.000
```

Enter the IP subnet mask if required. The IP subnet mask will display **none** if none has been configured. When **none** is displayed, the 833AS will use the default subnet for the network class (i.e. for a Class C IP address, the IP subnet mask of 255.255.255.0 will be used).

Press ▼

```
IP Default Router
000.000.000.000
```

Enter the IP default router if required.

Press ▼

```
Token Speed
16 Mbps
```

If you have a Token Ring Feature Card installed, this panel will be displayed.

Set the value to match your Token Ring LAN speed (4 or 16 Mbps).

If you are using an IP address server, determine the MAC address of the 833AS by doing the following:

Press the ▲ key until you see this front panel:

```
Manager Setup
```

Press ▶

```
Status
```

Press ▼

```
MAC Address
020000044444
```

Provide this address to your IP Network Administrator.

Configuration for the Manager is now complete. Power down the 833AS.

Attaching the LAN Cable

You will need a LAN cable to attach the 833AS to the network connection.

Ethernet

You will need the appropriate cable to attach the 833AS to the Ethernet:

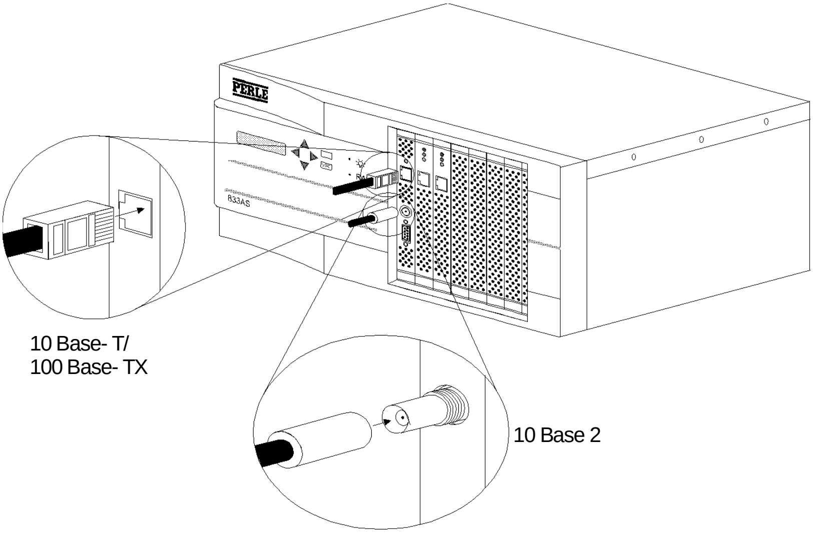
- 10Base-T: UTP, Category 3, 4 or 5
- 100Base-TX: Category 5 UTP or Type 1 STP
- 10Base-2: 50 ohm Thin Ethernet

For a complete discussion on Ethernet cable requirements, see “Cable Planning and Requirements” on page 14.

The Ethernet interface is on the System board of the 833AS, located in slot 1.

To attach the cable:

1. Ensure that the 833AS is powered off.



▲ Ethernet/LAN Cable Connection

No configuration is needed for the Ethernet physical port. The cable is automatically sensed.

2. Attach the cable as shown.
3. Power on the 833AS.

Token Ring

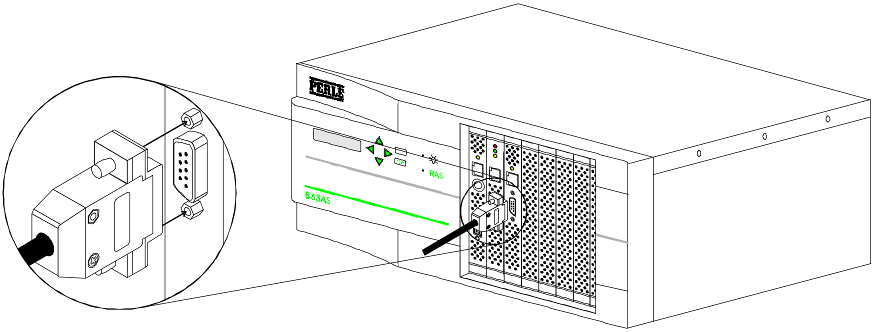
The Token Ring Feature Card may be installed in any slot other than slot 1. If you are attaching the 833AS to a Token Ring network, you will need either:

- A UTP cable (Type 3 wiring), or
- An STP (Shielded Twisted Pair) adapter cable (DB9 to either Type 1 or Type 6 Token Ring wiring).

To attach the cable:

1. Power off the 833AS.
2. Attach the cable as shown:

No configuration is needed for the Token Ring physical port. The cable is automatically sensed.



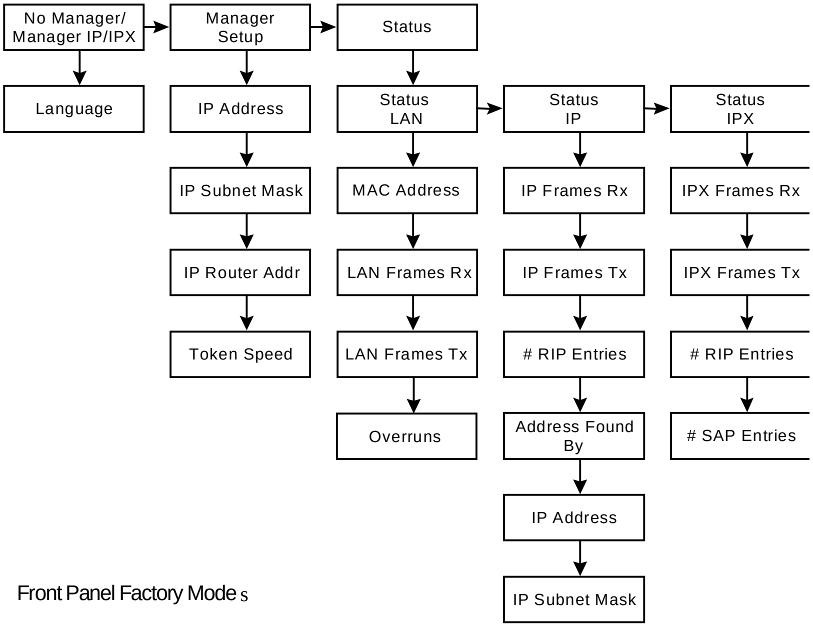
▲ Token Ring/LAN Cable Connection

3. Power on the 833AS.

Verifying Connection

On the LAN card, there is a Link LED which flashes to indicate network activity. If this LED does not flash, check the physical cabling between the 833AS LAN adapter and the Hub or MAU (Multistation Access Unit).

The Front Panel provides status information that allows you determine whether the 833AS basic configuration is correct. The menu structure for the Front Panel in Factory mode is shown in the diagram below.



Front Panel Factory Mode s

Status Fields are listed in the following section. A complete description of Front Panel Factory Mode is found in “Factory Default Mode” on page 247, and “Factory Default Mode” on page 249.

LAN Status

MAC Address

Displays the burned in MAC address of the 833AS LAN adapter.

LAN Frames RX

Displays the number of frames received by the 833AS LAN adapter. This should increment as the unit receives broadcast messages from the network.

LAN Frames TX

Displays the number of frames transmitted by the 833AS LAN adapter. This should increment as the unit responds to the broadcast messages from the network.

Overruns

Displays the number of frames that were discarded by the 833AS LAN adapter because of a receive overrun state. This condition indicates that the 833AS has received such a large burst of traffic that it is temporarily out of free internal resources. This number should be zero, or very small in proportion to the LAN # frames RX. If this number is large there is a problem on the existing network that is causing excessive broadcasts to be sent.

IP Status

IP Frames RX

Displays the number of IP frames received by the 833AS. This should increment on an IP network as the unit receives IP broadcasts from the network. If this remains at 0, there is likely a problem with the configured settings or you are not running IP on your network. The Manager will not connect using IP unless the 833AS receives IP broadcast messages.

IP Frames TX

Displays the number of IP frames transmitted by the 833AS. This should increment as the unit generates and responds to network IP broadcast messages.

# RIP (Routing Information Protocol) Entries

This number will be non-zero if the 833AS has received RIP broadcasts from other subnetworks.

Address Found by

Displays what mechanism was used to acquire the 833AS IP address. The value will be BOOTP, RARP, Configured, or None. If None is displayed, it indicates that the 833AS could not acquire an IP address or the IP protocol is not used. If you were using an Address server and Default is displayed, check the setup of the Address server.

IP Address

Displays the IP address used by the 833AS.

IP Subnet Mask

Displays the configured IP subnet mask.

IPX Status

IPX Frames RX

Displays the number of IPX frames received by the 833AS. This should increment on an IPX network as the unit receives IPX broadcasts from the network. If this remains at 0, there is likely a problem with the configured settings, or you are not running IPX on your network. The Manager will not connect using IPX unless the 833AS receives IPX broadcast messages.

IPX Frames TX

Displays the number of IPX frames transmitted by the 833AS. This should increment as the unit generates and responds to network IPX broadcast messages.

# RIP Entries

Displays the number of entries within the 833AS's IPX RIP table. There will be one RIP entry for each IPX router detected.

Note that a Novell file server defines an "internal" network within the server itself, so there will be a RIP entry for each Novell file server. If the number of RIP entries is 0, no routes or file servers can be seen by the 833AS.

# SAP (Service Advertising Protocol) Entries

Displays the number of entries within the 833AS's IPX SAP table. There will be one SAP entry for each service advertised. If the number of SAP entries is 0, no servers can be seen by the 833AS.

Configuring the 833AS

Refer to Section 2: "Configuring the 833AS" for detailed instructions on the configuration process.

During this configuration process, you will:

- Connect the Manager with the 833AS. See “Chapter 4: Using the Perle 833AS Manager” .
- Download the 833AS System software.
- Set up the parameters for the T1 or E1 lines that you will use for incoming calls. See “Chapter 5: Configuring the Perle 833AS” .
- Configure the network parameters for the protocols that your remote users will use. See “Chapter 7: Configuring the Protocols” .
- Set up the type of security that you wish to use to control remote access to your network. See “Security” on page 179.
- If you select "User Database" as your method of security, add users to the 833AS's user database and set their access rights and capabilities. See “Chapter 8: Configuring the User Database” on page 153.
- Download the configuration to the 833AS. See “Downloading” on page 79. This download will cause the Front Panel operation to change from Factory mode to Normal mode.

In order to minimize the amount of configuration, defaults are provided that work for most installations. The 833AS Manager also provides a great deal of flexibility to meet the needs of special network requirements. However, most sites will not require these advanced capabilities.

You can take advantage of the Group features to allocate different lines and services to different groups of people. (See “Group Settings” on page 193). However, to simplify installation, it is recommended that Groups be set up after basic installation is complete and operation verified.

Attaching to the Telephone Network

You will need the appropriate cable to attach the 833AS to the telephone network. The T1/PRI and the E1/PRI Feature Card supports RJ-48C connections.

1. Ensure that the 833AS is powered down.
2. Attach the cable between the T1/PRI or EI/PRI Feature Card and the line termination point. This may be a CSU, or the telephone line demarcation point.
3. Some E1 R2 CAS connections may require a special "RJ48 to BNC" cable to attach to BNC terminated demarcation points.

What's next?

At this point, installation is complete. Proceed to Chapter 4 for instructions on loading Firmware and "Section 2: Configuration" for instructions on configuring the 833AS. You can now verify that remote users can dial into the 833AS and access the services. Also, you can install Perle Dial-Out software on LAN PCs, and verify that the Dial-Out is functioning correctly.

If you are using Perle Remote Access Client software, please see the *Perle Remote User's Guide* for details on software installation and operation.

If you are using Perle Dial-Out software, please see the *Perle Dial-Out User's Guide* for details on software installation and operation.

Chapter 4: Using the Perle 833AS Manager

About Using the Manager

This chapter describes how to install and use the 833AS Manager program.

You will read about:

- Overview
- System Requirements for the Manager
- Installing the Manager software
- Connecting to the Server
- Manager Main screen
- Loading Firmware

Overview

The 833AS Manager is a Microsoft Windows application that configures, monitors, and manages 833AS Servers. The Manager performs the following functions:

- Downloads Firmware to an 833AS.
- Creates Configuration Files to be downloaded to an 833AS.
- Will upload a configuration file from an 833AS. This uploaded file can be modified, saved on the Manager PC, or downloaded to another 833AS.
- Displays Statistics for an 833AS.
- Displays the Event Log of an 833AS.

These functions can be performed for all 833AS Servers that have valid network connections to the Manager. The network connection between the Server and Manager is done via IP or IPX protocols and is often referred to as an "in-band" connection. Note that the Manager can connect either from the 833AS LAN connection, or dialed in from the WAN.

System Requirements

The minimum PC requirements for the 833AS Manager software are:

- Hard drive with at least 4 MB free storage space.
- Microsoft Windows 3.1 or higher with MS-DOS version 5.0 or higher, or
- Windows 95 or 98, or
- Windows NT 3.5 or 4.0.
- Windows compatible mouse.

LAN Connection

The Manager software requires IP or IPX network facilities to be available on the Manager PC.

- For an IP connection, a working IP connection to the LAN is required. IP is built into Windows 95, Windows 98 and Windows NT. For Windows 3.1, a TCP/IP stack is provided on the Manager installation disks.
- For an IPX connection, a working IPX connection to the LAN is required. The 833AS Manager works with Novell IPX stacks, and the Microsoft 95 and NT IPX stacks.

WAN Connection

For a dial up connection, you require:

- Dial Up Client.
- Dial Up (Modem or ISDN) interface.
- If external interface, serial port and modem cable.
- Connection to phone network.

Dial up Networking functionality must be provided on the Manager PC if you are connecting via the WAN. The following Dial-Up Clients have been approved for use with the Manager:

- Perle Remote Client.
- Microsoft Windows 95/Windows 98 Dial-Up Networking Client.
- Microsoft Windows NT Version 3.5 or 4.0 Dial-Up Client.

A dial up interface is also required. This can be an analog modem or an ISDN Basic Rate Interface. These are available as both internal (a card in the PC) or external interfaces.

If you are using an external interface, you require an unused serial (COM) port on the Manager PC. A buffered serial port (for example, one that uses a 16550 UART) is strongly recommended. An unbuffered serial port supports a lower maximum baud rate than a buffered port. Serial ports on older devices are usually not buffered. You will also require a serial cable to connect the interface to the serial port.

Installing the Manager Software

To install the 833AS Manager software, follow these steps:

Windows 3.1

1. Start Microsoft Windows.
2. Place the 833AS Manager disk labeled Disk 1 in the diskette drive.
3. In **Program** Manager choose **Run** from the **File menu.**
4. Type **A:\Setup** where A: is the diskette drive letter.
5. Press **Enter.**
6. To complete installation, follow the prompts that appear on the screen.

Windows 95, Windows 98 and Windows NT

1. Start Microsoft Windows.
2. Click the **Start** button.
3. Click **Run.**
4. Type **A:\Setup** where A: is the diskette drive letter.
5. Press **Enter.**
6. To complete installation, follow the prompts that appear on the screen.

Setting up for Connection

You can connect to the Manager via IP or IPX protocols. If you are connecting the Manager for the first time, you must connect via the LAN. This is because the Dial in ports are not yet configured.

IPX Connection

No configuration is required for the Manager to communicate with a 833AS using IPX. By listening to the traffic on the LAN, the 833AS learns about all the networks that it can reach. It automatically discovers the IPX network numbers and all supported frame types on the network.

IP Connection

IP networks require devices to be configured with unique addresses. Depending on network topology, other parameters may have to be set. For an initial connection, you must set these parameters from the Front Panel. See “Set up the basic parameters” on page 41.

If the 833AS is on the same physical LAN segment as the Manager, you need only configure the IP address.

Most organizations have a department or individual responsible for IP address management. You should consult with them to get the correct values. The 833AS requires the following IP parameters to be established:

IP Address

This is the address that uniquely identifies the unit to the IP network. The 833AS supports a number of ways of acquiring this IP address:

- If you are managing your network IP addresses on either a BOOTP or RARP server, you can set the IP address there. The 833AS attempts to acquire the IP address from a BOOTP or RARP server by default. You will need the MAC address of the 833AS to do this. This address can be obtained from the Front Panel.
- You can configure an IP address from the Front Panel.

IP Subnet Mask

An IP network can be partitioned into subnetworks, or subnets. For IP networks on a single LAN segment, there are likely no subnets defined. A larger IP network with IP routers will likely have subnets defined.

If your IP network has not been partitioned, the IP subnet mask will default to the correct value. If you have set up subnets in your IP network, set the mask as defined by the IP Network Administrator.

IP Router Address

If the IP network path to the Manager passes through an IP router, enter the IP address of the router that is on the same LAN segment as the 833AS.

If the Manager must pass through a router to reach the 833AS, the router must pass broadcast messages between the networks. If the router blocks broadcasts, you must configure the 833AS IP address in the Manager. See “IP Connection Through Routers” on page 60 for details.

Connecting to the Server

To connect to the 833AS via the LAN, start the Manager. The Manager will automatically search for all 833AS Servers on the network.

The 833AS will appear in the Server list if the 833AS is correctly connected. See “Completing the Connection” on page 58 for details.

If the 833AS does not appear in the Server List:

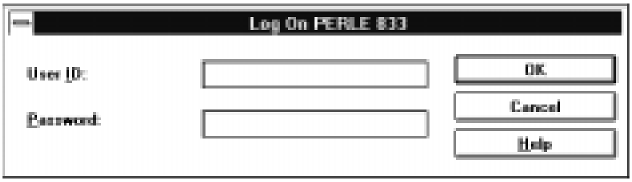
- The link LED on the Ethernet or Token Ring card will flash if the physical connection is OK. If this does not flash, check the 833AS LAN cable and the connection to the Ethernet hub or Token Ring MAU.
- Verify your client protocol configuration. If your PC can see other file and print servers on the network, the protocol configuration is likely OK.
- If you are connecting via IP, verify your 833AS IP settings. If the Manager must pass through a router, you will have to define the server in the Manager if the server blocks broadcasts. See “IP Connection Through Routers” on page 60

Dial In Connection

To establish a Dial In Connection:

1. Install the Manager on your PC.
2. Using your **Dial-up Client**, set up a dial-up Network connection:
   - Enable either **IP** or **IPX.**
   - If you are using an **IP** connection, your client requires an **IP** address. Most clients provide the option to configure the IP address in the Client, or use an IP address supplied by the Server. If you have disabled "**Allow client specified IP addresses**" in the 833AS configuration, set the **IP** address supplied by the Server. See “Allow Client Specified IP Addresses” on page 116.
   - Use the highest baud rate supported by your modem and serial port.
3. Set up your modem or ISDN interface.
4. Start up the **Dial-up** session. Enter the **User ID** and **Password** for the Server. The dial-up connect sequence should start.

5. Once the Dial-up session is connected, start the 833AS Manager. The **Main** Manager screen will be displayed and the **Log On** box will appear:



6. Reenter the **User ID** and **Password** as in Step 4. Click on **OK**.

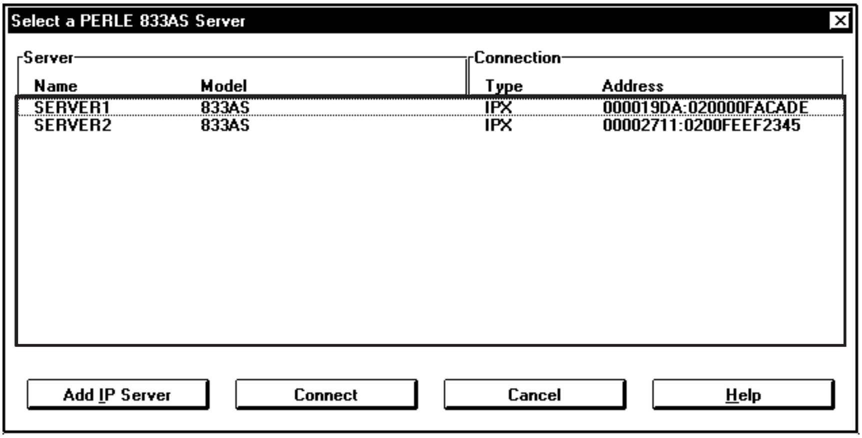
*The default User ID for an unconfigured 833AS is “**superusr**”, with no password. The User ID is case sensitive.*

This User ID and password is valid for an unconfigured 833AS only. You will be required to set up a User ID with Administration privileges when you configure the Server. This will not be required if you select “Radius” as your security method.

Completing the Connection

When the 833AS Manager connects to the network, it automatically locates all 833AS Servers on the network and displays them in the Server List window.

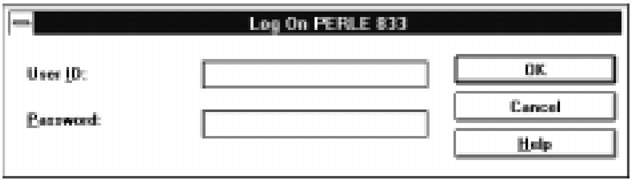
To complete the connection to a server:



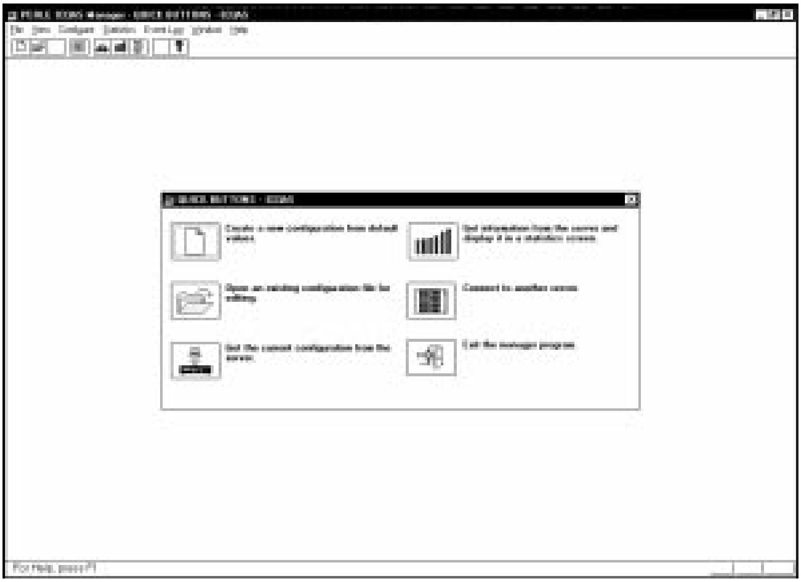
Server		Connection	
Name	Model	Type	Address
SERVER1	833AS	IPX	000019DA:020000FACADE
SERVER2	833AS	IPX	00002711:0200FEEF2345

1. Highlight the **Server** that you wish to connect to and click **Connect**. The **Log On** dialog box will appear. If you are connected by IP and the Server does not appear in the list, you may need to define it to the Manager. See "IP Connection Through Routers" on page 60.

2. Enter the **User ID** and **Password** for the selected Server and click **OK**.



3. If the **User ID** and **Password** are valid, then the Manager main screen is displayed.



Create a new configuration from default values.

Open an existing configuration file for editing.

Get the current configuration from the server.

Get information from the server and display it in a statistics screen.

Connect to another server.

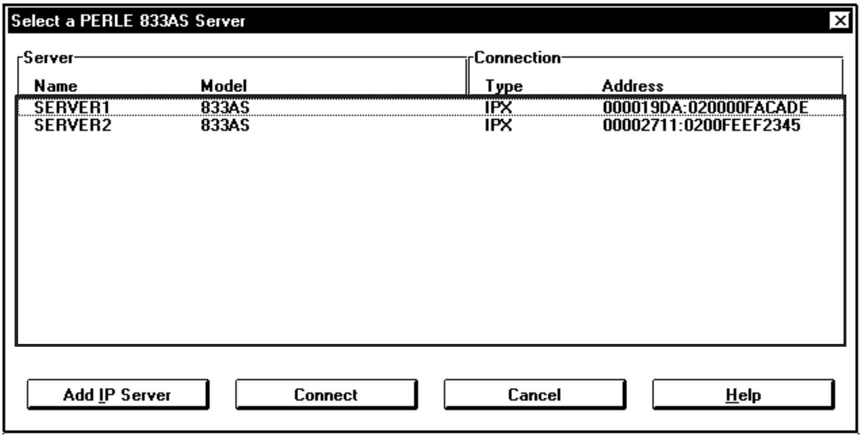
Exit the manager program.

4. If this is the first time that this 833AS is connecting to the Manager you will have to download Firmware to the 833AS. If the 833AS has Firmware, the Manager checks the Firmware level. If the Firmware is at an older revision level, you will be prompted to update the Firmware. See “Loading Firmware” on page 68.

Only one Manager can be connected to a Server at a time.

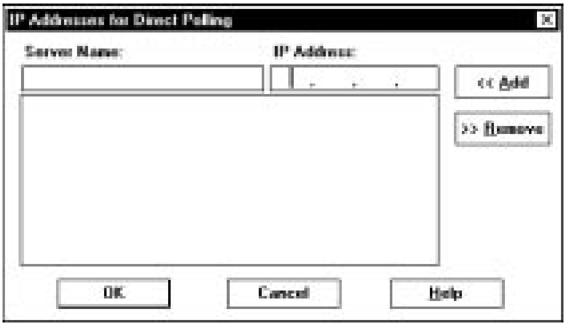
IP Connection Through Routers

The Manager can communicate to an 833AS through one or more routers. The Manager can discover the Servers using IP broadcasts. However, if the routers do not pass IP broadcasts, you will need to explicitly define the 833AS in the Manager:



Name	Model	Type	Address
SERVER1	833AS	IPX	000019DA:020000FACADE
SERVER2	833AS	IPX	00002711:0200FEEF2345

1. From the Server List, click on **Add IP Server**.



2. The **IP Addresses for Direct Polling** screen will display. Enter the name of the Server in the **Server Name** field.

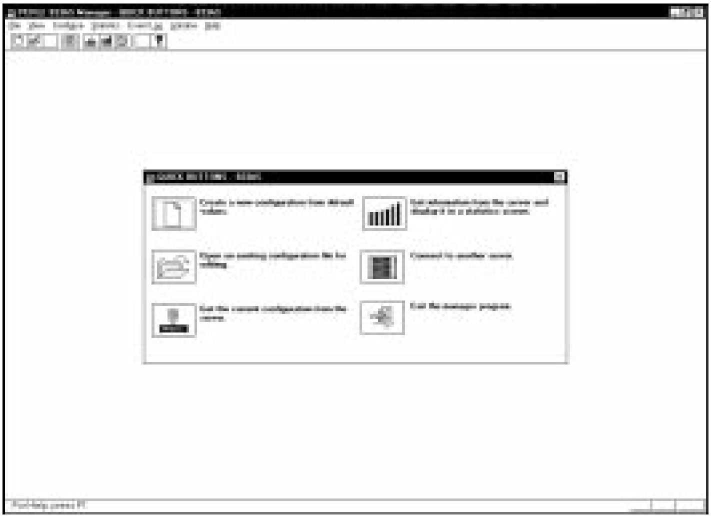
3. Enter the IP address of the Server in the **IP Address** field.

4. Click on **Add**.

The 833AS is now defined to the Manager. When the Manager connects via IP, it will check for the defined Servers. Note that the Manager will still automatically search for Servers on connection.

Using the Manager Main Screen

The Perle 833AS main screen contains menus and the following tools and windows:



Menu Bar

Contains menus that are used to control the Manager and configure Perle 833AS servers. The Menu bar contains the following menus—**File; View; Configure; Statistics; Event Log; Window; and Help.**

Tool Bar

Makes it easier to perform some of the most-used menu functions.

Quick Buttons Window

A quick way to use the main functions of Perle 833AS. Each function is represented by a button. The **Get Configuration** and **Statistics** buttons are not available when the Manager is not connected to a Perle 833AS.

Status Bar

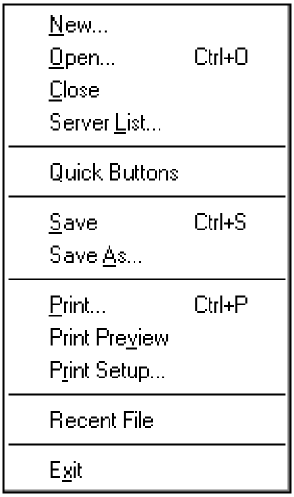
Gives information about menus and menu items when they are selected, and about the status of some keys on the keyboard.

Menu Bar

The menu bar contains all of the menus available when running the Manager. Each menu contains a list of options that drop down from the Menu title. Some of the menu items are only active when a configuration file is open.

File Menu

The following options appear under the **File** menu:



New

Create a new configuration.

Open

Open an existing configuration.

Close

Close the selected configuration file.

Server List

Show all Perle 833AS servers found.

Quick Buttons

Display the Quick Buttons window.

Save

Save the currently selected configuration file.

Save As

Save the currently selected configuration file as a new file.

Print

Print the currently selected configuration file.

Print Preview

Display the currently selected configuration file as it would be printed.

Print Setup

Select a different printer or change the printer setup.

Recent File List

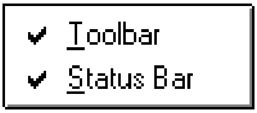
The most recent files that were opened are listed here. Select a file from the list to open that file.

Exit

Quit Perle 833AS Manager. If unsaved changes have been made to any files, you will be prompted to save or cancel the changes.

View Menu

The following options appear under the **View** menu:



Tool Bar

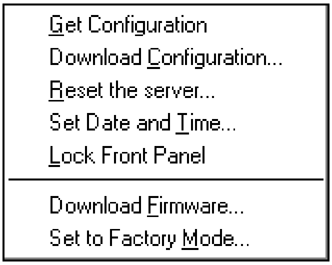
Toggles the tool bar off and on.

Status Bar

Toggles the status bar off and on.

Configure Menu

The Configure menu is enabled when the Manager is connected to an 833AS server. The following options appear under the **Configure** menu:



Get Configuration

Upload the configuration from the connected server and display it in the Configuration File window.

Download Configuration

Download a configuration file to the Perle 833AS.

Reset the Perle 833AS

Reset the Perle 833AS or selected Feature Card. Any sessions handled by the Feature Card or Server will be terminated.

Set Date and Time

Set the system date and time on the Perle 833AS.

Lock Front Panel

Enables/Disables the Front Panel Access Lock. If enabled, the password must be entered at the Front Panel to gain access.

Download Firmware

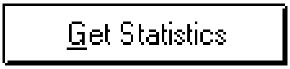
Download a new version of operating code (Firmware) to the Perle 833AS.

Set to Factory Mode

Delete the current configuration and set the server to Factory Default Mode.

Statistics

This option is available on the **Statistics** menu:

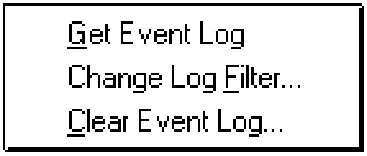


Get Statistics

Display the **System Statistics** window. The **System Statistics** window gives information about the Perle 833AS to which the Manager is connected.

Event Log

The following options appear under the **Event Log** menu:



Get Event Log

This will get the event log file from the connected Perle 833AS and display the data in a scrollable window. The columns in the table are date, time, event and user name if applicable.

Change Log Filter

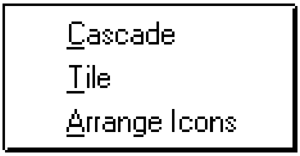
This will lets the user select any of the event types recorded by the 833AS. Only those events will be recorded.

Clear Event Log

This will clear all the data from the connected server’s log file.

Window Menu

The following operations appear under the **Window** menu:



Cascade

Resize and overlap all open windows so that their title bars are visible.

Tile

Resize and arrange all windows across the work space with no overlap.

Arrange Icons

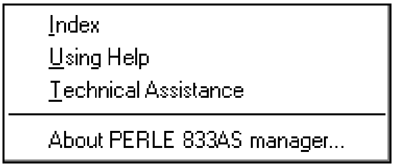
Applies only when at least one configuration window has been minimized, making it into an icon. Choose this option to arrange all icons neatly, starting in the lower left corner.

Open Window List

Lists the windows that are currently open. Select a window to make it active.

Help Menu

The following options appear under the **Help** menu:



Index

Displays the Perle 833AS Manager Help index.

Using Help

Displays general information about using Windows Help.

Technical Assistance

Displays toll-free and direct phone numbers to contact Perle Technical Assistance.

About Perle 833AS Manager

Display the version number of the Perle 833AS Manager program and a copyright notice.

Tool Bar

The tool bar provides point and click shortcuts to many of the most frequently used menu commands.

New File

Create a new configuration file with default values.

Open File

Open an existing configuration file.

Save File

Save the currently selected configuration file.

Server List

Display the list of Perle 833AS remote access servers. Select a server to make a connection.

Get Configuration

Get the current configuration from the connected Perle 833AS.

Get Statistics

Get the Statistics data from the Perle 833AS and display it in the **System Statistics** window.

Get Event Log

Get the event log from the Perle 833AS.

Print

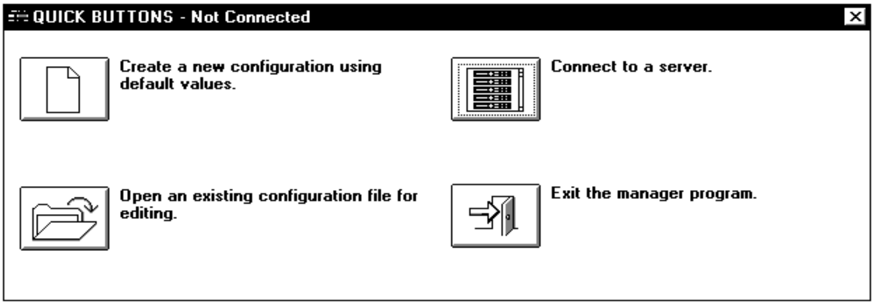
Print the current configuration information.

Help

Display the Perle 833AS Manager **Help Index**.

Off-Line Configuration

The Manager can create or edit a configuration without being attached to a Server. If you wish to do this, click the **Cancel** button on the **Server List Window**. The following quick buttons will appear.



QUICK BUTTONS - Not Connected

Create a new configuration using default values.

Connect to a server.

Open an existing configuration file for editing.

Exit the manager program.

Loading Firmware

Firmware is the basic operating code of a 833AS. A new 833AS must have Firmware downloaded before it is fully functional. This Firmware is contained on the Manager installation disks.

If you wish to install a new version of Firmware in your 833AS, you can download the Firmware from the Manager. You will be prompted to update your Firmware when you connect to a Server under these conditions:

- If the Manager detects that there is no Firmware.
- If the existing Firmware is at an older revision level.
- If you have installed a new feature card, and there is no Firmware for that card type on the unit.

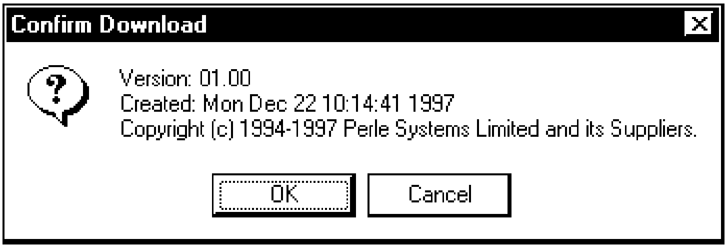
Note that you can choose not to update the Firmware if the current Firmware meets your requirements.

The Firmware upgrade must first be installed on the PC on which you are running the Manager. Follow the instructions included with the Firmware upgrade to install the Firmware on the PC.

The new Firmware will not take effect until the 833AS is restarted.

➲ To download Firmware:

1. Using the 833AS Manager, connect to the 833AS that you wish to download.
2. If the Manager detects that the Firmware download should be done, a dialog box will appear:



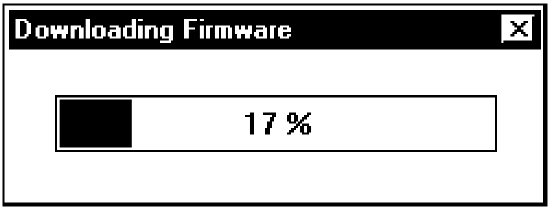
Confirm Download

Version: 01.00
Created: Mon Dec 22 10:14:41 1997
Copyright (c) 1994-1997 Perle Systems Limited and its Suppliers.

Click **OK** to continue, **Cancel** to cancel the download.

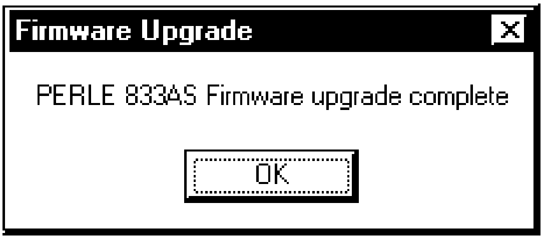
You can also start a download by selecting **Download** Firmware from the **Configure Menu**.

3. A dialogue box will appear displaying the Firmware version that you are about to download. Confirm the download by clicking **OK**. The download will begin and the **download status** is displayed.



Downloading Firmware

4. After the download had completed, the Manager will display “**Download complete**”. The following dialog box will appear:



Firmware Upgrade

PERLE 833AS Firmware upgrade complete

5. For the Firmware to take effect, the 833AS must be restarted. When the Server has completed its restart, it will appear in the **Server List** Window. If you choose to restart the 833AS, any existing sessions will be abruptly terminated.

⚠ *The download should not be interrupted. If the download does not complete, do not reset the 833AS. Restart the Manager and download the Firmware again.*

If the 833AS is reset before the download completes, the target 833AS will revert to Factory Default Mode.

Although you can download the Firmware from a Dial In connected Manager, it is strongly recommended that this be done from a LAN connected Manager.

Section 2: Configuration

Chapter 5: Configuring the Perle 833AS

Chapter 6: Configuring the Feature Cards

Chapter 7: Configuring the Protocols

Chapter 8: Configuring the User Database

Chapter 9: Configuring the Server

Chapter 5: Configuring the Perle 833AS

About Configuring the Perle 833AS

This chapter describes how to configure the 833AS. You will read about:

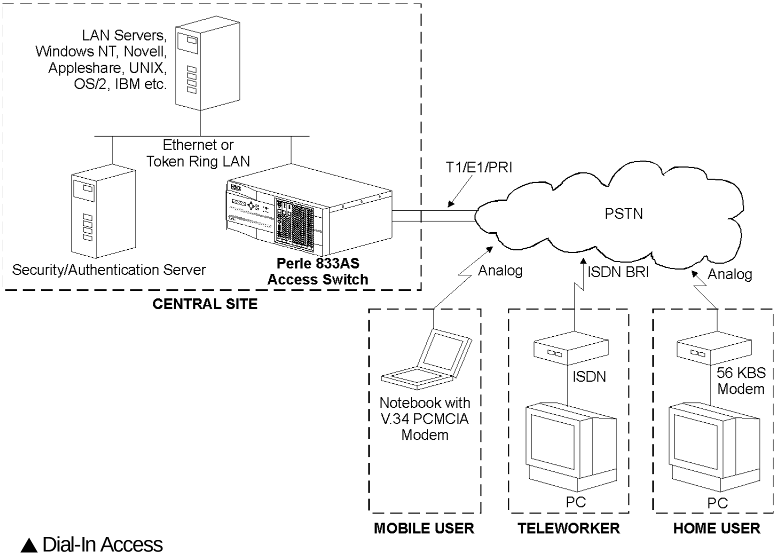
- How the 833AS Works.
- Configuration Overview.
- Using Configuration Files.
- Setting the Date and Time.

How the 833AS Works

The 833AS supports two main modes of operation - Dial-In and Dial-Out.

Dial-In Access

The 833AS lets a user Dial-In with a PC from a remote location to gain access to a LAN. To the remote user, the PC behaves as if it is directly connected to the LAN. This type of connection is known as *remote node*.


LAN Servers, Windows NT, Novell, Appleshare, UNIX, OS/2, IBM etc.
Ethernet or Token Ring LAN
Security/Authentication Server
Perle 833AS Access Switch
CENTRAL SITE
T1/E1/PRI
PSTN
Analog
ISDN BRI
Analog
Notebook with V.34 PCMCIA Modem
ISDN
PC
56 KBS Modem
PC
MOBILE USER
TELEWORKER
HOME USER

▲ Dial-In Access

Remote users can access file servers, Email, Mainframes, application servers, or any other server that is on the LAN.

Incoming Call Handling

When a call comes in on a channel of the T1 or E1 line, the Line card (T1/PRI or E1 PRI) checks the System card to see that there are resources available to handle the call. For example, a modem is required if it is an analog call.

The System card assigns the needed resources to the call. Resources are allocated on a round robin basis to ensure that all resources are used equally.

The Line card then switches the call via the telephony bus to the correct resource. The call is then answered by the Line card or a combination of the Line card and PerleDSP Modem card.

Client Handling

The Perle Server can support three types of clients. All can be supported simultaneously by the Server.

Router Client

This client operates with the Server as a router. Perle Remote and Microsoft Windows 95 and NT clients are examples of this type. It connects using its own remote access capabilities. When communicating to the Perle Server, the client PC can be set up to use either IPX, NetBEUI or IP protocol.

For messages originating from the client PC, the routing client will encapsulate the IP, NetBEUI or IPX protocol in a PPP frame. The Server will remove the PPP header, process the IP, NetBEUI or IPX header, and based on the addressing information supplied at the protocol level, attach the appropriate MAC header. The frame is then forwarded to the LAN.

For messages coming from the LAN and intended for a client PC, the Perle Server will remove the MAC header, process the IP, NetBEUI or IPX headers and based on the addressing information at the protocol level, forward the frame to the appropriate client PC by encapsulating the message within a PPP frame.

Bridge Client

This client operates with the Server as a bridge. The Perle Remote Client can operate as a bridging client as well as a routing client.

The Client establishes an asynchronous connection to the Server. Once a connection has been established with the PC Client, the Perle Server encapsulates LAN frames destined for the PC in PPP. It then transmits them to the PC client software over the asynchronous connection. The PC client strips off the PPP and delivers the frames to the NDIS or ODI (Multi-Link Interface Driver - MLID) Client software which then deliver the frames to a higher level protocol. In turn, higher level protocols on the PC deliver frames to the Perle supplied NDIS or ODI (MLID) client software which encapsulates them in PPP and transmits them to the Perle Server over the asynchronous connection. The Server strips off the PPP and transmits the frame over the LAN connection.

Apple Remote Access Client

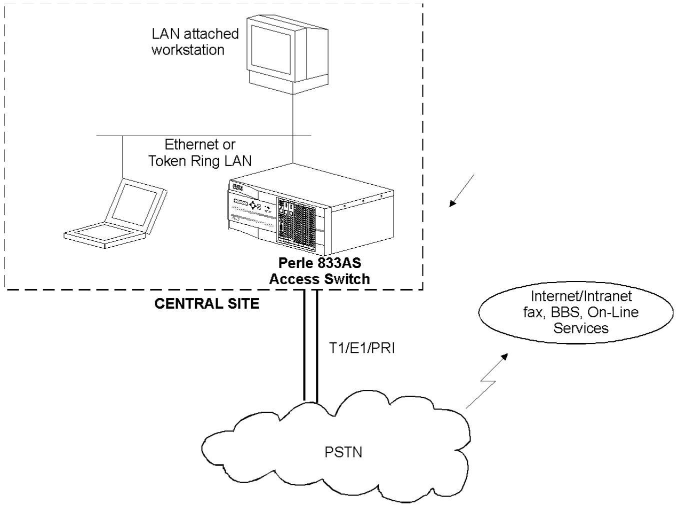
The network protocol, AppleTalk, and the asynchronous protocol, Apple Remote Access (ARA) are specific to the Apple network environment.

For messages originating from the Macintosh client, the routing client will encapsulate the AppleTalk protocol in an ARA frame. The Server will remove the ARA header, process the AppleTalk header, and based on the addressing information supplied at the protocol level will attach the appropriate MAC header. The frame is then forwarded to the LAN.

For messages coming from the LAN and intended for a Macintosh client, the Perle Server will remove the MAC header, process the AppleTalk headers and based on the addressing information at the protocol level, forward the frame to the appropriate Macintosh client by encapsulating the message within an ARA frame.

Dial-Out Access

With Perle Dial-Out Client software, LAN attached PCs can use the PerleDSP Modem and lines of the 833AS as Dial-Out modems. To the PC application, the PerleDSP Modem and line attached to the 833AS look like a modem connected to the PC COM port. Most PC applications that require a modem are supported. With appropriate software, users can connect to a BBS, Internet provider, or any other service accessible by the telephone network. When used with WinFax Pro, users can send faxes from their PC.


LAN attached workstation
Ethernet or Token Ring LAN
Perle 833AS Access Switch
CENTRAL SITE
T1/E1/PRI
Internet/Intranet fax, BBS, On-Line Services
PSTN

The Dial-Out client communicates with the 833AS using IP or IPX protocol. When the Dial-Out client starts, it broadcasts a message on the network to discover what 833AS Servers are available for Dial-Out. Each Server capable of handling the request will respond to the client. For each Server, a list of lines that can be used for Dial-Out are displayed.

The 833AS works with the Dial-Out client to emulate an external modem connected to a COM port at the PC. This is supported using the following interfaces:

DOS

- INT14
- Novell NASI/NACI

Windows 3.x/95/98/NT

- Windows Communication Interface (COM port redirection)

Dial-Out will use the internal PerleDSP Modems of the 833AS and a channel of the line on the T1 or E1 interface. Although there are significant differences between making a call on a T1/E1 line and a standard phone line, the 833AS will make all the necessary conversions. The application on the Dial-Out PC issues standard "AT" commands. See “Appendix 2: AT Command Set” on page 251.

Configuration Overview

The 833AS is a very flexible Server and the Manager allows you to fully exploit this potential. To simplify the configuration process, the Manager has been designed with intelligent defaults that will meet the needs of the majority of installations. These defaults are provided for most parameters that must be configured. Any configurations that you need or want to make must be made within a Configuration File.

For all installations, you *must* configure:

- Feature Cards installed in your 833AS.
- Server name.
- Server password.
- Date and time.
- T1/PRI or E1/PRI line parameters.

For all installations, you can *optionally* configure:

- SNMP parameters.
- Groups.
- LAN-to-LAN connections.

For Dial-In, you *must* configure:

- Parameters for the protocols that you will use.
- User records.
- Security parameters.

For Dial-Out, you *must* configure:

- Dialout parameters.
- Server IP or IPX parameters.

Using Configuration Files

The Configuration file contains all the system and user configurations for the 833AS. Once a file has been created, it can be used to set the configuration for one Server or as a base for any number of Servers. The User Database portion of the configuration can be treated independently from the system configuration.

Configuration files have the file extension **.rcf**. User Database files have the file extension **.rus**.

Creating

To create a new configuration file:

1. From the Manager **File** menu, select **New**.
2. The **Configuration File** window will appear.

Opening

To open an existing configuration file:

1. From the Manager **File** menu, select **Open**.
2. Select the **Configuration file** from the file list and click "**OK**".
3. The **Configuration File** window will display the selected file.

Uploading

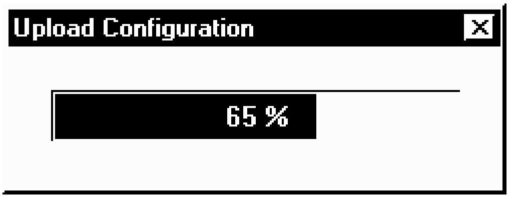
To upload a configuration:

1. From the Manager **File** menu, select **Server List**.
2. The **Server List** window appears. Select an 833AS from the list.
3. The **Log On** dialog box appears. Enter a **User ID** and **Password**, and click **OK**. The User must have administrative privileges to proceed.

*The default administrative name for an unconfigured 833AS is: User ID: **superusr**, no password.*

4. From the Manager **Configure** menu, select **Get Configuration**. Or, click the **Get Configuration from the Server** quick button.

5. The configuration will be uploaded from the server. The following dialog box will be displayed showing the upload progress:



6. The **Configuration File** window will display the uploaded configuration file.

Saving

The configuration file should be stored on the Manager PC for backup.

To save the configuration file:

1. From the Manager **File** menu, select **Save**.
   - If the configuration file already exists, the changes will be saved to the existing file.
   - If the file is new, enter a file name for the new configuration, and click **OK**.
   - If you wish to create a copy of a configuration, from the Manager **File** menu, select **Save As**.

Downloading

The configuration file needs to be downloaded to the 833AS for the parameters to take effect.

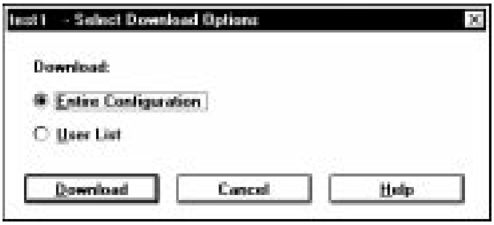
For system changes to take effect, the 833AS must be reset. If a Feature Card is reset, parameters related to that card only will take effect. A Feature Card reset will terminate any existing user sessions on that Feature Card. If a system reset is done, all sessions will be terminated.

As a rule, it is safest to reset the entire 833AS. However, if you have changed parameters on the T1, E1, or Line cards only, you can reset the related Feature Card. Changes to the user database will take effect immediately. However, if a user is disabled in the configuration and is currently dialed in, the user will not be disconnected.

To download a configuration:

1. Connect the Manager to the target 833AS.
2. Open the configuration file that you wish to download
3. From the **Configure menu**, select **Download Configuration**.

4. The **Download Configuration** dialog box appears. Click the radio button beside one of the following options:



Inst1 - Select Download Options

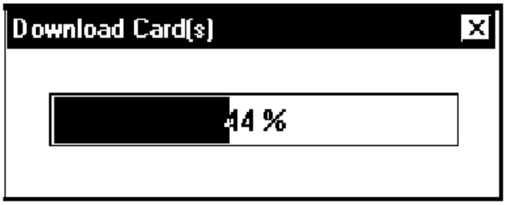
Download:

● Entire Configuration

○ User List

- **Entire Configuration:** The entire configuration (system and user) will be downloaded.
- **User List**: The user list will be downloaded.

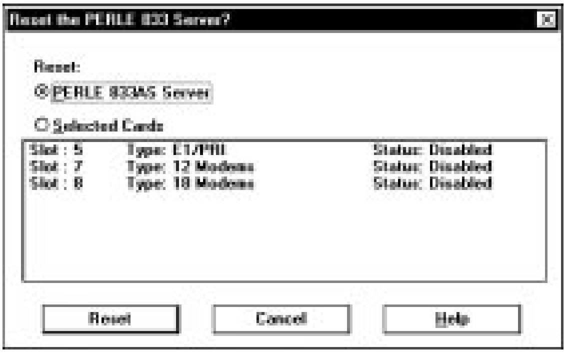
5. Click the **Download** button. The download will begin, and the following dialog box will appear:



Download Card(s)

44 %

6. When the download is complete, the **Reset** dialog box will appear if the entire configuration was downloaded.



Reset the PERLE 833 Server?

Reset:

● PERLE 833AS Server

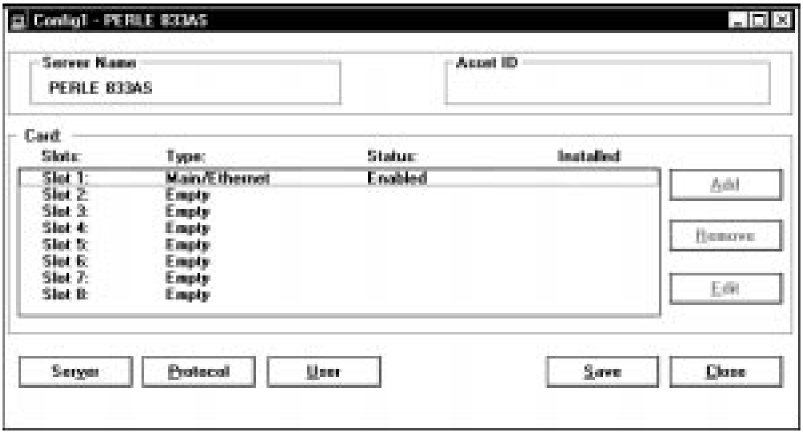
○ Selected Cards

```
Slot : 5      Type: E1/PRI          Status: Disabled
Slot : 7      Type: 12 Modems       Status: Disabled
Slot : 8      Type: 18 Modems       Status: Disabled
```

7. Select the **Feature Card** or the **System**. Click **OK.**

Configuration File Window

The Configuration File Window is the main window for the configuration facility of the Manager.



Config1 - PERLE 833AS

Server Name: PERLE 833AS

Asset ID:

Card

Slots:	Type:	Status:	Installed:
Slot 1:	Main/Ethernet	Enabled	
Slot 2:	Empty		
Slot 3:	Empty		
Slot 4:	Empty		
Slot 5:	Empty		
Slot 6:	Empty		
Slot 7:	Empty		
Slot 8:	Empty		

Server Name

The configured name of the Server. This name also appears in the Server List, and the Front Panel of the 833AS.

Asset ID

The configured Asset ID of the Server. This can be used to display a tracking identifier such as the serial number of the Server.

Card

This area displays information about the Feature Cards in this 833AS. It also is used to select a Feature Card to configure.

Slot

The slot of the Feature Card.

Type

The type of Feature Card installed in this slot.

Status

Indicates whether a Feature Card is enabled or disabled in configuration. It is valid for a Feature Card to be enabled in configuration but not be installed in the Server.

Installed

Indicates whether the Feature Card is installed in this slot.

Add

Adds a Feature card to the configuration.

Remove

Removes a Feature card from the configuration.

Edit

Edits the configuration of the currently selected Feature card.

Server

Provides settings for the entire server. See “Chapter 9: Configuring the Server” on page 173.

Protocol

Access the protocol settings. See “Chapter 7: Configuring the Protocols” on page 111.

User

Access the configuration for the User Database. See “Chapter 8: Configuring the User Database” on page 153.

Save

Saves the configuration.

Close

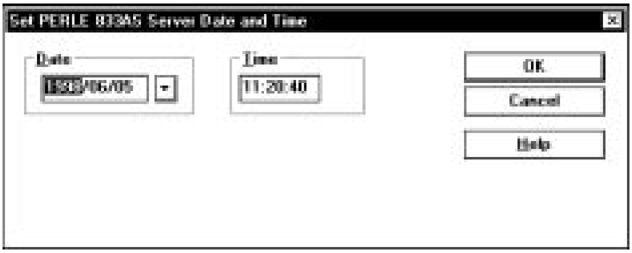
Closes the configuration file. If you have made changes, you will be asked if you want to save them.

Setting the Date and Time

The date and time is used to time stamp 833AS log messages.

To set the 833AS Server date and time:

1. From the **Configure** menu, select **Set Date and Time**. The following dialog box appears:



Set PERLE 833AS Server Date and Time

Date: 1999/06/05

Time: 11:20:40

2. Set the date and time, and click **OK**. The new date and time take effect immediately.

Chapter 6: Configuring the Feature Cards

About Configuring the Feature Cards

In this chapter, you will read about:

- Overview of Feature Card Configuration
- Feature Card Capacity
- Feature Card List
- Configuring the Ethernet Card
- Configuring the Token Ring LAN Card
- Configuring the T1/PRI Card or Dual T1/PRI Card
- Configuring the E1/PRI Card or Dual E1/PRI Card
- Configuring the PerleDSP Modem Cards

Overview

The 833AS has been designed to be a high performance modular platform for remote access. The base 833AS unit contains a System card which supports:

- 10Base-T/10Base2 10 Mbps Ethernet
- 100Base-TX 100 Mbps Ethernet

You can tailor your system to meet your needs by adding the appropriate Feature cards. The following feature cards are available for the 833AS:

T1/PRI Card

Provides a line interface to a T1 network. Can operate as a channelized T1 interface or an ISDN PRI interface.

Dual T1/PRI Card

Provides 2 line interfaces to a T1 network. Each interface can operate as a channelized T1 or ISDN PRI interface.

E1/PRI Card

Provides a line interface to an E1 network. Operates as an ISDN PRI or R2 CAS interface.

Dual E1/PRI Card

Provides 2 line interfaces to an E1 network. Each operates as an ISDN PRI interface.

Token Ring LAN Card

Provides an interface to a 4 or 16 Mbps Token Ring LAN network.

PerleDSP Modem Card

Provides multiple Central Site modems on a card. Each modem on the card supports:

- All standard modulations up to 33.6 Kbps
- K56Flex 56Kbps modulation
- V. 90 56 kbps modulation
- Class 2 Fax support

On power up, the 833AS automatically detects which Feature cards are installed. If a valid configuration has been defined for a Feature card, that card will be started.

The 833AS reports to the Manager which cards are installed, allowing you to determine which cards require configuration. If you are not connected to the 833AS that you are configuring (configuring off-line), you can add Feature cards to the configuration.

A card does not have to be installed to be configured. If you plan on adding Feature cards in the future, you can pre-configure them. This pre-configuration will have no adverse effect. When you receive the card, install it and power up the unit. The pre-configuration will be used and the card will be operational.

Feature Card Capacity

The number of Feature cards supported by the 833AS are as follows:

- System card - maximum 1 (installed with base unit)
- Token Ring LAN card - maximum 1
- T1/PRI card - maximum 4
- Dual T1/PRI card - maximum 2
- E1/PRI card - maximum 4
- Dual E1/PRI card - maximum 2
- PerleDSP12 or PerleDSP18 Modem card - maximum 5
- Perle 12, 18, 24 or 30 HD Modem Card

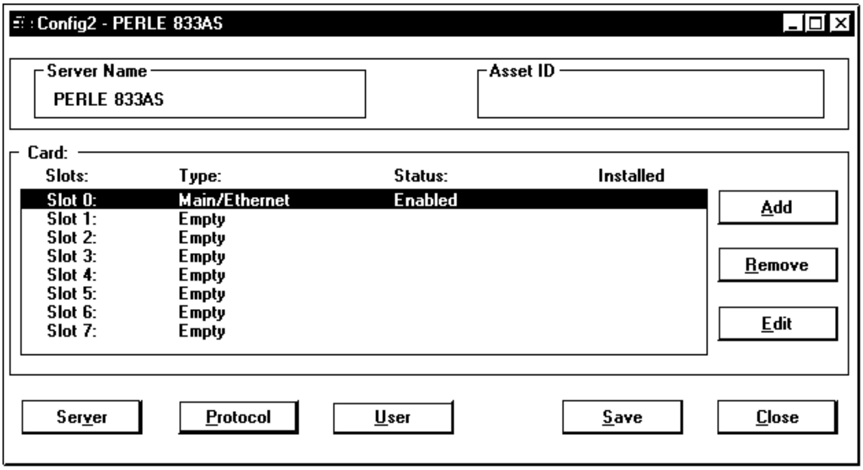
You can freely mix modem cards in a unit. Up to 5 modem cards can be used in an 833AS unit witha maximum of 120 modems. You typically will want to have one modem available for each channel that can receive an analog call. If you have more modems than channels, the extra modems will be added to the modem pool and used on a round robin basis.

You cannot mix T1/PRI cards with E1/PRI cards, but you can freely mix T1/PRI and dual T1/PRI feature cards or you can mix E1/PRI and dual E1/PRI cards as long as the total line interfaces does not exceed 4.

If you install a Token Ring LAN card, the Ethernet interface on the System card will be disabled.

Feature Card List

The Configuration File Window contains the Feature Card list.



Server Name: PERLE 833AS

Asset ID:

Card:

Slots:	Type:	Status:	Installed
Slot 0:	Main/Ethernet	Enabled	
Slot 1:	Empty		
Slot 2:	Empty		
Slot 3:	Empty		
Slot 4:	Empty		
Slot 5:	Empty		
Slot 6:	Empty		
Slot 7:	Empty		

The Card area displays information about the Feature cards in this 833AS. It is also used to select a Feature card to configure. The fields in the Card area are:

Slot

The slot of the Feature card.

Type

The type of Feature card installed in this slot.

Status

Indicates whether a Feature card is enabled or disabled in configuration.

Installed

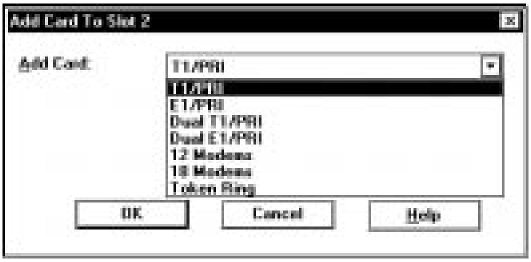
Indicates whether a Feature card is installed in this slot.

If the Manager is currently attached to the 833AS being configured, the Card list will display all cards detected by the 833AS as well as any slots that have Feature card configurations. If the Manager is off-line, the Card list will be based on Feature card configurations only.

Adding

To add a new Feature Card to the Manager:

1. In the **Card** area, highlight the slot where you wish to install the card. Click **Add**.
2. The **Add card** dialog box will display. From the drop menu, select the card that you wish to add. Click **OK.**



Add Card To Slot 2

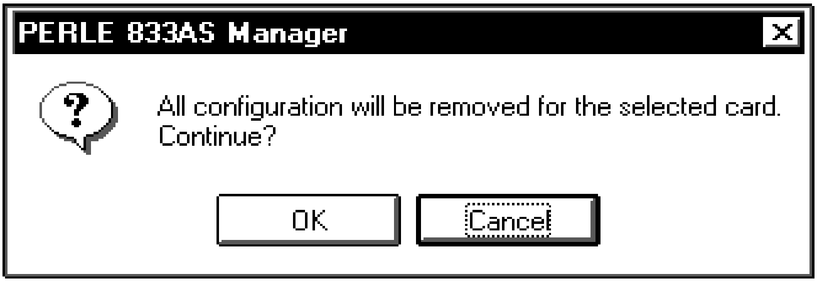
Add Card: T1/PRI

The card is now added. The configuration screen for that card will appear. You can configure the card now, or click **Cancel** if you wish to configure it later.

Removing

To remove a Feature Card from the Manager:

1. In the **Card** area, highlight the card you wish to remove. Click **Remove**.
2. The following dialog box will display.



PERLE 833AS Manager

All configuration will be removed for the selected card. Continue?

3. Click **OK** to confirm. The configuration for the card is now removed.

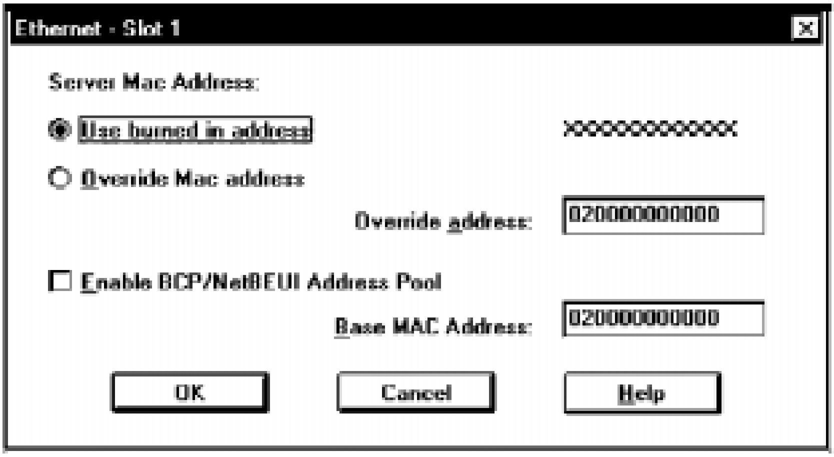
Editing

To Edit a Feature Card configuration on the Manager:

1. In the **Card** area, highlight the card you wish to edit. Click **Edit**.
2. The configuration screen for the card will appear.

Configure the Ethernet Card

The Ethernet card configuration screen is as follows:



Ethernet - Slot 1

Server Mac Address:

● Use burned in address XXXXXXXXXXXX

○ Override Mac address

Override address: 020000000000

□ Enable BCP/NetBEUI Address Pool

Base MAC Address: 020000000000

Server MAC Address

This specifies the MAC address used by the Ethernet interface for the server.

Use Burned In Address

The burned in MAC address was allocated from a range assigned to the 833AS. It is guaranteed to be unique from all other burned in MAC addresses. In most installations this address should be used.

Override MAC Address

If you wish to explicitly assign the MAC address, select Override MAC address, and enter the address in the field below. The address format is 12 character hex. This address will be restricted by the Manager to a Universally Administered Ethernet address. This address has bit 0 of the most significant byte set to 0, and bit 1 of the most significant byte set to 1. For example, addresses starting with 02, 06, 0A, 0E, 12, 16... are legal.

Enable BCP/NetBEUI MAC Address Pool

Certain protocols require that the 833AS emulate a LAN adapter, and supply a MAC address on behalf of the Dial In Client. This option allows you to define a pool of 64 MAC addresses, starting at the **Base MAC Address** defined below.

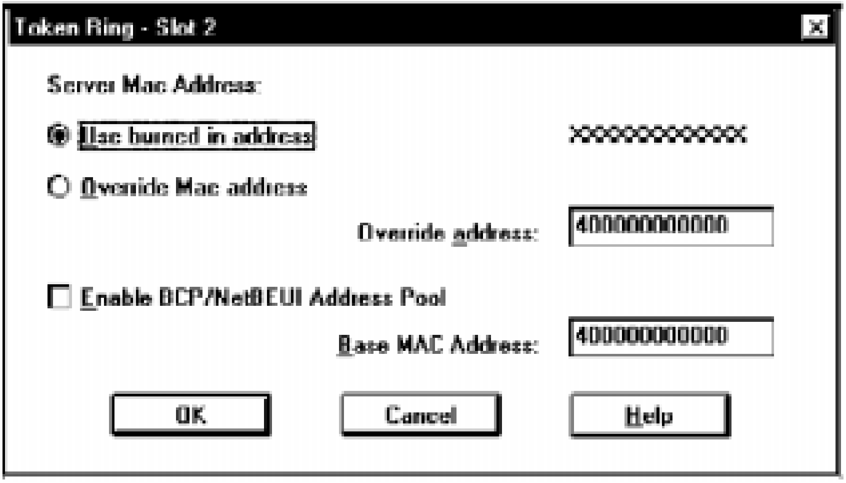
If you are using NetBEUI, you must enable this pool. For more details, see “Using NetBEUI” on page 151. If you are using BCP, the Client MAC address can be obtained from the User record or the pool. See “Configuring the Bridge Function (BCP)” on page 144 for more details.

Base MAC Address

This is the base address for the MAC Address Pool. The address is a 12 hex digit value that ends in 00. The legal values are 020000000000 to 02FFFFFFFF00 for Ethernet. You can use the default provided from a special manufacturer's range. However, all Perle 833AS units share this default range, so the value should be changed if you are using multiple units on your network that have **Enable BCP/ Netbeui MAC Address Pool** enabled.

Configure the Token Ring Card

The Token Ring card configuration screen is as follows:



Token Ring - Slot 2

Server Mac Address:

● Use burned in address XXXXXXXXXXXX

○ Override Mac address

Override address: 400000000000

□ Enable BCP/NetBEUI Address Pool

Base MAC Address: 400000000000

Server MAC Address

This specifies the MAC address used by the Token Ring interface for the server.

Use Burned In Address

The burned in MAC address was allocated from a range assigned to the 833AS. It is guaranteed to be unique from all other burned in MAC addresses. In most installations this address should be used.

Override MAC Address

If you wish to explicitly assign the MAC address, select Override MAC address, and enter the address in the field below. The address format is 12 character hex. This address will be restricted by the Manager to a Universally Administered Token Ring address. This address has bit 7 of the most significant byte set to 0, and bit 6 of the most significant byte set to 1. The legal values are 400000000000 to 7FFFFFFFFFFF.

Enable BCP/NetBEUI MAC Address Pool

Certain protocols require that the 833AS emulate a LAN adapter, and supply a MAC address on behalf of the Dial In Client. This option allows you to define a pool of 64 MAC addresses, starting at the **Base MAC Address** defined below.

If you are using NetBEUI, you must enable this pool. For more details, see “Using NetBEUI” on page 151. If you are using BCP, the Client MAC address can be obtained from the User record or the pool. See “Configuring the Bridge Function (BCP)” on page 144 for more details.

Base MAC Address

This is the base address for the MAC Address Pool. The address is a 12 hex digit value that ends in 00. The legal values are 400000000000 to 40FFFFFFFF00 for Token Ring. You can use the default provided from a special manufacturer's range. However, all Perle 833AS units share this default range, so the value should be changed if you are using multiple units on your network that have **Enable BCP/ Netbeui MAC Address Pool** enabled.

Configure the T1/PRI or Dual T1/PRI Cards

Overview

A T1 line is a digital transmission link with a capacity of 1.544 Mbps. By using Time Division Multiplexing the line is split into 24 channels with one call occupying one channel. From the user perspective, each channel looks like an individual phone line with its own phone number.

For this application, a T1 line can be used as a channelized T1 line or a Primary Rate Interface (PRI) digital line.When operating as a channelized T1 line, a channel carries voice (analog) information. Digital information can be transmitted by using a modem to convert the data into analog.

Each channel of an ISDN PRI line can ideally carry 64Kbps of data. Voice or modem information can be transmitted on a channel by converting the voice into digital. Even though both ends of a connection may be using ISDN, it is possible that the carrier may route a connection through a channelized T1 link. This will reduce the maximum speed of the ISDN connection to 56Kbps. Note that this 56Kbps negotiation will automatically occur, and no special configuration will be required.

When a call is made on one of the T1 channels, it is signaled on the T1 line. This signaling emulates the dialing and answer sequence of a standard telephone. There are a number of different signaling schemes in use and you configure the 833AS to match the scheme that is used by your carrier. For a PRI ISDN connection, a T1 channel is dedicated solely for signaling.

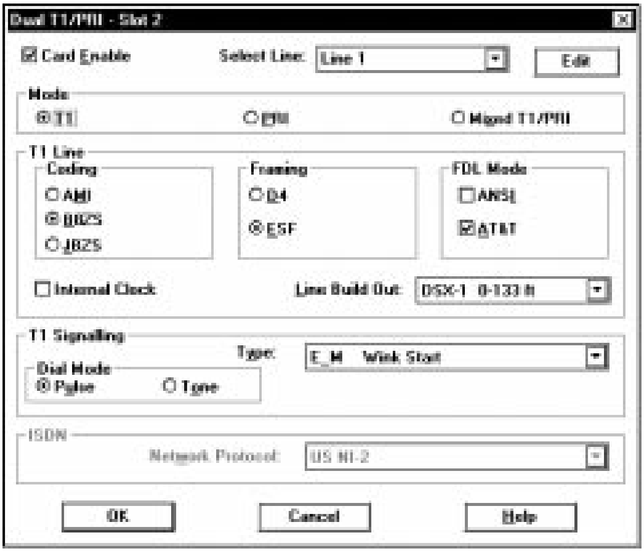
Network equipment attaches to a T1 line via a CSU. This unit provides line coding and conditioning functions as well as performing line diagnostics under the control of the phone network.

The T1/PRI Feature Card has a CSU built in. However, an external CSU can be used by operating the card in DSX-1 mode. An external CSU isolates the T1 line from the 833AS and keeps the line from causing Central Site alarms to be activated if the 833AS is powered off. Selecting CSU/DSX-1 mode is done with the Line Build Out setting on the T1/PRI configuration - no hardware settings are required.

The Dual T1/PRI Feature Card is effectively 2 T1/PRI feature cards integrated into one.

Dual T1/PRI Configuration

Prior to configuring the T1/PRI parameters on a Dual T1/PRI feature card, you must select the line on the card that you are configuring.



Dual T1/PRI - Slot 2

☑ Card Enable

Select Line: Line 1

Mode

● T1 ○ PRI ○ Mixed T1/PRI

T1 Line

Coding

○ AMI

● B8ZS

○ JBZS

Framing

○ D4

● ESF

FDL Mode

☐ ANSI

☑ AT&T

☐ Internal Clock

Line Build Out: DSX-1 0-133 ft

T1 Signalling

Type: E_M Wink Start

Dial Mode

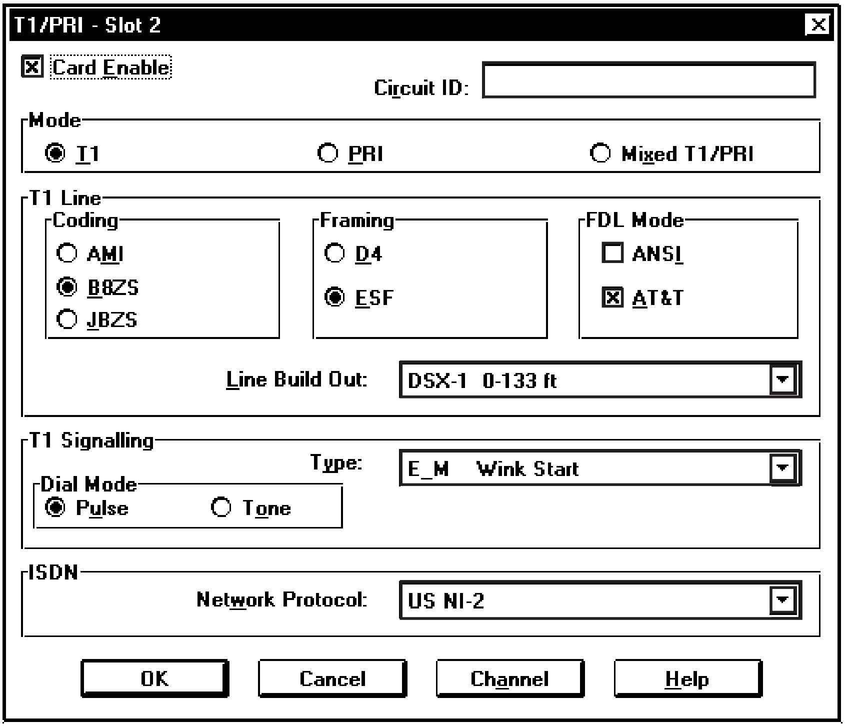
● Pulse ○ Tone

ISDN

Network Protocol: US NI-2

T1/PRI Configuration

The T1/PRI configuration screen is as follows These parameters apply to both the T1/PRI and Dual T1/PRI cards:



T1/PRI - Slot 2

☒ Card Enable

Circuit ID:

Mode: ● T1 ○ PRI ○ Mixed T1/PRI

T1 Line

Coding: ○ AMI ● B8ZS ○ JBZS

Framing: ○ D4 ● ESF

FDL Mode: □ ANSI ☒ AT&T

Line Build Out: DSX-1 0-133 ft

T1 Signalling

Type: E_M Wink Start

Dial Mode: ● Pulse ○ Tone

ISDN

Network Protocol: US NI-2

Circuit ID

This is an optional 16 character text field that can be used to describe or name the T1 line. This name will appear in the following locations:

- 833AS Front Panel
- SNMP DS1/T1 MIB, field dsx1Circuit Identifier

This field is for reference only. You do not have to match this field with the Circuit ID provided by the carrier.

Mode

This specifies the mode that the T1 line will operate.

T1

The line operates as a channelized T1 line with robbed bit signaling. The network will treat all calls as analog voice calls and modems are used to transfer the digital data. **T1 line** and **T1 Signaling** parameters must be configured for this mode.

PRI

The line operates as a Primary Rate Interface (PRI) ISDN line. The network will treat this as a digital line so that either ISDN digital calls or ISDN voice calls can be handled. If an ISDN voice call is used, modems are used to transfer the digital data. **T1 line** and **ISDN** parameters must be configured for this mode.

Mixed T1/PRI

Some carriers offer a service that allows a single T1 line to act as both a channelized T1 and as a PRI line. In this case, some channels of the T1 line operate as analog voice channels with robbed bit signaling and other channels operate as ISDN digital channels.

ISDN services often carry a price premium over channelized T1 services. For analog modems, ISDN offers no performance benefit over channelized T1. By allocating ISDN channels for ISDN digital calls only and T1 channels for the modem calls, you may save money. T1 line, T1 Signaling, ISDN and Channel parameters must be configured for this mode.

T1 Parameters

The following parameters are set for all **T1** modes:

Coding

Specifies the technique used to encode data bits on the T1 line. This information is provided by the carrier. The T1/PRI card supports these coding types:

- AMI (Alternate Mark Inversion). Also known as JB7 (Jam Bit 7).
- B8ZS (Binary 8 Zero Substitution)
- JBZS (Jammed Bit Zero Suppression)

Framing

The 24 channels of the T1 line are assembled into a frame. This parameter sets the frame format to be used. This information is provided by the carrier.

The T1/PRI card supports these framing types:

- D4 (Also known as Superframe or SF)
- ESF (Extended Superframe)

FDL mode

Facilities Data Link (FDL) allows the carrier to diagnose the operation of the line by requesting information and tests from the terminating equipment. The mode used should be supplied by the carrier.

These FDL modes are supported:

- ANSI
- AT&T

FDL is supported for ESF framing only. If you are using an external CSU, FDL is supported by the CSU.

Line Build Out

The Line Build Out is used to select between DSX-1 mode and CSU mode, and set the signal strength on the T1 connection. If you are using DSX-1 mode, set the value to the cable length between the 833AS and the CSU. If you are using CSU mode, ask your carrier to provide the value. Values are as follows:

- DSX-1 0-133 ft.
- DSX-1 133-266 ft.
- DSX-1 266-399 ft.
- DSX-1 399-533 ft.
- DSX-1 533-655 ft.
- CSU 0 dB
- CSU -7.5 dB
- CSU -15 dB
- CSU -22.5 dB

T1 Signaling

The following parameters must be set for **T1** and **Mixed T1/PRI** mode.

Type

Specifies the technique used for robbed bit signaling. With robbed bit signaling, the physical connections used for on hook, off hook and ringing are simulated using bits in the T1 datastream. There are different techniques for doing this. The **Type** matches the type of robbed bit signaling specified by your carrier.

The following **Types** are supported:

- E & M Immediate Start
- E & M Delay Start
- E & M Wink Start
- FXS Ground Start
- FXS Loop Start
- SAS Ground Start
- SAS Loop Start

Dial Mode

The following Dial modes are supported for Dial Out and Callback:

- Pulse: Using robbed bit signaling, dial out and callback calls are done by emulating pulse dialing.
- Tone: The modem assigned for the session dials the call using DTMF (Dual Tone/Multi-Frequency) tones. This can result in quicker call setup times than with pulse dial.

When using the Dial-Out feature, the call will be dialed out using the mode set here regardless of the AT command (ATDT or ATDP) used.

This setting has no effect on dial in calls.

Internal Clocking

Normally, the T1 clocking is derived from the telco line. However, in some cases (for example, if you are connected to proprietary equipment), you may want to have the 833AS generate the signal clocking. This can be done by enabling this option.

If this is enabled for 1 card, it will be enabled for all line cards.

ISDN

The following parameter must be set for PRI and Mixed T1/PRI mode:

Network Protocol

Specifies the network protocol used by the carrier. These network protocols are supported:

- US NI-2
- AT&T 4ESS
- AT&T 5ESS
- Northern Telecom DMS 100
- Northern Telecom DMS 250
- Japan INSNet 1500

Channel

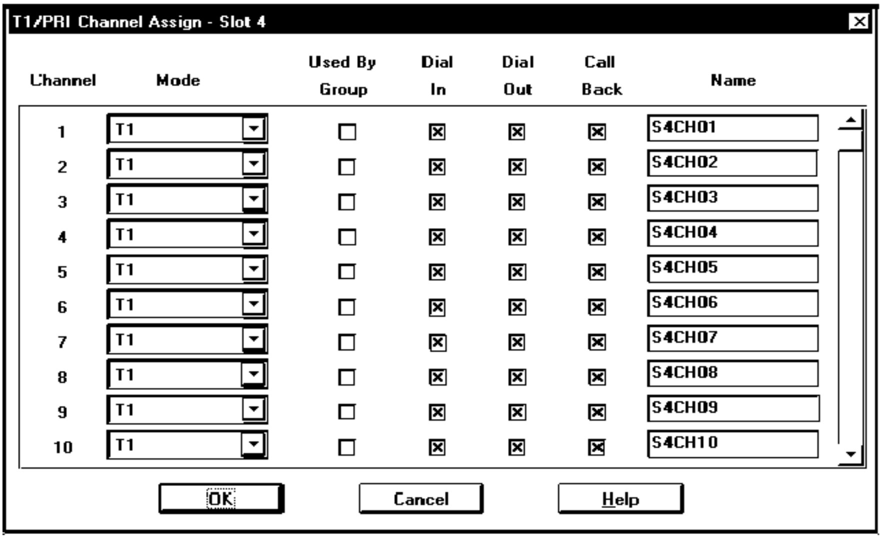
These capabilities of individual channels of the T1 line can be set:

- Enable/disable the channel.
- Enable/disable dial in, dial out or callback for this channel.
- Set channel as ISDN, ISDN digital or channelized T1.
- Specify a name for this channel.

Unless you have specified Mixed T1/PRI mode, it is not necessary to change these settings. The defaults will set all channels to enable dial in, dial out and callback, and default channel names will be created. If you specify Mixed T1/PRI mode, use the Mode setting on this screen to select which channels will be used for T1 and which channels will be used for ISDN.

If T1 mode is set, settings will be available for channels 1-24. If PRI or Mixed T1/PRI mode is set, channel 24 will not be displayed. This is because channel 24 is dedicated to the ISDN signaling channel.

The following channel parameters may be set:



T1/PRI Channel Assign - Slot 4

Channel	Mode	Used By Group	Dial In	Dial Out	Call Back	Name
1	T1	□	☒	☒	☒	S4CH01
2	T1	□	☒	☒	☒	S4CH02
3	T1	□	☒	☒	☒	S4CH03
4	T1	□	☒	☒	☒	S4CH04
5	T1	□	☒	☒	☒	S4CH05
6	T1	□	☒	☒	☒	S4CH06
7	T1	□	☒	☒	☒	S4CH07
8	T1	□	☒	☒	☒	S4CH08
9	T1	□	☒	☒	☒	S4CH09
10	T1	□	☒	☒	☒	S4CH10

Mode

- *T1*: Channel is set as a T1 voice channel. Incoming calls will be processed by the Modem card.
- *ISDN*: Channel is set as an ISDN bearer channel. Incoming ISDN digital calls will be processed by the PRI card, and incoming ISDN voice calls will be processed by the Modem card.
- *ISDN digital*: Channel is set as an ISDN bearer channel for digital calls only. Both ISDN digital and ISDN voice calls will be processed by the PRI card as digital calls.

  Some carriers offer an ISDN voice only service at a lower cost than an ISDN digital service. With this service all calls will be presented to the terminating equipment as voice calls even if they originated as digital calls. This setting forces all calls to be treated as digital calls regardless of how they originated.
- *Disabled*: Channel is disabled. Incoming calls on this channel will not be processed and this channel will not be used for dial out or callback.

If you have ordered a T1 line with fewer than 24 channels or a PRI line with fewer than 23 bearer channels, disable the unused channels.

Group

This is a display only field. This field will be checked if you have defined a group that includes this channel. A channel assigned to a group has the dial in, dial out and callback attributes defined by the group. For more information, see “Group Settings” on page 193.

Dial In

When checked, channel will accept dial in calls.

Dial Out

When checked, channel is available for dial out calls.

Call Back

When checked, channel is available for call backs.

Name

Name of the channel. This name is for reference only and will appear in the following places:

- 833AS Manager Statistics
- 833AS Front Panel

Maximum length is 16 characters. The default name is automatically generated as SxCHy, where x = slot number of the T1/PRI card, and y = channel number.

Configuring the E1/PRI and Dual E1/PRI Feature Cards

Overview

An E1 telephone line supports up to 30 telephone calls on a single physical line. By using Time Division Multiplexing, the line is split into 32 channels with one call occupying one channel. From the user perspective, each call carrying channel (known as a bearer channel) looks like an individual phone line with its own phone number.

The 833AS E1/PRI supports an E1 line that operates as a PRI ISDN or R2 CAS connection.

The Dual E1/PRI Feature Card is effectively 2 E1/PRI integrated into one.

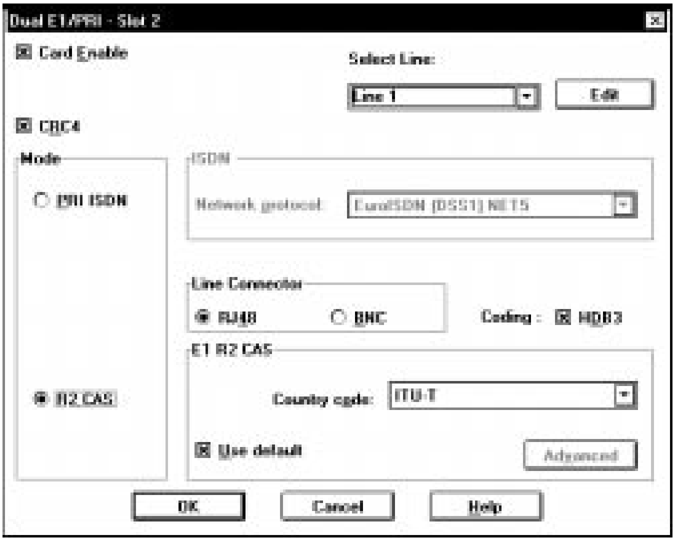
Network equipment attaches to an E1 line via a CSU. This unit provides line coding and line conditioning functions as well as performing line diagnostics under the control of the phone network. This CSU will typically be supplied by the carrier.

This feature allows the 833AS to function in channelized E1 networks which uses R2 CAS Signalling. The 833AS supports the ITU/CCITT Recommendations Q.4xx for E1 R2 CAS. this is the default mode. Different countries implement variants of the R2 signalling protocol. This release also supports the China variant.

R2 CAS consists of two components - Line Signalling and MFC (Multi Frequency Code) inband signalling. This Line signalling is sent on a dedicated signalling channel (channel 16). This is used to signal to the telephone network on/off hook, hang-up, and other line conditions. MFC signalling (tone frequencies) is sent inband on the individual channels to exchange the calling digits, billing information and other call specific information.

Dual E1/PRI Configuration

Prior to configuring the E1/PRI parameters on a Dual E1/PRI feature card, you must select the line on the card that you are configuring.



Dual E1/PRI - Slot 2

☒ Card Enable

Select Line: Line 1

☒ CRC4

Mode

○ PRI ISDN

● R2 CAS

ISDN

Network protocol: EuroISDN (DSS1) NET5

Line Connector

● RJ48 ○ BNC

Coding : ☒ HDB3

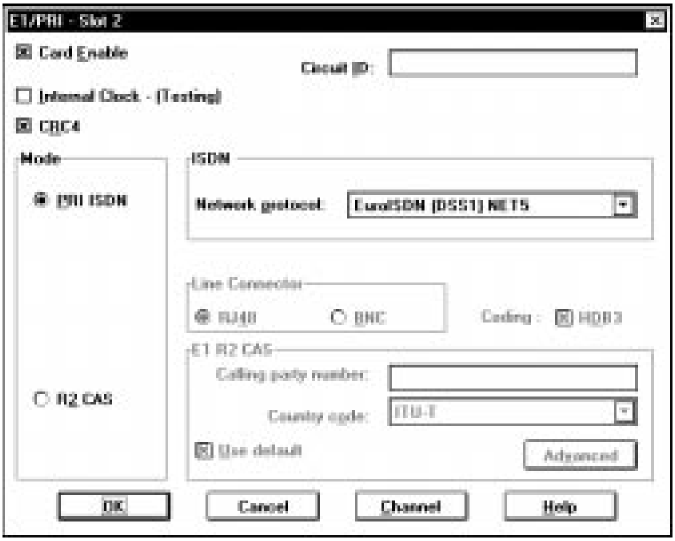
E1 R2 CAS

Country code: ITU-T

☒ Use default

E1 Parameters

The following parameters are set for E1:



E1/PRI - Slot 2

☒ Card Enable

Circuit ID:

□ Internal Clock - (Testing)

☒ CRC4

Mode

● PRI ISDN

○ R2 CAS

ISDN

Network protocol: EuroISDN (DSS1) NET5

Line Connector

● RJ48 ○ BNC

Coding : ☒ HDB3

E1 R2 CAS

Calling party number:

Country code: ITU-T

☒ Use default

Circuit ID

This is an optional 16 character text field that can be used to describe or name the E1 line. This name will appear in the following locations:

- 833AS Front Panel.
- SNMP DS1/E1 MIB, field dsx1CircuitIdentifier.

This field is for reference only. You do not have to match this field with the Circuit ID provided by the carrier.

Coding

Specifies the technique used to encode data bits on the E1 line. This information is provided by the carrier. The user can enable or disable HDB3 (High Density Bipolar 3) coding.

Framing

The 32 channels of the E1 line are assembled into a frame. This parameter sets the frame format to be used. This information is provided by the carrier.

The E1/PRI card supports these framing types:

- CRC4
- No-CRC4

Internal Clocking

Normally, the E1 clocking is derived from the telco line. However, in some cases (for example, if you are connected to proprietary equipment), you may want to have the 833AS generate the signal clocking. This can be done by enabling this option.

If this is enabled for 1 card, it will be enabled for all line cards.

ISDN

The following parameters must be set:

Network Protocol

Specifies the network protocol used by the carrier.

These network protocols are supported:

- EuroISDN ETSI NET5
- 1TR6

Channel

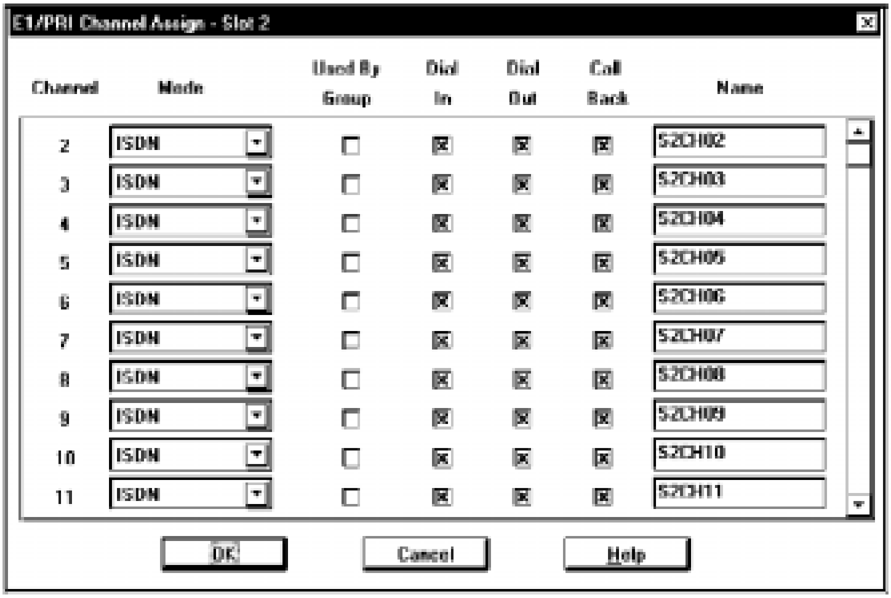
These capabilities of individual channels of the E1 line can be set:

- Enable/disable the channel.
- Enable/disable dial in, dial out or callback for this channel.
- Set channel as ISDN or digital ISDN.
- Specify a name for this channel.

It is not necessary to change these settings. The defaults will set all channels to enable dial in, dial out and callback, and default channel names will be created.

The ISDN signaling channel will appear in this list but will have the settings disabled.

The following channel parameters may be set:



E1/PRI Channel Assign - Slot 2

Channel	Mode	Used By Group	Dial In	Dial Out	Call Back	Name
2	ISDN	□	☒	☒	☒	S2CH02
3	ISDN	□	☒	☒	☒	S2CH03
4	ISDN	□	☒	☒	☒	S2CH04
5	ISDN	□	☒	☒	☒	S2CH05
6	ISDN	□	☒	☒	☒	S2CH06
7	ISDN	□	☒	☒	☒	S2CH07
8	ISDN	□	☒	☒	☒	S2CH08
9	ISDN	□	☒	☒	☒	S2CH09
10	ISDN	□	☒	☒	☒	S2CH10
11	ISDN	□	☒	☒	☒	S2CH11

Mode

- *ISDN*: Channel is set as an ISDN bearer channel. Incoming ISDN digital calls will be processed by the PRI card and incoming ISDN voice calls will be processed by the Modem card.
- *ISDN Digital*: Channel is set as an ISDN bearer channel for digital calls only. Both ISDN digital and ISDN voice calls will be processed by the PRI card as digital calls. Some carriers offer an ISDN voice only service at a lower cost than an ISDN digital service. With this service, all calls will be presented to the terminating equipment as voice calls even if they originated as digital calls. This setting forces all calls to be treated as digital calls regardless of how they originated.
- *Signal*: Channel was set as the ISDN signaling channel on the main E1/PRI screen. Bearer channel settings (mode, dial in, dial out, and callback) do not apply and are disabled for this channel.
- *Disabled*: Channel is disabled. Incoming calls on this channel will not be processed and this channel will not be used for dial out or callback.

If you have ordered a PRI line with fewer than 30 bearer channels, disable the unused channels.

Group

This is a display only field. This field will be checked if you have defined a group that includes this channel. A channel assigned to a group has the dial in, dial out and callback attributes defined by the group. For more information, see “Group Settings” on page 193.

Dial-In

When checked, the channel will accept dial in calls.

Dial-Out

When checked, channel is available for dial out calls.

Call Back

When checked, channel is available for call backs.

Name

Name of the channel. This name is for reference only.

It will appear in the following places:

- 833AS Manager statistics
- 833AS Front Panel

Maximum length is 16 characters. The default name is automatically generated as SxCHy, where x = slot number of the E1/PRI card, and y = channel number.

R2 CAS

Calling Party Number

This is the phone number of the calling party.

Country Code

Two variants or the R2 CAS signalling protocol are available - ITU or China.

Use Default

There are some advanced “country specific” parameters used by R2 CAS. The default values for these parameters are set to work in the specified country. Most of the time the user does not need to change these parameter values. The user should be familiar with the ITU/CCITT Recommendations Q.4xx and the National specifications for R2 CAS Signalling before changing these values. If there is a special requirement to change these parameters, click **Use defaults** off and go to the **Advanced** menu.

Internal Clock

In most situations, the telephone network will provide the clock source for receiving and transmitting data. In some special cases, the 833AS may be required to provide the clock source. This feature can also be used in conjunction with a loopback cable to verify that the E1 interface is functional.

Line Connection

Two types of physical connectors can be used to connect the 833AS to the telephone network, the 120-ohm RJ-48 or the unbalanced 75-ohm BNC. A special cable is required to attach to a BNC network.

Advanced Menu

Answer signal code (1 to 15) and Answer signal group (Group A or Group B)

- Answer signal to be used. The default is Group B, signal 1.

DNIS Maximum (5-64) and Minimum (0-64) digits

- Requested number of DNIS digits for each call. All calls that do not match the minimum and maximum settings that you specify will be dropped. The defaults are 7 and 4.

Cab signal (1-15)

- Specifies the Cab signal code. Default is 1.

KD Signal (1-15)

- Specifies the Chat signal code. Default is 1.

NC congestion signal code (1-15) and NC congestion signal group (Group A or Group B)

- Specified the noncomplicated congestion signal and group. This signal is sent to the central office when the 833AS is congested and cannot accept a call. The default is Group B, signal 4.

Channel

In R2 CAS, the individual channels must be configured as per your subscription:

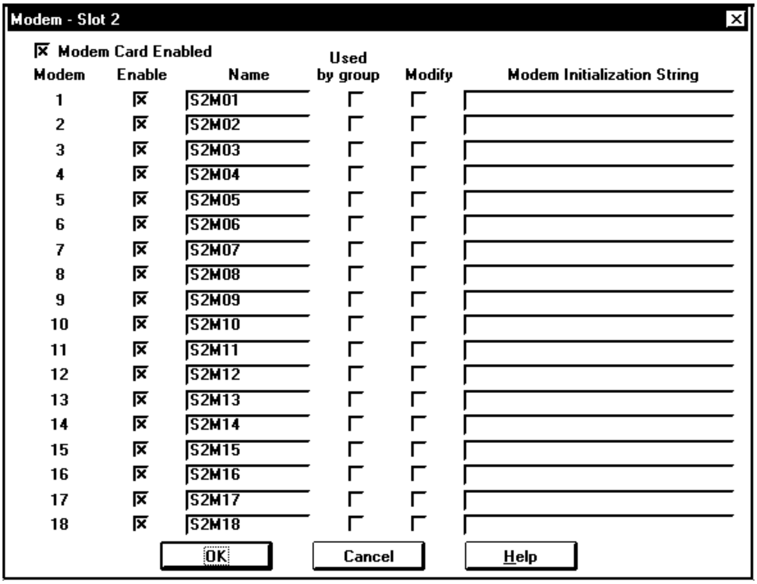
Incoming Only	Only accepts calls coming in from the telephone network
Outgoing Only	Only allows calls out to the telephone network
Both	Allow this channel to accept calls and allow outgoing calls
Disabled	Do not use this channel

Configuring the PerleDSP Modem Cards

No configuration is necessary for the modem card to operate in the 833AS. The modem configuration screen allows you to:

- Disable a modem on the card.
- Change the name of the modem from the default name.
- Customize the modem initialization string.

PerleDSP modem card screens have identical fields. The following parameters can be set:



Modem - Slot 2

☒ Modem Card Enabled

Modem	Enable	Name	Used by group	Modify	Modem Initialization String
1	☒	S2M01	□	□	
2	☒	S2M02	□	□	
3	☒	S2M03	□	□	
4	☒	S2M04	□	□	
5	☒	S2M05	□	□	
6	☒	S2M06	□	□	
7	☒	S2M07	□	□	
8	☒	S2M08	□	□	
9	☒	S2M09	□	□	
10	☒	S2M10	□	□	
11	☒	S2M11	□	□	
12	☒	S2M12	□	□	
13	☒	S2M13	□	□	
14	☒	S2M14	□	□	
15	☒	S2M15	□	□	
16	☒	S2M16	□	□	
17	☒	S2M17	□	□	
18	☒	S2M18	□	□	

▲ PerleDSP Modem Card

Enable

Check to enable the modem. If you suspect that there is a problem with a particular modem, you can disable it by clearing the check box. The modem will then be removed from the modem pool.

Group

This is a display only field. This field will be checked if you have defined a group that includes this modem. A modem assigned to a group has the dial in, dial out and callback attributes defined by the group. For more information, see “Group Settings” on page 193.

Name

Name of the modem. This name is for reference only and will appear in the following places:

- 833AS Manager statistics.
- 833AS Front Panel.
- SNMP Modem MIB, field mdmIDProductDetails.

Maximum length is 16 characters. The default name is automatically generated as SxMy, where S = slot number of the Modem card, and y = Modem number.

Modify

Check this box if you wish to override the default modem initialization. You may wish to do this if you have users dialing in with old modems that cannot negotiate correctly with current modems.

Modem Initialization String

Enter the modem initialization string here. This string will be attached to the end of the default modem initialization. Please note that the base modem initialization will have reset the modem. It is not recommended that you do another modem reset (do not perform an AT&F), because there are additional parameters required for the correct operation of the 833AS. You should minimize the changes to only those items required for your environment. All commands must be valid AT commands as defined in Appendix 2.

Be very careful if you are overriding the default modem string. Setting this improperly could prevent the modem from receiving incoming calls entirely. It is strongly recommended that you place any modems with modified initialization into a separate modem group. See section see “Group Settings” on page 193.

The modem behaves differently from a stand-alone modem because it does not directly interface to the telephone line. Phone call handling is by the Line card (T1/PRI or E1/PRI). Once the call is established it is switched to the modem. Therefore, modem commands that do line control (such as ATA, ATH) are not handled solely by the modem. How they behave is dependent on the settings of the line card.

Chapter 7: Configuring the Protocols

About Configuring the Protocols

In this chapter you will read about:

- Overview of Protocol Configuration
- Configuring IP
- Configuring IPX
- Packet Filtering
- Configuring the Bridge Function (BCP)
- Configuring PPP
- Using Apple Remote Access (ARA)
- Using NetBEUI

Overview

The Perle833AS supports a variety of different communication protocols. The protocols are used on the communication line to transport data between different devices. Protocols in the 833AS are used for the following functions:

Networking

Protocols are used between the Dial-In client and service that the Dial-In client is accessing. Some examples of Networking protocols are:

- IP
- IPX
- NetBEUI
- AppleTalk
- Lantastic

The 833AS supports IP, IPX, NetBEUI and AppleTalk as routed protocols. Other protocols are handled by bridging. See “Client Handling” on page 74 for details.

WAN Transport

Protocols are used to transport data across the Dial in connection between the client PC and the 833AS or between the 833AS and a router on another LAN. These protocols are designed to optimize transmission across an asynchronous connection. The networking protocol is encapsulated within the WAN transport protocol. Protocols supported for WAN transport by the 833AS are:

- PPP
- ARA

833AS Management

Protocols are used between the 833AS Manager and 833AS. Protocols supported for managing the 833AS are:

- IP
- IPX

Protocol configuration is organized on a per-protocol basis. For example, all parameters related to IP are grouped on the IP screen, all IPX parameters on the IPX screen, etc. You will need to configure all protocols that you will be using. To simplify this task, defaults are provided wherever possible. If you are not using a protocol, you do not have to set up that configuration. However, the network traffic processed by a server can be reduced if you disable protocols not being used.

Since IP and IPX are used for management of the 833AS, you have to define the 833AS itself as a node on the IPX or IP network. This requires setting up IP or IPX address parameters for the 833AS itself.

Clients dialing into the 833AS require protocol addresses. This will typically be provided by the client. With IP, the 833AS can provide an IP address or an IP address can be assigned from an address server.

The 833AS can act as a Bridge. Bridging is used to transport protocols other than IP, IPX, NetBEUI and ARA. Most commonly, it is used to connect a PC to an IBM Mainframe or Midrange computer to get a 3270 or 5250 display session. Logical Link Control 2 (LLC2) protocol is used. Client software must support Bridge Control Protocol (BCP) for this function to work. Perle Remote Client software included with the 833AS supports BCP.

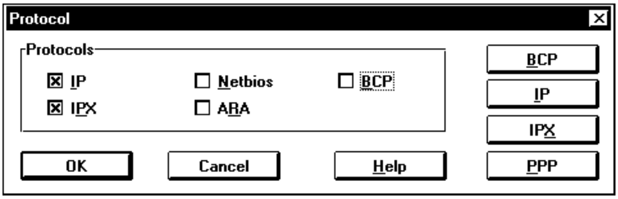
No configuration is required for ARA.

Configuring the Protocols

To configure the Protocols:

From the Configuration File window, click on **Protocol**

The **Protocol** screen appears. The fields are as follows:



Protocol

Protocols

☒ IP　□ Netbios　□ BCP

☒ IPX　□ ARA

Disable any **Protocols** that the server does not need to process. A protocol is disabled by removing the mark in the checkbox. Only the IP and IPX protocols are enabled by default.

Please note the following:

- If the **IP** or **IPX** protocol is disabled, then any other configuration item that uses this protocol will not be accessable.
- If a security feature that uses the **IP** or **IPX** protocol has already been configured, you will not be allowed to disable the protocol.

BCP

To configure **Bridge Control Protocol**, click the **BCP** button.

IP

To configure **IP**, click the **IP** button.

IPX

To configure **IPX**, click the **IPX** button.

PPP

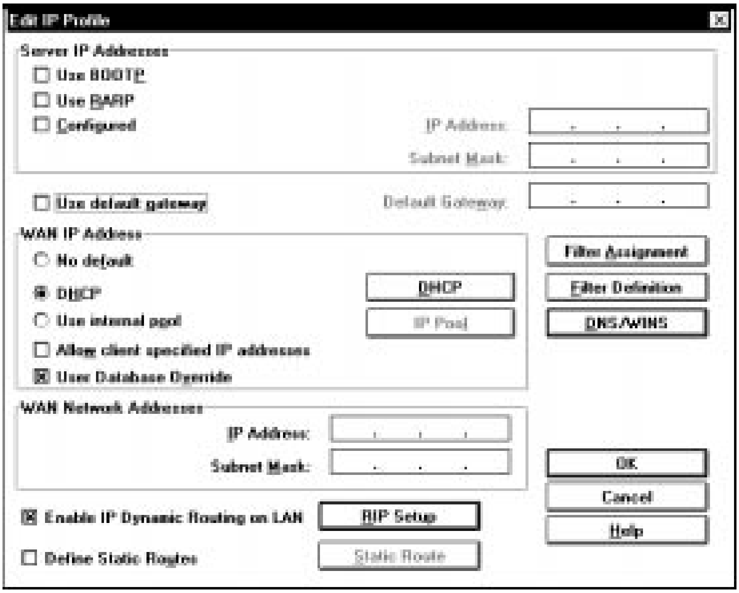
To configure **PPP**, click the **PPP** button.

Configuring IP

IP networks require devices to be configured with unique IP addresses. Depending on network topology, other parameters may have to be set. You will have to set up the IP parameters for the 833AS itself and establish IP parameters for the WAN client's dialing in to the 833AS.

Most organizations have a department or individual responsible for IP address management. Consult with them to get the correct values.

➲ The **Edit IP Profile** screen has the following settings:



Edit IP Profile

Server IP Addresses

☐ Use BOOTP

☐ Use RARP

☐ Configured

IP Address: . . .

Subnet Mask: . . .

☐ Use default gateway

Default Gateway: . . .

WAN IP Address

○ No default

● DHCP

○ Use internal pool

☐ Allow client specified IP addresses

☒ User Database Override

WAN Network Addresses

IP Address: . . .

Subnet Mask: . . .

☒ Enable IP Dynamic Routing on LAN

☐ Define Static Routes

Server IP Address

The Server requires an address that uniquely identifies the unit to the IP network. The Perle 833AS supports a number of ways of acquiring this IP address:

- You can configure an IP address.
- If you are managing your network IP addresses on either a BOOTP or RARP server, you can set the IP address there. The Perle833AS can acquire the IP address from a BOOTP or RARP server if it has been configured from within these servers. You will need the MAC address of the Perle 833AS to do this. This address can be obtained from the Front Panel.

Use BOOTP

When checked, the 833AS will attempt to acquire the Server IP address from a BOOTP server.

A DHCP (Dynamic Host Configuration Protocol) server that supports BOOTP may also be used. Many DHCP servers support BOOTP for the permanent assignment of addresses for servers on the network.

Use RARP

When checked, the 833AS will attempt to acquire the **Server IP** address from a RARP server.

Configured

When checked, the 833AS will use the IP address defined in the **IP address** and **subnet mask** fields.

IP Address

Enter a valid **IP address** in this field. See your IP Network Administrator for this information.

IP Subnet Mask

An IP network can be partitioned into subnetworks, or subnets. IP networks on a single LAN segment are not likely to have subnets defined. However, larger IP network with IP routers are likely to have subnets defined.

If your IP network has not been partitioned, the IP subnet mask will default to the correct value. If you have set up subnets in your IP network, set the mask as defined by the IP Network Administrator.

Use Default IP Gateway

When checked, lets the 833AS access external IP networks via a Default IP Router. Routers can be used to separate your IP network from external IP networks. It is common to have one router that provides a controlled link to these outside networks (such as the Internet). This router is known as the Default IP router. It also may be referred to as the Default router or Default gateway.

If you have enabled Use Default IP Gateway, enter the IP address of the router in this field. See your IP Network Administrator for this information.

WAN IP Address

Clients dialing in to the 833AS using the IP protocol need their own IP address. All clients are assigned IP addresses on the Internal WAN Network that has a subnet address distinct from the subnet address of the 833AS LAN port segment. The 833AS will packets between the LAN port segment and the Internal WAN Network. The Perle 833AS can manage the client IP addresses using a number of different schemes:

- You can define an internal pool of IP addresses in the 833AS. A user dialing in will be assigned an unused address from this pool.
- If your network uses a DHCP server to manage IP addresses, the 833AS can obtain an address for a dial in client from this server.
- The client dialing in can provide the IP address.
- You can configure an IP address for each user in the User database. If you are using an external user database that supports the configuration of IP addresses (such as RADIUS), the 833AS can use that address.
- You can use a pool or server to get the IP address but allow the user to override it if there is an address supplied by the user database or the client.

In all of the above cases, the IP addresses assigned to the dial in client must be within the range defined for the Internal WAN Network. See “WAN Network Address” on page 122 for more details.

The following parameters control the assignment of the WAN IP address:

No Default

Select **No default** if you do not want to assign a WAN IP address from the internal pool or a DHCP server.

DHCP

Select **DHCP** to use a DHCP server on your network to assign WAN IP addresses.

Use Internal Pool

Select **Use Internal Pool** if you wish to define an internal IP address pool. The IP address will be assigned from this pool.

Allow Client Specified IP Addresses

When checked, the client supplied IP address will be used if available. This address will override all other WAN IP addresses. (user database, internal pool or DHCP server).

User Database Override

When checked, the IP address will be supplied by the user database (internal or RADIUS) if it is configured for that user. This address will override WAN IP addresses supplied by the internal pool or DHCP server.

Be careful, as you can set these parameters so that some users dialing in will not be assigned an IP address. For example, if:

- there is no default source of IP addresses. (internal pool or DHCP)
- there is no IP address in the user's record.
- the client does not supply an IP address.

...there will be no IP address assigned and the connection will not be established.

DHCP

By default, the 833AS will look for all DHCP servers on the network. If you wish to configure the addresses of the DHCP servers or change the lease parameters, click on the **DHCP** button. For details on DHCP configuration, see the next section.

IP Pool

If you have selected **Use Internal Pool**, you must configure the IP Pool. To access the IP Pool configuration, click on this button. For details on IP Pool configuration, see “IP Pool” on page 119.

DNS/WINS

The 833AS can forward the address of a Domain Name Server (DNS) or Windows Internet Name Server (WINS) to a dial in client. If DHCP is enabled, the DHCP server can provide these addresses. You can also configure DNS and WINS addresses. If DHCP is not enabled, the 833AS will forward the configured values. To configure the DNS/WINS addresses, click on **DNS/WINS**. For details on DNS/WINS configuration, see “DNS/WINS” on page 121.

DHCP

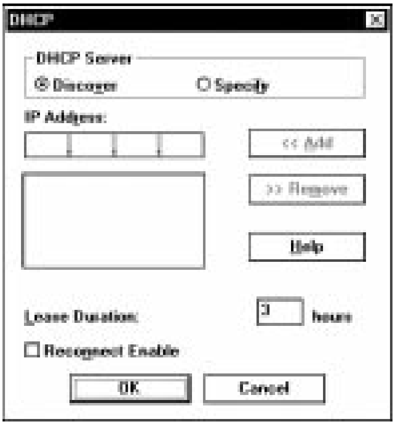
DHCP (Dynamic Host Control Protocol) permits the management of IP addresses and IP options from a centralized location. DHCP servers are used to assign addresses to devices that do not require a fixed IP address. When an IP address is required, the 833AS will request an address from the DHCP server. This address is used for the duration of the connection. This is referred to as an address *lease*.

If DHCP is enabled, the 833AS will give the dial in client an IP address that was leased from the DHCP server. When the 833AS leases an address from the DHCP server, it specifies the length of time of the lease. However, the 833AS will automatically renew the lease to make sure that the client does not lose the use of the address.

The 833AS cannot obtain its own IP address from the DHCP server using DHCP. However, most DHCP servers can act as a BOOTP server.

The DHCP server's address pool must consist of addresses belonging to the WAN Internal Network.

The DHCP configuration screen allows you to set the characteristics of DHCP support. The configuration screen is as follows:



DHCP Server: ● Discover ○ Specify

IP Address:

Lease Duration: 3 hours

☐ Reconnect Enable

DHCP Server

Discover

Select **Discover** to allow the 833AS to find any DHCP servers on the local network.

Specify

Select **Specify** to configure the IP addresses of the DHCP servers. Up to 4 DHCP server addresses can be configured.

IP Address

To add a DHCP server, enter the address in the **IP Address** field, and click **Add**.

To remove a DHCP server, highlight the address in the IP address list, and click **Remove**.

Lease Duration

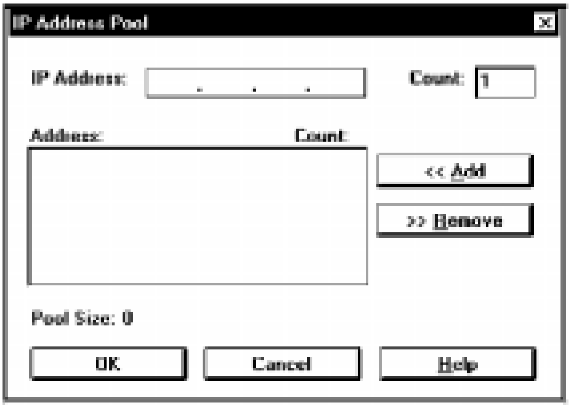
This field specifies the length of time that the DHCP server will allow the 833AS to use the leased IP address on behalf of the client. The range is 1 to 99 hours. Longer lease times will increase the chances that the client can reconnect to the 833AS and get the same IP address.

Reconnect Enable

Click on this check box to allow a dial in user to disconnect and then reconnect at a later time and retain the same leased IP address. This feature requires that all dial in users have a unique User ID. Note that if the client disconnects and the reconnect time expires, the lease will end. Also, if the lease expires, then another user may have been assigned that address.

IP Pool

You can set up a pool of IP addresses for dial in clients. The first available address will be assigned to the client when a client connects. Typically, you would want to have an IP address available for each simultaneous user that can dial in. The **IP Pool** screen is as follows:



IP Address Pool

IP Address: . . .

Count: 1

Address: Count:

Pool Size: 0

IP Address

The IP address field specifies the base address of a range of IP addresses.The count field specifies the number of addresses to be added, starting at the base.

To add IP addresses to the IP pool, enter the address in the **IP Address** field and count and click **Add**.

The address must be in the range xxx.xxx.xxx.001 through xxx.xxx.xxx.254. You must ensure that the IP addresses conform to the subnet mask set for the Internal WAN Network.

A maximum of 120 IP Addresses can be added.

Count

Specifies the number of addresses to be added, starting at the base address. If no count is specified, a count of one will be used. If the count would cause an illegal IP address to be generated (exceeding xxx.xxx.xxx.254), the count will be reduced to ensure that it is legal.

IP Pool display

Displays the base address and count for the IP Pool entries.

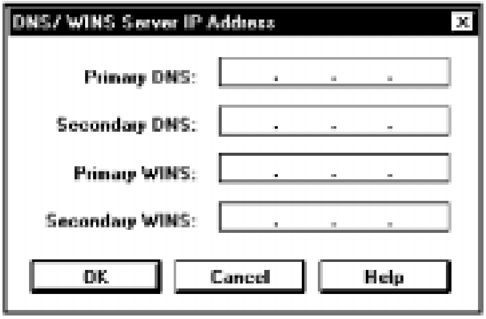
To remove IP addresses from the pool, highlight the entry in the **IP Pool** display and click **Remove**.

Pool Size

Displays the actual number of IP addresses that have been defined for the IP Pool. If this count is less than the number that you have entered, you have address ranges that overlap.

DNS/WINS

The 833AS can forward the address of a Domain Name Server (DNS) or Windows Internet Name Server (WINS) to a dial in client. If DHCP is enabled, the DHCP server can provide these addresses. You can also configure DNS and WINS addresses. If DHCP is not enabled, the 833AS will forward the configured values. The DNS/WINS configuration screen is as follows:



Primary DNS

Enter the **IP address** of the **Primary DNS** server. Blank indicates no Primary DNS server.

Secondary DNS

Enter the **IP address** of the **Secondary DNS** server. Blank indicates no Secondary DNS server.

Primary WINS

Enter the **IP address** of the **Primary WINS** server. Blank indicates no Primary WINS server.

Secondary WINS

Enter the **IP address** of the **Secondary WINS** server. Blank indicates no Secondary WINS server.

WAN Network Address

Clients dialing in to the 833AS must be assigned IP addresses on an Internal WAN Network. This section defines the Internal WAN Network used by the 833AS and should be completed after consulting with your IP Network Administrator. The address of this Internal WAN Network must be different from the address of the LAN segment network, although the Internal WAN Network may be a subnet of the LAN segment network.

IP Address

Enter the IP address that will be used by the 833AS on the Internal WAN Network.

Subnet Mask

Enter the subnet mask for the Internal WAN Network.

All dial-in client IP addresses, regardless of how they are acquired, must belong to the network defined by this IP Address and Subnet Mask.

Packet Filtering

The Packet Filtering feature allows the Perle 833AS Server to accept or reject incoming data packets that match an entry on a list of defined filters. The filters are based on *protocol* and *packet addresses*.

After the filters have been defined, up to 10 IP and/or 10 IPX filters can be assigned to the Perle 833AS or to each user or to both.

Filters will be used by the Perle 833AS Server in the following way:

1. The user record for the dial-in user will be checked. If the record has been configured to Disable Server Filters, then only the user assigned filters will be checked. Proceed to point 4.
2. Incoming data packets are compared with the filters assigned to the server starting with the first filter in the Server Filter Assignment list. As soon as the packet matches one of the filters, then the packet is accepted or rejected and no further checking is done.
3. If the packet does not match any of the filters assigned to the server, then the user record will be checked. If there are no user assigned filters, then the server default action will be carried out to accept or reject the packet and no further checks are done.
4. The incoming data packet will be compared to the filters assigned to the user, starting with the first filter in the User Filter Assignment list. As soon as the packet matches one of the filters, then the packet will be accepted or rejected.
5. If the packet does not match any user assigned filters, then the user default action will be carried out to accept or reject the packet.

Packet filtering works in conjunction with the **RADIUS** and **Shared User Database** security systems.

Shared User Database

Filters can be configured and assigned to a user record on the Remote Perle 833AS. These records will be sent to the Local Perle 833AS when a user dials in and makes a connection.

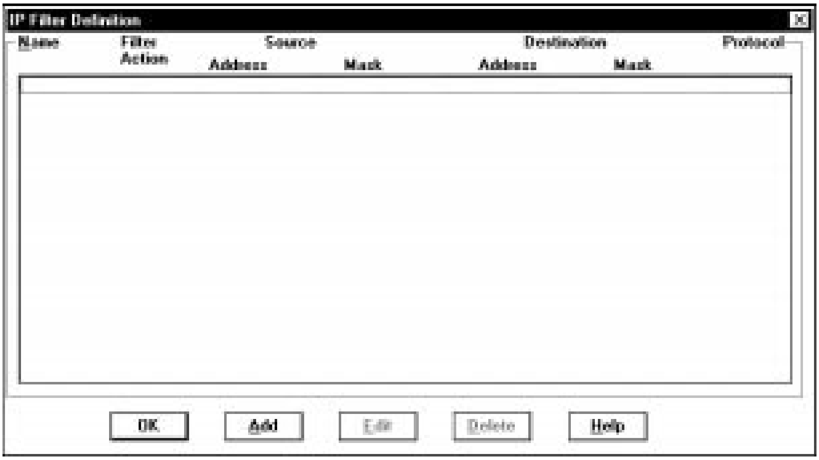
RADIUS

To use packet filtering with the RADIUS security server:

1. Define the filters on the Perle 833AS Server.
2. Configure the user record on the RADIUS server with the names of the filters to be assigned to the User.
3. When a user dials into the Perle 833AS, the name of the filters will be sent from the RADIUS server to the Perle 833AS.

Filter Definition

Up to 50 filters can be assigned for the IP protocol. IP filters can specify the Address, Mask, Sub-Protocol and Port of the IP packet. The filters can accept or reject incoming packets based on source and destination addresses. After you click the **Filter Definition** button in the **Edit IP Profile** window, the **IP Filter Definition** window appears. The fields are as follows:



Add

To add a filter defintion, click **Add**. The **Add IP Filter Defintion** window will appear. See “Add/Edit IP Filter Definition” on page 125 for details on how to create a filter definition.

Edit

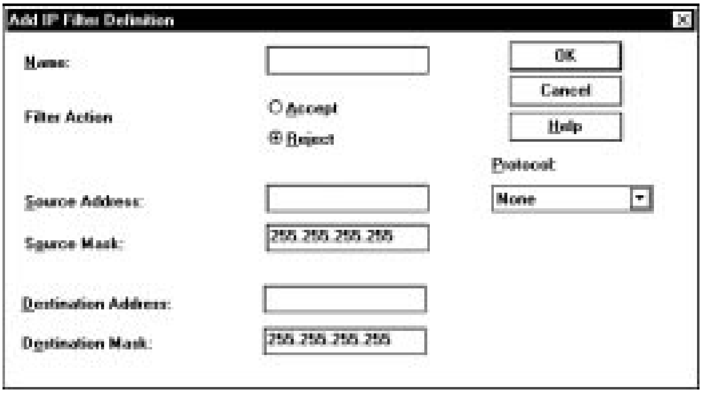
To edit a filter definition, select a filter from the list and click **Edit**. The **Edit IP Filter Definition** window will appear. See “Add/Edit IP Filter Definition” on page 125 for details on how to modify the filter definition.

Delete

To delete a filter definition, select a filter from the list and click **Delete**. The filter definition will be removed.

Add/Edit IP Filter Definition

To complete or modify the filter definition, enter the information in the following fields:



Add IP Filter Definition

Name:

Filter Action ○ Accept ● Reject

Source Address:

Source Mask: 255.255.255.255

Destination Address:

Destination Mask: 255.255.255.255

Protocol: None

Name

The filter name can be up to 8 characters in length. You will use the name to assign filters to the server or user. The name can also be used when adding filters to a user record on a RADIUS security server.

Filter Action

Select whether to **Accept** or **Reject** incoming IP packets if the packet matches all parameters defined in this filter. The default setting is **Reject**.

Source Address

This field is the IP address of the station that is sending the IP packet. The address should be entered in dotted decimal notation.

Source Mask

This feature masks off both the filter source address and the packet source address by using the Boolean AND function. If the two results are equal, then the address matches.

Destination Address

This field is the IP address of the station to which the IP packet is being sent. The address should be entered in dotted decimal notation.

Destination Mask

This feature masks off the filter destination address and the packet destination address by using the Boolean AND function. If the two results are equal, then the address matches.

Protocol

The entries in this pull-down list are TCP, UDP, ICMP, and Other.

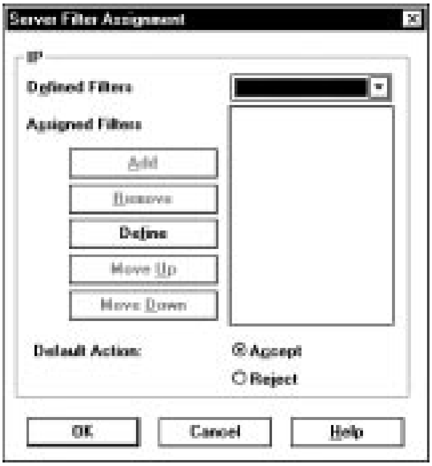
- If you select TCP or UDP, the Port Number section appears. Enter the Source and Destination in the corresponding fields.
- If you select Other, make an entry in the **Protocol** field.

Once you have entered the correct information, click **OK** to save your changes.

Filter Assignment

Up to 10 IP filters can be assigned to the server. The server will process these filters from the top down, so the order may be important. See "Packet Filtering" on page 123 for more details on how the filters are used.

To assign IP filters for the 833AS, click **Filter Assignment**. The **Server Filter Assignment** window appears. The fields are as follows:



Defined Filters

This is a pull-down list for previously defined packet filters.

Assigned Filters

This area can contain a list of up to 10 IP filters to be assigned to the 833AS for processing.

Add

Select a filter name from the Defined Filters pull-down list and click **Add** to add the filter to the Assigned Filters list.

Remove

You can delete a filter assignment by selecting a filter name from the Assigned Filters list and clicking the **Remove** button.

Define

If you need to define more filters, click the **Define** button. The **IP Filter Definition** dialog box appears.

Move Up, Move Down

You can change the order of the assigned filters by selecting a filter name from the Assigned Filters list and clicking the **Move Up** or **Move Down** buttons.

Default Action

Set the **Default Action** to be taken if a packet does not match any assigned filter. The choices are to **Accept** or **Reject**.

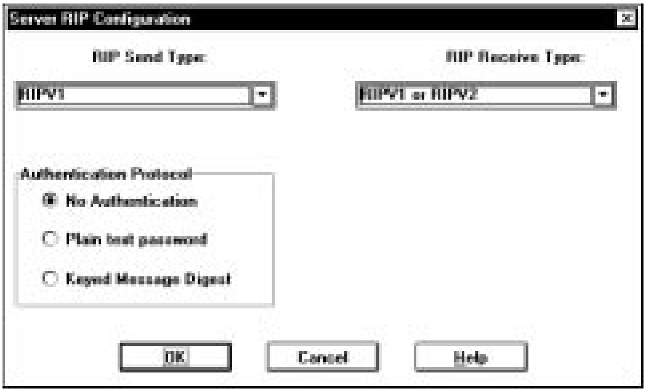
Enable IP Dynamic Routing

When checked, the 833AS will use the IP RIP table built from RIP messages received from other routers to determine how to route a message.

Server RIP Configuration

The 833AS supports both version 1 and version 2 RIP. To configure RIP properties, click **RIP Setup**.

The Server RIP Configuration screen has the following settings:



Server RIP Configuration

RIP Send Type: RIPV1

RIP Receive Type: RIPV1 or RIPV2

Authentication Protocol

● No Authentication

○ Plain text password

○ Keyed Message Digest

RIP Send Type

From the pulldown list select the type of RIPs to be sent over the LAN connection. The available choices are as follows.

■	No RIP	Do not send RIPs
■	RIPV1	Send version 1 RIPs
■	RIPV1 COMPATIBLE	Send version 2 RIPs (no multicasts) so as to be version 1 compatible

RIPV2	Send version 2 RIPs

RIP Receive Type

From the pulldown list select the type of RIPs to be received over and processed from the LAN connection. The available choices are as follows.

No RIP	Do not process received RIPs
RIPV1	Process received version 1 RIPSs
RIPV1 or RIPV2	Process received version 1 or version 2 RIPs
RIPV2	Process received version 2 RIPs

Authentication Protocol

If either the Send or Receive type RIP protocol chosen includes RIPv2, you have the option of choosing the form of authentication protocol to be used when processing RIPv2 messages. If RIPv2 is not being used at all then the Authentication Protocol defaults to the only valid selection which is No Authentication.

If RIPv2 is being used, you may decide to use either Plain Text Password authentication or Keyed Message Digest. If either of these options are selected, only the input fields for the chosen option will be displayed. You may also choose to have No Authentication when using RIPv2.

If you choose Plain Text Password authentication, two additional fields appear. You must enter the password into the first field and then confirm it in the second. The values typed into these fields are not displayed but rather asteriks are shown as keys are typed. The password can be up to 16 characters.

If you choose Keyed Message Digest authentication, you will have a list of five (5) keys that can be set. To set a particular key, highlight the key and press the Setup button.

WAN Port RIP operation operates in a similar fashion to the LAN ports, but can be individually configured for each WAN port (see user profile - “LAN to LAN”).

Define IP Static Routes

When checked, the 833AS will use the configured IP static routes table to determine how to route a message. If both dynamic and static routing are enabled, then both the IP RIP table and the configured IP static routes table will be used to route messages.

You may wish to enable static routes if:

- You have a very large local IP network
- RIP messages are not used to exchange network information. An example of this would be an IP network that used only OSPF.
- You have a defined a dial-on-demand LAN-to-LAN connection to a router on another network
- You have defined a LAN-to-LAN connection to a router on another network that does not use RIP.

Refer to the sections on IP Static Routing and LAN-to-LAN for more details.

IP Static Routing

When dynamic routing is enabled, the Perle 833AS knows the structure of connected networks (both the local network and those accessed through LAN-to-LAN connections) by receiving RIP messages from other routers and creates an IP RIP Table for the networks it knows about.

There is room in this table to keep entries for 500 routers. If there are more routers than this in the networks to which your 833AS is connected (both local and LAN to LAN), some of the RIP table entries will be overwritten and unavailable.

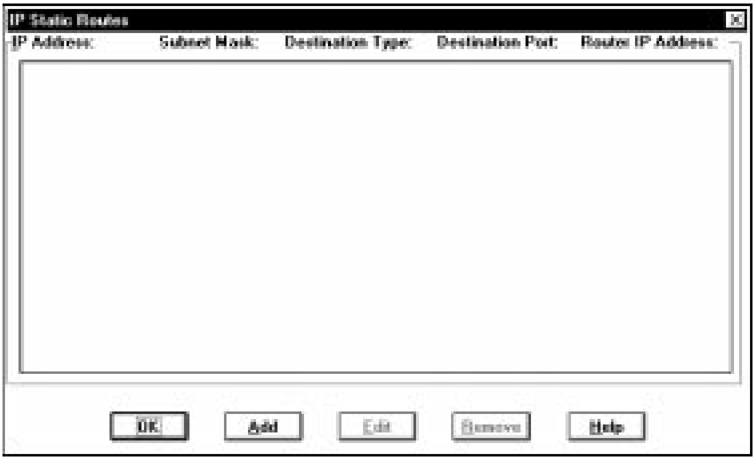
By defining IP static routes and disabling dynamic routing, the network administrator can configure the Perle 833AS with the addresses of only the routers needed to reach the desired routes and the Routing Table will not change.

The static routing feature can also be used to restrict which hosts (servers) can be accessed from the 833AS. Note, however, that even when IP Dynamic Routing is disabled, if a default gateway is defined, it will still be used to attempt to route messages that cannot be routed by paths defined in the IP static routing table.

Defined IP Static routes are also of benefit when using LAN-to-LAN connections. If you do not wish to maintain a permanent connection to the remote router and only wish to dial it on demand, then adding it as a static route will keep the route in the Routing Table even if it is not actively used for a period that would normally result in it being aged out.

Also, a Static Route for a remote router that does not support RIP would allow that remote router to be included in the Routing Tables of the 833AS and of all other routers on the network that support RIP.

Each entry in the IP static route table contains the following information:



IP Address

The IP address of this network.

Subnet Mask

The subnet mask of this network.

Destination Type

Specifies whether the destination type is Network or Host.

Destination Port

Specifies whether the destination is to be reached through the local network or through a LAN-to-LAN connection.

Router IP Address

The IP address of the router that will be used to reach the destination.

Add

To configure a new static route, click on the **Add** button.

Edit

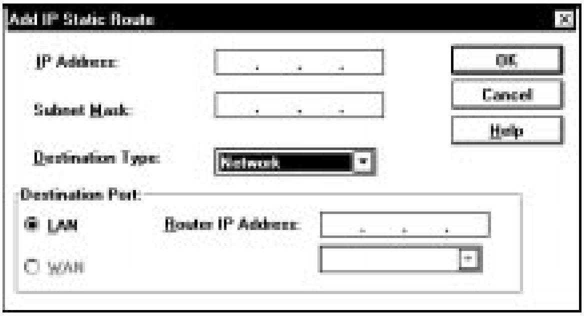
To edit an existing entry, select an entry from the table, and click the **Edit** button.

Delete

To delete an existing entry, select an entry from the table, and click the **Delete** button.

Add/Edit IP Static Routes

The **Add/Edit IP Static Route** screen is as follows:



Add IP Static Route

IP Address: . . .

Subnet Mask: . . .

Destination Type: Network

Destination Port:

● LAN Router IP Address: . . .

○ WAN

IP Address

The IP address of the network that you wish to reach. Although this must be a complete IP address, any bits that are masked by the subnet mask are treated as 0.

If you have selected Destination type as Host, enter the **IP address** of the host you wish to reach.

Subnet Mask

The subnet mask of the network that you wish to reach. If destination type is host, the subnet mask is automatically set to 255.255.255.255 to ensure that the host address is uniquely defined.

Destination Type

Specifies whether the destination type is Network or Host. If destination type is Network, the entry will define a route to a single network.

If destination type is host, the entry will define a route to a single host.

Destination Port

Specifies whether the destination is reached via the 833AS's LAN port or via a WAN port through a LAN-to-LAN connection. If the destination is to be reached via the LAN port, click on LAN and enter the IP address of the router that will be used to reach the destination. To specify a WAN port, click on WAN and then select the desired LAN-to-LAN connection from the drop-down menu.

The Perle 833AS Manager will broadcast an IP message to find any other Perle 833AS on the network. If Dynamic Routing is disabled, a route to the Manager's network may need to be configured in the Static Routing Table. If the Manager and the 833AS are on the same network, or there is a Default gateway defined and the Manager can be reached via the Default gateway, you do not require an entry in the Static Routing Table for the Manager.

Configuring IPX

The 833AS has been designed to connect to an IPX network without needing an IPX configuration. It is recommended that you take advantage of this during the initial install. However, the 833AS is able to set IPX parameters to handle special conditions.

IPX networks allow devices to be added without the need of assigning IPX addresses. IPX networks use either the Ethernet or Token Ring interface MAC address to uniquely identify devices.

An IPX network can consist of a single LAN or an internet of two or more interconnected LAN subnetworks. Each subnetwork has its own network address that is assigned by the IPX network administrator.

IPX can be transported over a number of different frame types. For Ethernet, IPX can be transported over these frame types:

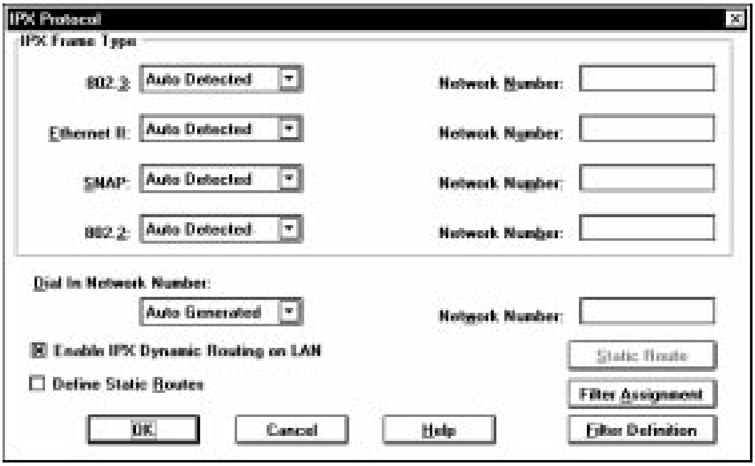
- 802.3
- Ethernet II
- SNAP (Subnetwork Access Protocol)
- 802.2

For Token Ring, IPX can be transported over these frame types:

- SNAP
- 802.2

It is not necessary to run more than one frame type. However, it may not be possible to standardize on one frame type on a LAN subnetwork because some LAN interfaces are restricted in the choice of frame type. If there are multiple frame types on a subnetwork, they behave as if they are on separate subnetworks and a network address is required for each.

The **IPX Protocol** screen is as follows:



IPX Protocol

IPX Frame Type

802.3: Auto Detected Network Number:

Ethernet II: Auto Detected Network Number:

SNAP: Auto Detected Network Number:

802.2: Auto Detected Network Number:

Dial In Network Number: Auto Generated Network Number:

☒ Enable IPX Dynamic Routing on LAN

☐ Define Static Routes

IPX Frame Type

For each available frame type, you can select:

Auto Detected

The 833AS will monitor the LAN to see if there are any frames of that type. If it does, it determines the network number from the frame number.

If you do not have any Novell servers on the subnetwork or the servers are removed from service on a regular basis, you should configure the network number.

Configured

The network number for the frame type is set by configuration and is entered in the **Network Number** field. This guarantees that the **Network Number** will always be available and lets the 833AS connect to the network faster by eliminating repetitive searches.

If you enable static routing, you must configure the network number.

Disabled

All frames of the frame type will be ignored.

Network Number

The **Network Number** is entered if the frame type was set as Configured. It must match the network number that is used on the subnetwork. See your IPX Network Administrator for this information.

The **Network Number** is formatted as 1 to 8 hex digits.The numbers FFFFFFFF and 0 are reserved.

Dial In Network Number

People dialing in to the Perle 833AS look like they are on a subnetwork separate from the LAN. This subnetwork requires its own network number. The following options are available from the drop box:

- *Auto Generated*: The 833AS will automatically choose a network number at power up time. Although the network number may change on the next power up, this will have no effect on the dial in connections.
- *Configured*: The dial in network number is set by configuration and is entered in the Network Number field. If you are using tools to monitor your network it is preferable to have a constant network number.

Network Number

The **Network Numbe**r is formatted as 1 to 8 hex digits. The numbers FFFFFFFF and 0 are reserved.

Enable IPX Dynamic Routing

When checked, the 833AS will use the IPX RIP table built from RIP messages received from other routers to determine how to route a message.

Define IPX Static Routes

When checked, the 833AS will use the configured IPX static routes table to determine how to route a message. If both dynamic and static routing are enabled, then both the IPX RIP table and the configured IPX static routes table will be used to route messages. Enabling only IPX Static Routing may be required if you have a very large IPX network. You can also restrict the servers that can be accessed from the WAN. See the next section for details on this feature.

IPX Static Routing

The Perle833AS knows the structure of the IPX network by receiving RIP messages from other routers. It also knows what services are available on the IPX network by receiving SAP messages from all servers (One server may support multiple services).

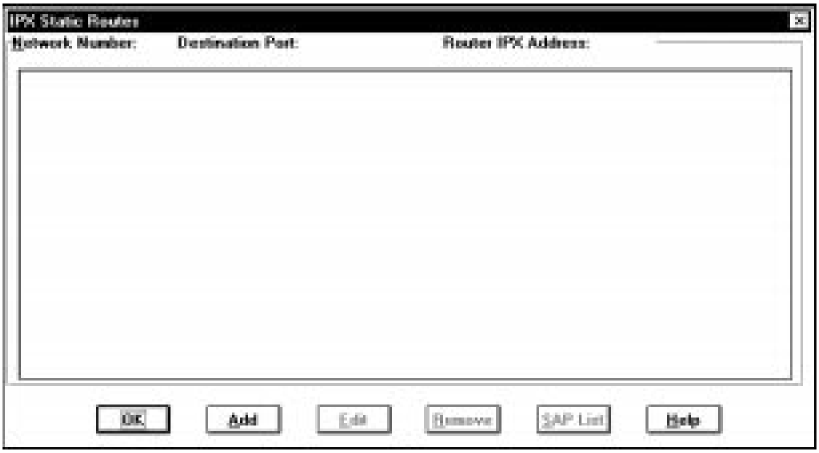
A router has an entry for each and every service that can be reached through it. As a result, the RIP and SAP tables can be very large for large networks. There is room in the Perle 833AS IPX routing tables to store 500 RIP entries and 1000 SAP entries. If your network has more routers and services than this, some of the table entries will be overwritten and those routes and services will be unavailable.

Static routing lets the network administrator configure the Perle833AS with the addresses of only the routers and services required. Dynamic routing is disabled and the Routing Tables will not change.

Static routing can also be used to restrict which services can be accessed from the WAN. Only those services that are entered in the SAP table will be available to dial in users.

The IPX Static Routes table contains the routing entries. You must have an entry for every subnetwork that you wish to access. An entry specifies the network number of a subnetwork that you wish to reach and the address of the router on the local network that will forward the messages to that network.

Each entry in the IPX static route table contains the following information:



Destination Network Number

Specifies the destination network that you wish to reach. The **Network Number** is formatted as 1 to 8 hex digits.

Destination Port

Specifies whether the destination is reached via the 833AS's LAN port or via a WAN port through a LAN-to-LAN connection. If the destination is to be reached via the LAN port, click on LAN and enter the network and node address of the router that will be used to reach the destination. To specify a WAN port, click on WAN and then select the desired LAN-to-LAN connection from the drop-down menu.

Router IPX Address

This consists of two components - the network number of the local router and the node (MAC) address of the local router.

- *Network Number*: Specifies the network number for the local router. This must be one of the network numbers that was configured in the IPX Frame Type section on the previous screen.
- *Node Address*: Specifies the MAC address for the local router. It is formatted as 12 hex digits.

Add

To configure a new static route, click on the **Add** button.

Edit

To edit an existing entry, select an entry from the table, and click the **Edit** button.

Delete

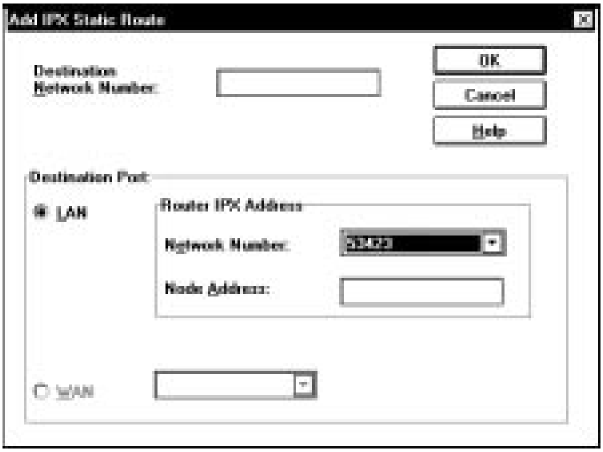
To delete an existing entry, select an entry from the table, and click the **Delete** button.

SAP List

Displays the SAP list for the selected entry. For each IPX Static Route table entry, you must configure the services you wish to have available. One server may have multiple services on it, and you need to have a separate SAP entry for each one.

Add/Edit IPX Static Routes

The following dialog box will appear if you are adding a new IPX static route, or editing an existing IPX static route.



Add IPX Static Route

Destination Network Number:

Destination Port

● LAN

Router IPX Address

Network Number: [illegible]

Node Address:

○ WAN

Destination Network Number

Enter the network number for the destination network that you wish to reach. The **Network Number** is formatted as 1 to 8 hex digits.

Destination Port

Specifies whether the destination is reached via the 833AS's LAN port or via a WAN port through a LAN-to-LAN connection. To specify a WAN port, click on WAN and then select the desired LAN-to-LAN connection from the drop-down menu. To specify a LAN destination, click on LAN, select a network number and enter a node address.

Network Number

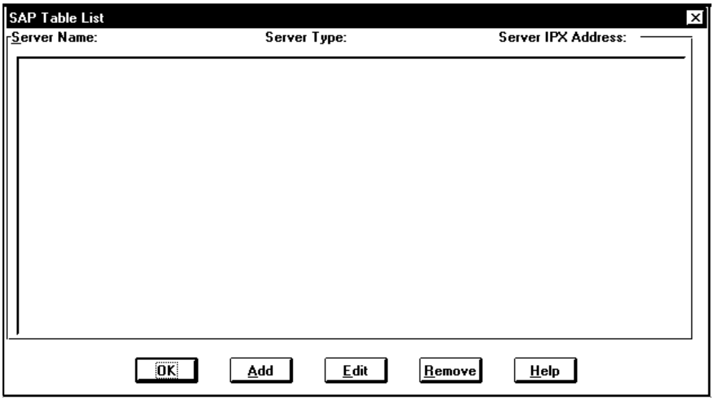
Specifies the **Network Number** for the local router. This must be one of the network numbers that was configured in the IPX Frame Type section on the previous screen.

Node Address

Specifies the **MAC address** for the local router. It is formatted as 12 hex digits.

IPX SAP Table List

The IPX SAP Table list displays the static SAP entries that have been configured. Fields are as follows:



Server Name

The server name of the IPX server.

Server Type

The type of IPX server. This is represented as 4 hexidecimal digits.

Server IPX Address

The IPX address of the server. Consists of the **Network Number** and the **Node Address** of the server.

Add

To configure a new SAP entry, click on the **Add** button.

Edit

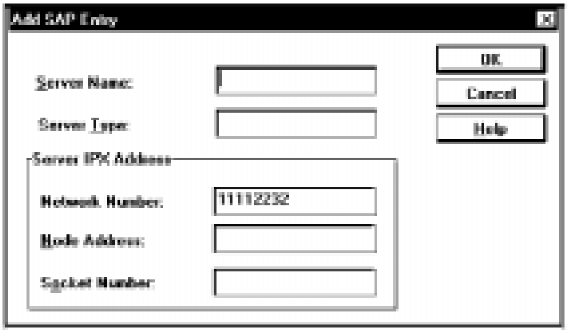
To edit an existing entry, select an entry from the table, and click the **Edit** button.

Delete

To delete an existing entry, select an entry from the table, and click the **Delete** button.

Add/Edit IPX SAP Entries

The **Add/Edit IPX SAP Entry** screen is as follows:



Add SAP Entry

Server Name:

Server Type:

Server IPX Address

Network Number: 11112232

Node Address:

Socket Number:

Server Name

The server name of the IPX server. The name can be up to 48 characters long.

Server Type

The type of IPX server. This is represented as 4 hexidecimal digits.

Network Number

The network number for this server as defined in the IPX Static Routes table entry. This cannot be changed from the SAP screens.

Node Address

Specifies the MAC address for the server. It is formatted as 12 hex digits.

Socket Number

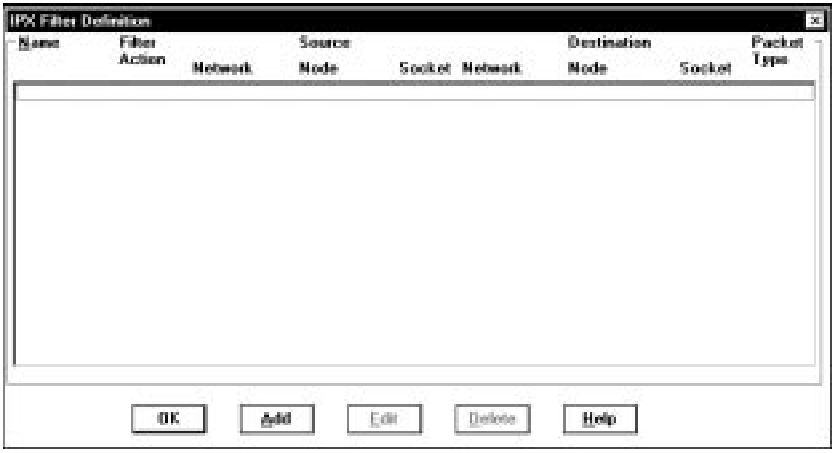
Services in an IPX network communicate with the requester using sockets. This field specifies the socket number of the desired service. It is formatted as 4 hex digits.

If Static Routing is enabled and the Manager is not on the local subnetwork, then the route to the Manager's network must be defined. A SAP entry is not created for the Manager.

If you are using any security servers configured for IPX (i.e. Novell Bindery, Axent, NT Domain) to provide 833AS security, you must set the routing path and SAP entries for these servers.

Filter Definition

Use this window to create and manage the list of up to 50 filters for the IPX protocol. IPX filters can specify the Network, Node, Socket and Sub-Protocol. The filters can accept or reject incoming packets based on source and destination network and node addresses and socket numbers. The fields are as follows:



Add

To add a filter definition, click **Add**. The **Add IPX Filter Definition** window will appear. See “Add/Edit IPX Filter Definition” on page 142 for details on how to create a filter definition.

Edit

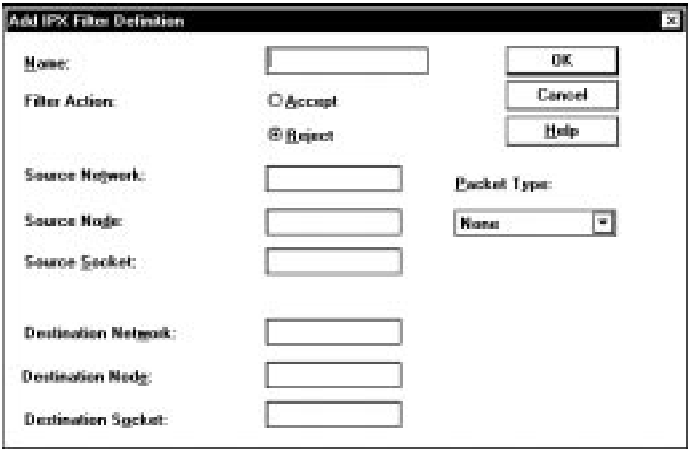
To edit a filter definition, select a filter from the list and click **Edit**. The **Edit IPX Filter Definition** window will appear. See “Add/Edit IPX Filter Definition” on page 142 for details on how to modify a filter definition.

Delete

To delete a filter definition, select a filter from the list, and click **Delete**. The filter definition will be removed.

Add/Edit IPX Filter Definition

To complete or modify the filter definition, enter the information in the following fields:



Add IPX Filter Definition

Filter Action: ○ Accept ● Reject

Packet Type: None

Name

The filter name can be up to 8 characters in length. You will use the name to assign filters to the server or user. The name can be used when adding filters to a user record on a RADIUS security server.

Filter Action

Select whether to **Accept** or **Reject** incoming IPX packets if the packet matches all parameters defined in this filter. The default setting is **Reject**.

Source Network Address

The address of the network that contains the station that is sending the IPX packet. It can be up to 8 characters long.

Source Node Address

Enter the node address of the station that is sending the IPX packet. It consists of 12 hexadecimal characters.

Source Socket Number

The socket number on the station that is sending the IPX packet. The socket number can be up to 4 hexidecimal characters.

Destination Network Address

The address of the IPX network that the IPX packet is being sent to.

Destination Node Address

The node address that the IPX packet is being sent to.

Destination Socket Number

The socket number that the IPX packet is being sent to.

Packet Type

The entries in the pull-down list are RIP, SAP, SPX, NCP, and Other.

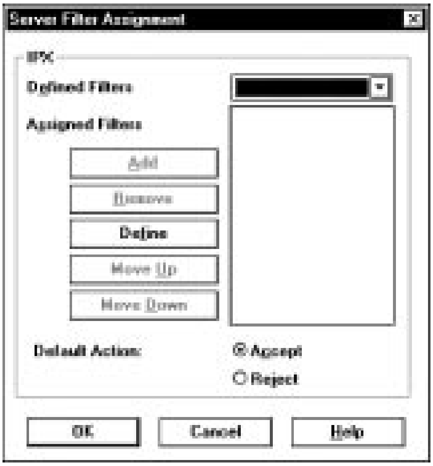
- If you select Other, make an entry in the **Type** field. The field can be up to 3 numeric characters.

Once you have entered the correct information, click **OK** to save your changes.

Filter Assignment

This window alllows you to assign up to 10 IPX filters to the server. The server will process these filters from the top down, so the order may be important. See “Packet Filtering” on page 123 for more details on how the filters are used.

To assign IPX filters for the 833AS, follow these steps, click **Filter Assignment**. The **Server Filter Assignment** window appears.



See “Filter Definition” on page 124 for information about the fields and buttons.

Configuring the Bridge Function (BCP)

Bridging is used to transport supported protocols other than IP, IPX, NetBEUI and ARA. Most commonly, it is used with LLC2 protocol to connect a PC to an IBM Mainframe or Midrange computer to get a 3270 or 5250 display session.

The MAC address of the LAN identifies devices on the network and is passed from one end to the other. A WAN client dialing in emulates a LAN adapter and this emulated adapter requires a MAC address that is provided by the server. The 833AS has these schemes for providing that address:

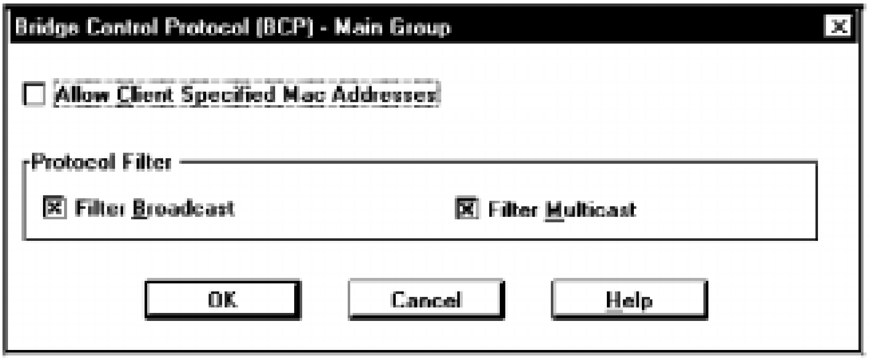
- You can assign a MAC address to the user record. This should be done if the user needs to know what the MAC address is or the MAC address has to be fixed. For example, an IBM host may not establish a session with a PC if the MAC address had changed from the previous session.
- You can create an internal pool of MAC addresses. The MAC address will be assigned at the time that the PPP session is established. The relationship between the channel of the incoming call and the MAC address is not fixed. Using the internal pool is a good choice:
    - If the protocol on the Client PC does not need the MAC address at the time the PC is started.
    - If it is not important that the user always has the same MAC address.
- You can enter the MAC address in the user database for some users and use the internal pool for the others.

The 833AS LAN adapter will see every MAC address that is present on the LAN. For best performance, the Ethernet and Token Ring LAN adapters incorporate an Address Filter. This filter will pass through only those addresses destined for the 833AS. All other addresses will be discarded in hardware.

When a user connects with Bridge Control Protocol (BCP) to the 833AS, the MAC address is loaded into the Address Filter. If the user record does not contain a MAC address, the next available free MAC address from the pool will be used.

To use the MAC address pool, it must be enabled within the LAN Feature Card configuration. See “Configure the Ethernet Card” on page 90 and “Configure the Token Ring Card” on page 91.

The **BCP** screen is as follows:


Bridge Control Protocol (BCP) - Main Group

☐ Allow Client Specified Mac Addresses

Protocol Filter

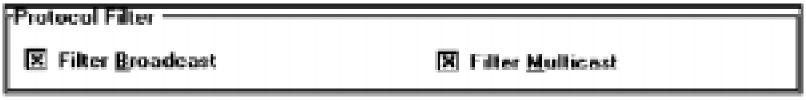
☒ Filter Broadcast ☒ Filter Multicast

Allow Client Specified Address

When checked, the **Client Specified MAC Address** will be used if available. Usually, MAC Addresses are centrally administered, and it is recommended that the Client Specified MAC Addresses are not allowed.

Protocol Filter

This option can be used to independently filter out LAN broadcasts and multicast frames so they are not passed on to the WAN client. With LLC2 protocol, no filtering should be set. The filter settings have no effect on Routing clients such as Perle Remote or Windows Dial Up Networking clients.


Protocol Filter

☒ Filter Broadcast ☒ Filter Multicast

Filter Broadcast

When checked, the 833AS will not pass any broadcast messages received from the LAN to the WAN client.

Filter Multicast

When checked, the 833AS will not pass any multicast messages received from the LAN to the WAN client.

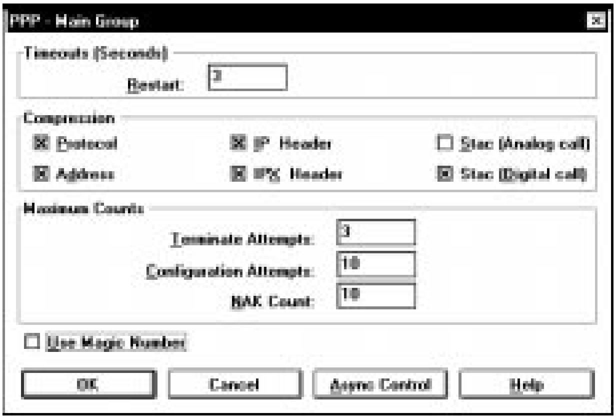
Configuring PPP

PPP is used for communication between the Dial In PC and the 833AS. These settings will apply to all clients (except ARA) dialing in, regardless of whether the LAN protocol is IP, IPX, NetBEUI, or Bridge. The defaults should work in almost all situations. It is recommended that you do not change these values during the initial installation of the 833AS.

When a client dials in to the 833AS, the PPP stacks on each side attempt to negotiate a common set of operating parameters. Modern clients can typically handle a wide range of operating parameters and will successfully negotiate with the 833AS. However, some older clients may have restrictions in their PPP stacks and may require specific settings for the compression and maximum counts parameters.

PPP is not used with Apple Remote Access (ARA) clients. PPP settings have no effect on the dial out function.

The PPP screen is as follows:



PPP - Main Group

Timeouts (Seconds)

Restart: 3

Compression

☒ Protocol ☒ IP Header ☐ Stac (Analog call)

☒ Address ☒ IPX Header ☒ Stac (Digital call)

Maximum Counts

Terminate Attempts: 3

Configuration Attempts: 10

NAK Count: 10

☐ Use Magic Number

Time-outs

Restart

When the 833AS connects with the client, they negotiate operational values between them. It is possible that the client will not respond to an 833AS negotiation message. This timer sets the maximum time the 833AS will wait for a response to negotiation messages.

Compression

Protocol

When checked, the 833AS will attempt to negotiate protocol compression during connection.This reduces the size of the PPP header. For protocol compression to be used, both the 833AS and the client must negotiate this option.

Address

When checked, the 833AS will attempt to negotiate address compression during connection. This reduces the size of the PPP header. For address compression to be used, both the 833AS and the client must negotiate this option.

IP Header

When checked, the 833AS will attempt to negotiate IP header compression.

IPX Header

When checked, the 833AS will attempt to negotiate IPX header compression.

Stac (Analog call)

When checked, the 833AS will attempt to negotiate Stac (software) compression for all analog calls.

Stac (Digital call)

When checked, the 833AS will attempt to negotiate Stac (software) compression for all digital calls.

Maximum Counts

Terminate Attempts

This parameter specifies the number of times that the 833AS will retry the terminate procedure before considering the link to be disconnected.

Configuration Attempts

This parameter specifies the total number of configuration attempts the 833AS will try before the line is dropped. During PPP start-up, the server and client will attempt to negotiate operating parameters. If the negotiation fails on the first attempt, the 833AS will try again.

NAK Count

This parameter specifies the number of NAK messages that will be permitted by the server before the line is dropped. During PPP start-up, either side can reject the message requesting the operating parameters by sending a NAK.

Use Magic Number

The magic number can be used to allow PPP to detect a loopback condition in the link. If the magic number is enabled, PPP will discard any messages looped back to itself. Some very old clients do not support magic numbers. The **Use Magic Number** should be disabled if the client does not support magic numbers.

Async Control

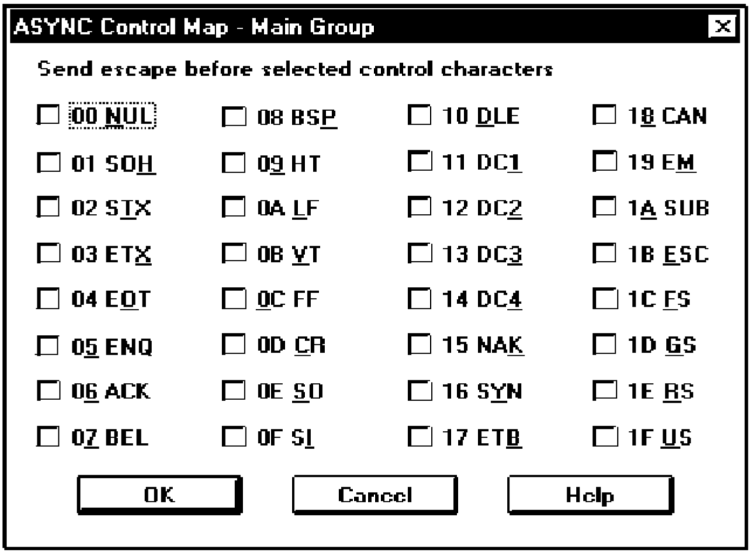
Click this button to access the **Async Control** screen.

Async Control

This is an advanced feature of PPP that lets you select any control characters that are not allowed to be transmitted on the network. Whenever a selected control character appears in the data stream, it is preceded by an escape sequence and changed into non-control characters. The destination then converts these characters back to the original value.

With a T1, E1, or PRI connection to the phone network, all control characters may be transmitted by the 833AS. On the other hand, the client may be using network equipment that requires some control characters to be masked off. The client should negotiate these characters with the 833AS, and no control characters should need to be set in the 833AS **Async Control** map. If you are using older clients that cannot successfully negotiate this map, you will need to set the control characters in the **Async Control** map.

For best performance, select only those characters that must be masked off. Any selected control characters are translated to multiple characters, degrading performance.



ASYNC Control Map - Main Group

Send escape before selected control characters

□ 00 NUL
□ 01 SOH
□ 02 STX
□ 03 ETX
□ 04 EOT
□ 05 ENQ
□ 06 ACK
□ 07 BEL
□ 08 BSP
□ 09 HT
□ 0A LF
□ 0B VT
□ 0C FF
□ 0D CR
□ 0E SO
□ 0F SI
□ 10 DLE
□ 11 DC1
□ 12 DC2
□ 13 DC3
□ 14 DC4
□ 15 NAK
□ 16 SYN
□ 17 ETB
□ 18 CAN
□ 19 EM
□ 1A SUB
□ 1B ESC
□ 1C FS
□ 1D GS
□ 1E RS
□ 1F US

▲ Async Control Map

Using AppleTalk

The Perle 833AS has built-in support for the AppleTalk networking protocol and no special configuration is required. This allows an Apple Remote Access (ARA) client running on a Macintosh to dial in to the 833AS and access the AppleTalk network. AppleTalk is supported on both Ethernet and Token Ring connected Perle 833ASs. Both ARA Version 1 and 2 clients are supported.

It is recommended that you use Version 2 ARA client software. If you are using a Version 1 ARA client, you must change the modem initialization settings for the Perle 833AS. Version 1 ARA software requires that the modem does not negotiate compression or error correction. Other dial in clients and protocols will still work in most cases, but performance for these clients could be degraded. If you require modems that support Version 1 clients, it is recommended that these be placed in a separate group.

If you are using a Version 2 ARA client, the modem settings as shipped by Apple may not work. As with the Version 1 client you may disable error correction in the server. However, you can retain your server settings by changing the modem configurations used with the ARA software. See your modem vendor for these files. Also, the Apple Remote Access Modem Toolkit Version 2.0 available from Apple will permit you to create custom modem configurations.

The client name and password configured in the ARA client must match the name and password within the 833AS. This name and password will be used solely to access the 833AS, and do not correspond to names and passwords used to access any other Macintosh.

Fixed call back is supported by the ARA client.

Using NetBEUI

The Perle833AS supports the NetBEUI (NetBIOS Extended User Interface) protocol. This permits clients such as the Windows 95 and Windows NT Dial up Networking clients to be used in a NetBIOS environment.

NetBEUI requires that the client dialing into the 833AS emulate a LAN adapter. The 833AS supplies a MAC address from an address pool for this emulated LAN adapter. Although this MAC address must be unique on your network, it does not have to remain constant every time a client connects.

The MAC address pool is defined in the LAN Feature card configuration. By default, this MAC address pool is disabled. See “Configure the Ethernet Card” on page 90 and “Configure the Token Ring Card” on page 91 for details on defining the pool.

Because the Perle 833AS supports up to 10 sessions per connection using NetBIOS the maximum number of sessions in the client's NetBEUI configuration must be set to 10 or less.

Chapter 8: Configuring the User Database

About Configuring the User Database

In this chapter you will read about:

- Overview of User Database
- Configuring the Internal User Database
- Configuring the Standard Profile

Overview of the User Database

For a user to gain access to the 833AS, the user must be defined to the system. You can do this in a number of different ways:

833AS Internal Database

You can define the user in the internal database of the 833AS. The internal database lets you set up the following for each user:

- User ID.
- User password.
- Administration privileges.
- Fixed MAC address, if required.
- User IP address, if required.
- Inactivity time-out.
- Amount of connect time.
- Call Back.
- Protocols
- Packet Filtering
- LAN-to-LAN

Shared User Database

Access to an 833AS can be controlled by using the Internal Database that is configured in a Remote 833AS server.

External Security Systems

The 833AS can use network security servers to control access to the 833AS. The servers supported are: **Novell Bindery, RADIUS, Axent, SecurID, NT Domain**.

Certain features may not be available when using any of the external security servers, because these databases do not contain all the information in the internal database. To remove this limitation, the 833AS lets you establish standard profiles for information that is common to a group of users. You can also set up an internal user record even if the user is entered in the external database. This strategy makes sense if you have a small number of users that require the special services.

Internal User Database

The internal user database of the 833AS can store user records for 2000 users. These user records are used:

- For password authentication if the 833AS has been configured for User Database security. See “Configuring User Authentication Security” on page 181.
- To assign either a fixed MAC address for Bridging clients, or a User IP address for IP clients.
- To provide information on Call Back options, connect time and inactivity time-outs.

To reduce the amount of configuration required, the user record has been split into two screens. The first screen sets basic access security, and allows the assignment of a fixed MAC address or User IP address, if required. The **Use Standard Profile** checkbox on this screen tells the 833AS to use the settings for callback, inactivity time-outs and connect time limits that were defined in the **Standard Profile**.

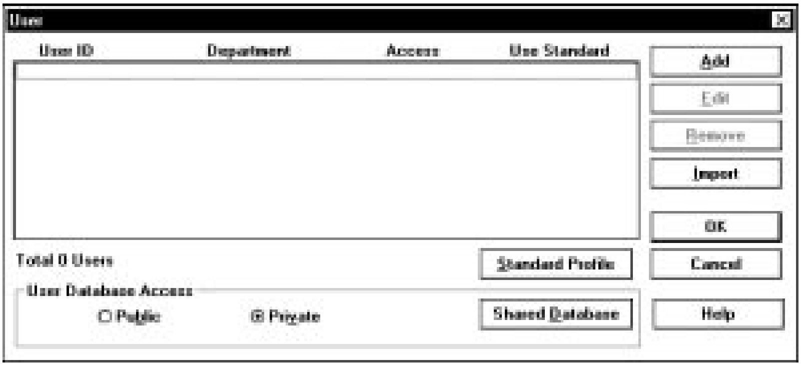
If you wish to use different settings for callback**,** inactivity time-outs and connect time for this user, deactivate **Use Standard Profile**. You can then get the second user screen by clicking on the **Profile** button. If you wish to use Fixed Call Back (i.e. call back from the 833AS to a number stored in the user database), you must activate the second screen.

Configure the Internal User Database

From the Configuration File window, click on **User**.

User Main

The User main screen appears. Fields are as follows:



Total 0 Users

User Database Access: ○ Public ● Private

User

This area displays information about all the users configured in the User Database.

User ID

The name of the user.

Department

Department to which the user belongs.

Access

Displays whether a user's access is enabled or disabled, and if enabled, whether the user has administration privileges.

Use Standard

Displays whether the user is using a Standard profile.

Add

Adds a user to the database.

Edit

Enables editing of the user currently highlighted in the User list.

Remove

Removes the user currently highlighted in the User list from the database.

Import

Performs the merging of existing 833 user databases into the current database.

Standard Profile

Edits the Standard Profile.

User Database Access

Options for access to the User Database. The options are **Public** and **Private**.

Public

The User Database on this server will be accessible to any Perle 833AS on the LAN which has been configured for **Search Remote**.

Private

The User Database will be accessible only to users that connect to this local Perle 833AS. However, the local Perle 833AS can access the user databases on other Perle 833AS servers on the LAN if the local server is configured for **Search Remote**.

Shared Database

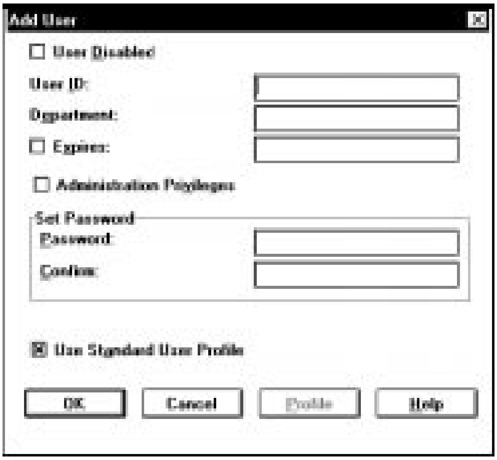
Click this button to configure the 833AS to access other servers with shared User Databases.

Add/Edit User

The **Add/Edit User** screen is used to enter permissions and user parameters for a user.

At least one user record with administration privileges must be entered in the internal database. This allows access by the 833AS Manager for configuration and monitoring.

The **Add/Edit User** screen is as follows:



User Disabled

A user record is enabled by default. If you want to prevent a user from accessing the 833AS, but do not want to delete the user from the database, click on this checkbox.

User ID

Enter the name of the user. The **User ID** field is case sensitive. Maximum length is 32 characters. The name is used in combination with the password for Local security.

Some clients may restrict User ID length to less than 32 characters.

Department

The department name is a 16 character long text field that can be used to describe users. It is used solely as a display field within the Manager, and is not used for granting privileges or access.

Expires

Select this option if you wish to disable this user record on a specific date. Enter the **Date** in the field in yy/mm/dd format.

You can also click on the **Drop** button on the date field to display a calendar. Use the scroll buttons at the top of the calendar to select the **Month**, then click on the **Day** to select.

Administration Privileges

Select this option to grant this user **Administration Privileges**. A user with administration privileges can use the 833AS Manager to configure and monitor this 833AS.

At least one user record must be created with administration privileges for each 833AS to allow access by the Manager.

Set Password

The password is used to authenticate the user if Local security is used. The **Password** field is case sensitive. Maximum length is 32 characters. Enter the password in both the Password and Confirm fields.

Some clients may restrict password length to less than 32 characters.

If you are using RADIUS or Bindery external databases, or a third party security device such as SecurID, this password is not used unless the user has been given administration privileges.

All users with administration privileges will be required to enter a valid password.

There are multiple ways of establishing the IP address for a user. For a complete discussion on this topic, See "IP Connection to the Manager" on page 40.

Use Standard Profile

When checked, the values in the **Standard Profile** will be used for **Inactivity Timeout, Connect Time**, and **Call Back**. If you wish to use **Fixed Call Back** (i.e. call back from the 833AS to a number stored in the user database), the **Standard Profile** cannot be used.

When cleared, the **Profile** button will be enabled, allowing these values to be customized for the user.

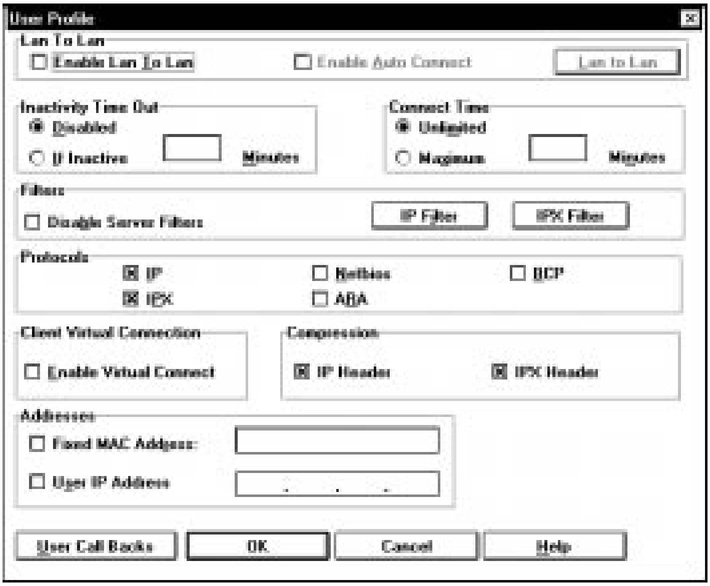
Profile

Click on the button to access the **User Profile** parameters.

User Profile

The extended user parameters on the **User Profile** screen allow you to set values for LAN-to-LAN, Inactivity Time-out, Connect time, Call Back and Filters for this user. These values will override the values set in the Standard Profile. If you wish to use Fixed Call Back (i.e. call back from the 833AS to a number stored in the user database), the Standard Profile cannot be used.

The **User Profile** screen is as follows:



User Profile

Lan To Lan

□ Enable Lan To Lan □ Enable Auto Connect [Lan to Lan]

Inactivity Time Out

● Disabled

○ If Inactive ____ Minutes

Connect Time

● Unlimited

○ Maximum ____ Minutes

Filters

□ Disable Server Filters [IP Filter] [IPX Filter]

Protocols

☒ IP □ Netbios □ BCP

☒ IPX □ ARA

Client Virtual Connection

□ Enable Virtual Connect

Compression

☒ IP Header ☒ IPX Header

Addresses

□ Fixed MAC Address: ____

□ User IP Address . . .

Enable LAN-to-LAN

When checked, this option allows a remote Router to access the 833AS.

Enable Auto Connect

When this option is selected, the 833AS maintains a permanent connection to the remote server. The 833AS initiates this connection at bootup and will automatically retry if the link goes down. The Inactivity Time Out and the Maximum Connect Time parameters are disabled when Auto Connect is active.

LAN-to-LAN

To set up the parameters for the remote router, click this button to open the LAN-to-LAN window.

Inactivity Time Out

This feature will disconnect a dial in user if there has been no activity on the link during a time out interval. The default is to disable this feature and let the user stay connected until they disconnect.

➲ To configure an Inactivity time out:

1. Click the **If inactive** button.
2. Enter a **time value** in minutes.

Note that bridged protocols may generate data traffic even though the user may not be performing any functions. This may cause the connection to remain open even when the user is inactive.

Use caution when setting this option. A user that is connected to a network when this timer expires will be disconnected, which may adversely affect the operation of certain applications.

Connect Time

This feature will disconnect a dial in user after a preset time limit, regardless of activity. The default is to allow the user Unlimited connect time.

➲ To configure a time limit:

1. Click the **Maximum** radio button.
2. Enter a value for connect time in minutes.

User Call Backs

With User Call Back enabled, when a user dials into the 833AS, the 833AS will disconnect the call and then call back the user.

This can be used:

- *For additional security*. The user record can contain a phone number to be used for call back. Only if the user is at that phone number will access be permitted.
- *For centralized billing*. With call back enabled, the dial in session is charged to the server. The user pays only for the short initial connection to the 833AS.

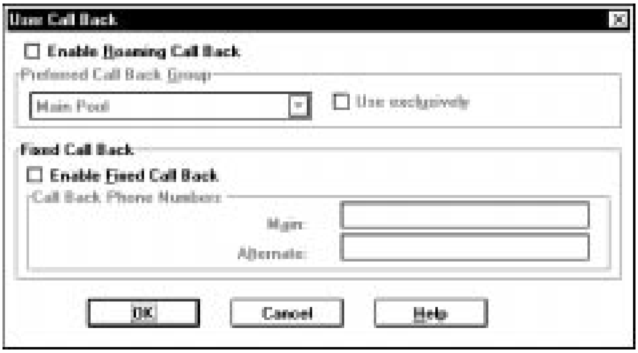
Call back can be either Fixed or Roaming.

- With Fixed call back, the call back numbers are stored in the user database. In the 833AS database, two phone numbers can be stored – a main and an alternate call back number. During the initial connection, the client asks for a call back, and can optionally specify whether to call back the main or the alternate phone number. (If no number is specified, the main number is used). The actual phone number is never transmitted on the phone line. If you are using a RADIUS database for user records, a single call back number can be set. RADIUS Call Back ID is not supported.

- With Roaming call back, the client supplies the call back number at connect time. The client must support the Call Back Control Protocol (CBCP). This is supported by the Perle Remote Client, the Microsoft Windows 95 and NT Dial in clients, as well as some other third party clients. Roaming call back is also supported by the Apple Remote Access client, using Apple's dial in protocol.

You can enable both roaming and fixed call back for a single user. If both are enabled, the 833AS will call back the roaming number if it is supplied at connect. If it is not supplied, fixed call back will be done.

Callback is available both for modem and ISDN BRI connections. The call back phone number will be dialed by the selected Line card (T1/PRI or EI/PRI). After connection, you may wish to send DTMF tones for special functions. For example, the callback may need to navigate through a PBX. You can use the Post Dial character in the call back phone number. All numbers after this character will be sent as DTMF tones regardless of how the number was dialed. For more information on this topic, see the AT command “Dn - Dial” on page 253.



User Call Back

□ Enable Roaming Call Back

Preferred Call Back Group: Main Pool □ Use exclusively

Fixed Call Back

□ Enable Fixed Call Back

Call Back Phone Numbers

Main:

Alternate:

Enable Roaming Call Back

When checked, this option will enable **Roaming Call Back**. If a client asks for roaming call back during connect, the 833AS will call back with the number supplied by the client. If a client does not request roaming call back, the session will be established as if roaming call back was not checked.

If this option is not checked, any roaming call back requests will be rejected at connect time. Client behavior will be dependent on the client – the client may either continue the session without call back, or end the session.

Preferred Call Back Group

By default, a call back will be performed on the next available line that has been enabled for call back. If you wish to allocate a specific group of channels for call back by this user, select the group in the drop box. The call back group must have been previously defined.

Use Exclusively

If you check **Use Exclusively**, the call back will occur only if there is a free channel available in the selected group. If Use Exclusively is not checked, the call back will use another channel enabled for call back if a channel from the preferred group is not available.

Enable Fixed Call Back

When checked, fixed call back will always be performed for this user when dialing in. If you are using the internal database, the call back will be done to the main phone number, or optionally to the alternate phone number if requested by the client. With RADIUS, the call back will be made to the phone number provided by the RADIUS server.

Call Back Phone Numbers

These are the phone numbers that are used by fixed call back. Each number can be up to 32 characters long. If you have enabled fixed call back, you must enter a Main phone number. The Alternate phone number is optional.

Filters

Disable Server Filters

To override the server-assigned filters and use only the user-assigned filters, click this box.

IP Filter

To assign IP filters for the user, click this button to open the User Filter Assignment window.

IPX Filter

To assign IPX filters for the user, click this button to open the User Filter Assignment window.

Protocols

Disable any **Protocols** that the user should not have access to by removing the check in the check box. All protocols are enabled by default. However, if the server has any protocols disabled, then that protocol will show as disabled for the User.

Client Virtual Connection

This feature is used by remote Dialin clients to save packet charges. The client drops the physical link to the 833AS when the line is idle but maintains the logical end-to-end connection (IP/IPX). The client reestablishes the physical link whenever there is end-to-end data to send. This feature must be supported by the Dial-In Clients.

Compression

Enable Protocol compression for IP and IPX for a specific user. If enabled, compression will be done on the protocol headers.

Addresses

Fixed MAC Address:

A user can be assigned a fixed MAC address by this field. Any valid MAC address may be used. For Ethernet, the legal values are 020000000000 to 02FFFFFFFF00. For Token Ring the legal values are 400000000000 to 40FFFFFFFF00.

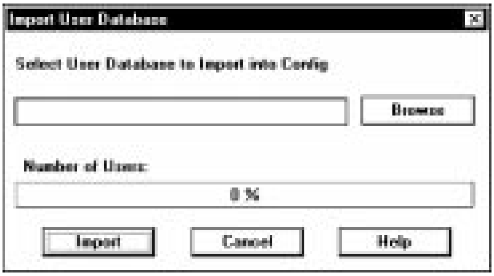
User IP address:

A user can be assigned a specific IP address by checking this field. The address is entered in dotted decimal format (for example xxx.xxx.xxx.xxx). The network portion of this address must be the same as the network portion of the server's IP address.

Import User Database

With this feature, you will be able to import 833AS User Databases and 833 User Lists and merge them into the server’s current database.

The **Import User Database** screen is as follows:



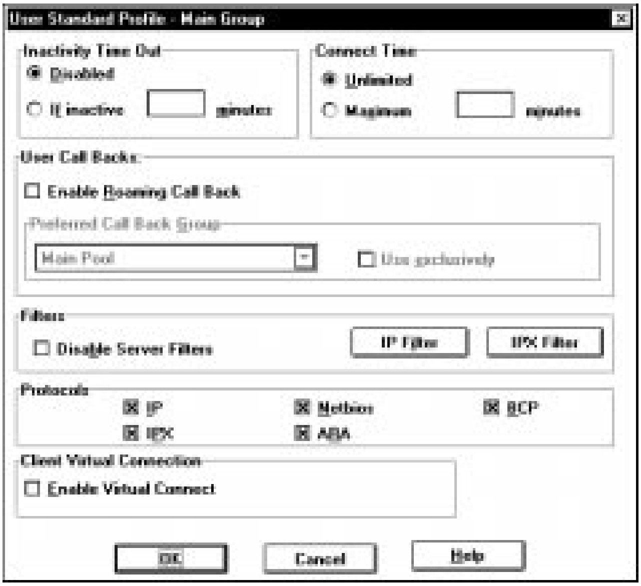
Import

Click this button if you want to import a user database from an existing configuration file.

Configuring the Standard Profile

From the **User Main** screen, click on **Standard Profile**.

The Standard Profile screen appears. Fields are as follows:



User Standard Profile - Main Group

Inactivity Time Out
● Disabled
○ If inactive [ ] minutes

Connect Time
● Unlimited
○ Maximum [ ] minutes

User Call Backs
☐ Enable Roaming Call Back
Preferred Call Back Group
Main Pool
☐ Use exclusively

Filters
☐ Disable Server Filters

Protocols
☒ IP ☒ Netbios ☒ BCP
☒ IPX ☒ ARA

Client Virtual Connection
☐ Enable Virtual Connect

Inactivity Time Out

This feature will disconnect a dial in user if there has been no activity on the link during a time out interval. The default disables this feature and lets the user stay connected until they disconnect. To configure an Inactivity time out, click the **If inactive** button, and enter a time value in minutes.

Use caution when setting this option. The operation of certain applications may be adversely effected when a user connected to the network is disconnected when the time expires.

Bridged protocols may generate data traffic even though the user may not be performing any functions. This may cause the connection to remain open even when the user is inactive.

Connect Time

This feature will disconnect a dial in user after a preset time limit, regardless of activity. The default is to allow the user Unlimited connect time. To configure a time limit, click the **Maximum** radio button and enter a value for connect time in minutes.

Call Backs

For a complete discussion on call back, See “User Call Backs” on page 160.

Enable Roaming Call Back

When checked, this option will enable **Roaming Call Back**. If a client asks for roaming call back during connect, the 833AS will call back with the number supplied by the client. If a client does not request roaming call back, the session will be established as if roaming call back was not checked.

If this option is not checked, any roaming call back requests will be rejected at connect time. Client behavior will be dependent on the client – the client may either continue the session without call back, or end the session.

Preferred Call Back Group

By default, a call back will be made on the next available line that has been enabled for call back. If you wish to allocate a specific group of channels for call back, select the group in the drop box. The call back group must have been previously defined. See “User Call Backs” on page 160.

If you check **Use Exclusively**, the call back will occur only if there is a free channel available in the selected group. If **Use Exclusively** is not checked, the call back will use another channel enabled for call back if a channel from the preferred group is not available.

Filters

For a discussion on protocol filters and how to define them, see “Packet Filtering” on page 123.

Disable Server FIlters

To override the server filters and only use the user-assigned filters, click the check box on the **Disable Server Filters** field.

IP Filter

To assign IP filters for the user, click this button to open the User Filter Assignment window.

IPX Filter

To assign IPX filters for the user, click this button to open the User Filter Assignment window.

Protocols

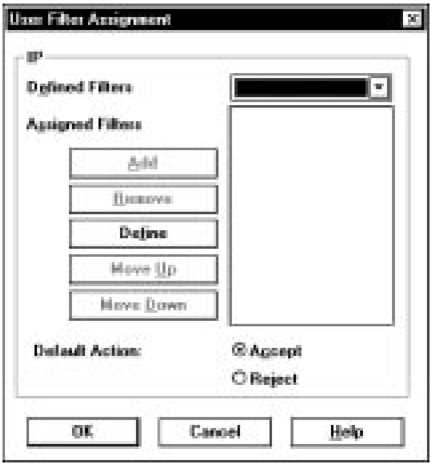
Disable any **Protocols** that the user should not have access to by removing the check in the check box. All protocols are enabled by default. However, if the server has any protocols disabled, then that protocol will show as disabled for the User.

Client Virtual Connection

This feature is used by remote Dialin clients to save packet charges. The client drops the physical link to the 833AS when the line is idle but maintains the logical end-to-end connection (IP/IPX). The client reestablishes the physical link whenever there is end-to-end data to send. This feature must be supported by the Dial-In Clients.

IP Filter Assignment

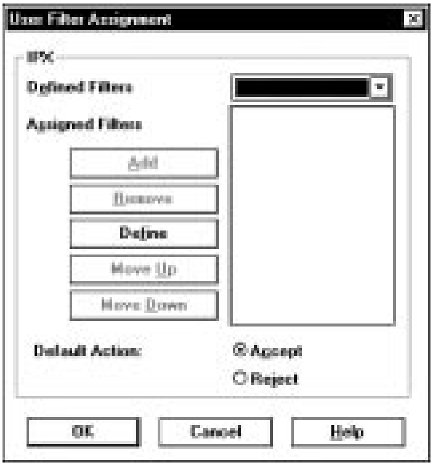
To assign an IP filter, click on **IP Filter**. The IP **User Filter Assignment** window appears. Up to 10 IP filters can be assigned to the user record. The server will process these filters from the top down, so the order may be important.



For instructions on how to define IP filters, see “Filter Assignment” on page 127.

IPX Filter Assignment

To assign an IPX filter, click on **IPX Filter**. The IPX **User Filter Assignment** window appears.



Default Action: ● Accept ○ Reject

For instructions on how to assign IPX filters, see “Filter Assignment” on page 143.

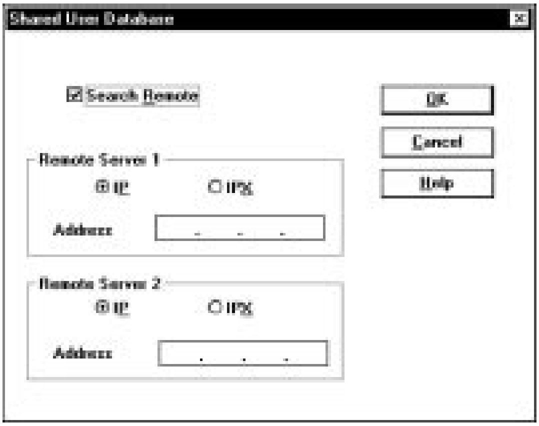
Shared User Database

The Shared User Database feature allows the Perle 833AS to access the User Database of specified remote Perle 833AS servers on the LAN. Two Remote Servers can be defined for the local server. When a user connects to the Perle 833AS, a search for the user record will occur in the following order:

1. Local User Database.
2. User Database on Remote Server 1.
3. User Database on Remote Server 2.

This option will work only if the remote Perle 833AS servers defined below have been configured for Public User Database Access.

To configure Shared User Databases, elect or open the proper configuration file. From the Users section of the **Configuration File** window, click the **Shared Databases** button. The **Shared User Database** dialog box appears. The fields are as follows:



☑ Search Remote

Remote Server 1
● IP ○ IPX
Address . . .

Remote Server 2
● IP ○ IPX
Address . . .

Search Remote

Set the check box of the **Search Remote** field to enable the Perle 833AS to search on remote servers.

Remote Server 1, Remote Server 2

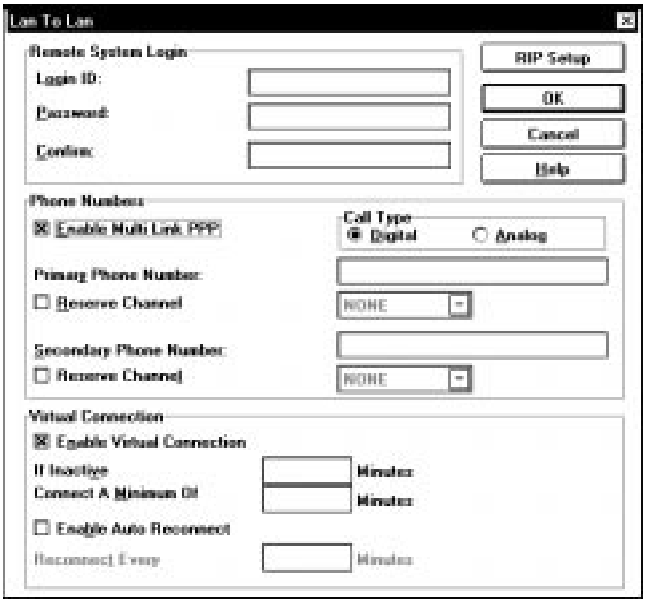
Specify the location of **Remote Server 1** and optionally **Remote Server 2** by selecting the Protocol supported by the remote server. The options are **IP** and **IPX**.

- If **IP** is selected, enter the IP **Address** of the remote server. The address should be in dotted decimal notation.
- If **IPX** is selected, enter the **Name** of the remote server. The name can be up to 15 alpha-numeric characters.

LAN-to-LAN

The LAN-to-LAN feature is used by remote Routers to establish IP/IPX connections with the 833AS. These connections can be initiated by either the remote Router or the 833AS.

The following list of parameters are used for LAN-to-LAN connections.



☒ Enable Multi Link PPP

Call Type: ● Digital ○ Analog

☐ Reserve Channel NONE

☐ Reserve Channel NONE

☒ Enable Virtual Connection

☐ Enable Auto Reconnect

Remote System Login

This section is used to setup the parameters for establishing the connection to the remote router. These include the dialing and authentication parameters:

Login ID

This is the Login ID for the remote router. Maximum length is 16 characters. The 833AS will appear to the remote router as this ID.

Password

This password is used to authenticate with the remote router. The Password field is case sensitive. Maximum length is 16 characters. Enter the password in both the Password and Confirm fields.

Enable Multilink PPP

The 833AS uses multilink PPP to support up to two physical links for each remote router connection. Each physical link has a unique phone number.

Phone Number

This field is used to enter the phone number of the remote router. The calls can be made on reserved channel numbers if necessary. The phone number fields are only required if the connection is initiated from the 833AS or virtual connection is enabled.

Call Type

Select the type of call to the remote router. Digital is used to call a router that has an ISDN BRI connection. Analog is used to call a router that has a modem connection.

Virtual Connection

When enabled, the 833AS will take down the physical links to the remote router but maintain the virtual connection at the protocol level (IP or IPX). The remote router must be setup to support virtual connection. The 833AS will simulate the RIPs, SAPs, and watchdogs messages when the virtual connection is enabled.

Enable Virtual Connection

This allows the setting of timing parameters for a virtual (spoofing) connection. Virtual connections may be initiated by:

- A defined LAN-LAN profile with the Enable Auto Connect flag set and with the Enable Virtual Connection flag set.
- A defined static route being brought up on demand and which has a LAN-LAN profile which has the Enable Virtual Connection flag set.
- An incoming call which logs into a user profile for which a LAN-LAN profile is defined having the Enable Virtual Connection flag set.

The following parameters may be set for the virtual connection:

If Inactive

This specifies the longest continuous time interval of inactivity(except for RIP, SAP and IPX Type 20 packet exchange) allowed before the virtuallink is brought down.

Connect a minimum of

This specifies the shortest continuous time interval inseconds allowed for a virtual connection. This setting is useful for setting a time period required to ensure the exchange of routing information on connection establishment.

Enable Auto Reconnect

When checked, this allows the 833AS to re-establish the virtual connection after a specified period of time defined by the Reconnect Every field. This field specifies the maximum downtime allowed on a link before the link is re-established. This optionis used to perodically reconnect for exchange of dynamic routing and other information between peer networks.

RIP Setup

RIP Send Type

From the pulldown list, select the type of RIPs to be sent over the LAN-to-LAN WANconnection. The available choices are as follows:

■	No RIP	Do not send RIPs
■	RIPV1	Send version 1 RIPs
■	RIPV1 Compatible	Send version 2 RIPs (no multicasts) so as to be version 1 compatible
■	RIPV2	Send version 2 RIPs

RIP Receive Type

From the pulldown list, select the type of RIPs to be received over and processed from the LAN-to-LAN WAN connection. The available choices are as follows:

■	No RIP	Do not process received RIPs
■	RIPV1	Process received version 1 RIPs
■	RIPV1 Compatible	Process received version 1 or version 2 RIPs
■	RIPV2	Process received version 2 RIPs

Chapter 9: Configuring the Server

About Configuring the Server

In this chapter you will read about:

- Overview
- Configuring the Server
- Dial-Out
- Security
- Configuring User Authentication Security
- Group
- SNMP

Overview

Parameters not related to Feature cards, protocols or users are contained within the Server screens. The following functions are configured by the Server screens:

- Server Identification
- Dial-Out
- Security
- Grouping
- SNMP

For most installations, parameters in this section do not have to be configured for the 833AS to work. However, it is recommended that you configure the Server identification.

Dial-Out contains advanced settings that do not need to be changed for most installations.

The 833AS supports a number of different types of user authentication security. If you are using the password security provided in the Internal 833AS User database, you do not need to change these settings.

Grouping is an advanced feature that allows you to select specific channels and modems and give them their own configuration. It is not necessary to configure groups in order to use the Server.

If you will be using an SNMP Manager such as HP OpenView to monitor the 833AS, you will need to set the SNMP parameters.

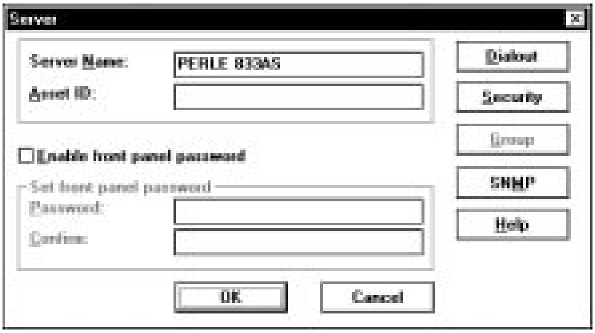
Configuring the Server

The Server screens contain the settings that apply to the entire server. For most installations, the defaults provided will work and no further settings will be required.

To configure the Server

From the Configuration File screen, click on **Serve**r.

The **Server** main screen appears. Fields are as follows:


Server

Server Name: PERLE 833AS

Asset ID:

☐ Enable front panel password

Set front panel password

Password:

Confirm:

Server Name

Enter the name you want to assign to the Server. Maximum length is 16 characters. This name is used for reference only, and appears within the Manager and the Front Panel of the 833AS.

Asset ID

If you wish to assign an **Asset ID** for the Server, enter it here. Maximum length is 16 characters. Some companies assign an **Asset ID** to permit them to track their equipment. This name is used for reference only, and appears within the Manager and the Front Panel of the 833AS.

Enable Front Panel Password

When checked, the Front Panel password is enabled.

The Front Panel can be password protected to prevent unauthorized persons from accessing it. It is recommended that you enable the Front Panel password because it is possible to perform commands from the Front Panel that can disrupt operation.

Password

The Front Panel password is entered in this field. Maximum length is 8 numeric (0-9) characters. The same password must be entered in the **Confirm** field.

Confirm

Re-enter your password.

Dial-Out

To access the Dial-Out settings, click this button. See page 176.

Security

To access the Security settings, click this button. See page 179.

Group

To access the Group settings, click this button. See page 193.

SNMP

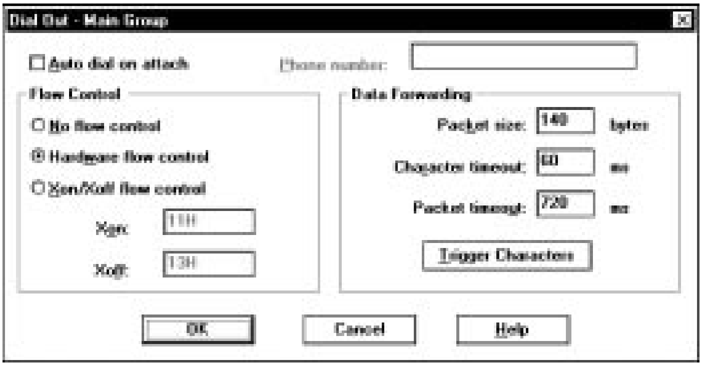
To access the SNMP settings, click this button. See page 203.

Dial-Out

This screen allows you to customize the **Dial-Out** settings. The **Auto dial on attach** setting can be used to automatically dial a phone number when a Dial-Out client acquires a Dial-Out connection.

The **Flow Control** and **Data Forwarding** settings have defaults that work for most installations and should only be changed if you have special requirements.

The **Dial-Out** screen is as follows:



Dial Out - Main Group

☐ Auto dial on attach

Phone number:

Flow Control

○ No flow control

● Hardware flow control

○ Xon/Xoff flow control

Xon: 11H

Xoff: 13H

Data Forwarding

Packet size: 140 bytes

Character timeout: 60 ms

Packet timeout: 720 ms

Auto Dial On Attach

When checked, the 833AS will automatically dial the number in the **Phone Number** field when the Dial-Out client acquires a Dial-Out connection.

Phone Number

Enter the phone number to be dialed in this field if **Auto Dial On Attach** is checked.

Flow Control

Flow Control regulates the flow of data between the 833AS T1/PRI or E1/PRI card and the modem.The 833AS has been set up to use hardware flow control and this value should not have to be changed. However, if you enable software flow control in the modem (via the modem initialization strings), you may need to modify these values.

- *No Flow Control*: When set, the 833AS will ignore any flow control indication from the modem.
- *Hardware Flow control*: When set, the 833AS will use hardware flow control with the modem.

- *Xon/Xoff Flow Control*: Also known as software flow control. When set, the 833AS will use characters received from the modem to flow control. The Xon/Xoff fields display industry standard values.

Data Forwarding

In order to optimize the connection to the Dial-Out client, the 833AS will collect individual characters received from the modem into a packet and forward this packet to the client. The parameters in this section dictate the conditions that will cause the packet to be forwarded.

Packet Size

Enter the maximum number of characters that the 833AS will collect before forwarding the packet to the Dial-Out client. The default setting is 140 characters. The minimum value is 1 character, and the maximum is 512 characters.

Setting the number lower increases the frequency of network transmissions because the packets are always sent when they are full. This results in higher LAN traffic. If you change the packet size, review the setting for the Packet Time Out.

Character Time Out

The maximum time that can elapse between characters received by the modem. If this time limit is exceeded, the packet will be forwarded to the Dial-Out client. Enter the duration of the Character Time Out in milliseconds. The default value is 60 milliseconds, with a maximum value of 65535 milliseconds. The value should be lower than the **Packet Time Out**.

This number can be decreased to improve the response at the client. It can be increased to reduce the frequency of network transmissions.

Packet Time Out

The maximum time that a packet will wait for characters from the modem before it is sent. If this time limit is exceeded, the packet will be forwarded to the Dial-Out client. Enter the duration of the packet **Time Out** in milliseconds. The default value is 720 milliseconds, with a maximum value of 65535 milliseconds.

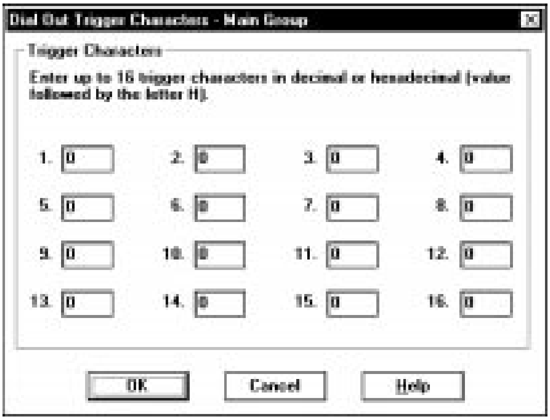
Reducing this value may improve the response of the client if the typical data transmission is smaller than a packet.

Trigger Characters

To access the **Trigger Characters** screen, click on this button.

Trigger Characters

A trigger character is a character that forces the transmission of a network packet. This can provide optimum performance if you are transmitting certain types of data to the Dial-Out client. For example, if you are transferring files and each block of transmitted data ends with a consistent and unique character, you can define the end character as a trigger.



Dial Out Trigger Characters - Main Group

Trigger Characters

Enter up to 16 trigger characters in decimal or hexadecimal (value followed by the letter H).

1. 0 2. 0 3. 0 4. 0

5. 0 6. 0 7. 0 8. 0

9. 0 10. 0 11. 0 12. 0

13. 0 14. 0 15. 0 16. 0

There is provision for up to 16 trigger characters. Enter the trigger character in decimal (range 0-255). You can also enter the trigger in hexadecimal by adding an "H" after the character. For example, the same trigger character could be entered as 33 (decimal) or 21H (hexadecimal).

Security

It is important that you manage access to your network by Dial-In Remote Users. In particular you should:

- Control who can connect to the 833AS.
- Control who can access your network resources such as file servers.
- Control who can configure and manage the 833AS.

The 833AS has facilities for controlling all the above.

Overview

User Authentication

When a user dials in, the 833AS ensures that the user is authenticated before allowing a session to be established. This authentication can be done by:

- *Using a password*. At the time of connect, the user must provide a user ID and password. If the password is incorrect, the call is disconnected. The password can be set up in the 833AS Internal User database, or an external database such as Novell Bindery or RADIUS.
- *Using a token authentication scheme* such as Security Dynamics SecurID or Axent. A token can take the form of a software key or an electronic card that provides a constantly changing number. At the time of connect, the user reads the current number from the software key or electronic card, and enters it in addition to the password and user ID. Token authentication provides for a higher level of security as the user must both possess the token and know the password.

PAP and CHAP

The Password Authentication Protocol (PAP) and the Challenge-Handshake Authentication Protocol (CHAP) are utilized in PPP security. They provide a secure mechanism to authenticate a user name and password. The 833AS Local security service as well as some third party security services require that the Dial-In Client software support PAP or CHAP.

CHAP provides a higher level of security than PAP and should be used wherever possible.

Call Back

You can enable the Fixed Call Back feature of the 833AS to enhance security. With Fixed Call Back, the user record contains a phone number to be used for call back. Once the user is authenticated, the call is dropped. The 833AS then calls back using the number stored in the User database. Only if the user is at that phone number will access be permitted.

Call back is detailed in“User Call Backs” on page 160.

Once a dial up session has been established, then the user is bound by the same network security as a user that is directly on the LAN. Although the 833AS does not control LAN security, in some cases you can restrict which networks and servers are available to the 833AS.

Administration Privileges

To manage the 833AS, a user must have Administration privileges set in their user record in the 833AS Internal database. If you are using RADIUS, you must set the “Administrative” (value=6) or the “Administrative and Call Back” (value=11) in the RADIUS Service-Type parameter in order to grant a user permission to manage the unit. If you are using Netware Bindery, Axent, SecurID or NT Domain, you still must create a user record for anyone with Administration privileges. See “Add/Edit User” on page 157.

Front Panel Password

The Front Panel Password restricts access to the control functions of the Front Panel. It is recommended that you enable the Front Panel Password (See “Enable Front Panel Password” on page 174). There is a Reset to Default function that deletes the current configuration. Once deleted, it is possible to create a new configuration to gain access. With the Front Panel password enabled, this function is restricted to only those people that have the password.

⚠ *If the Front Panel Password is enabled, it is still possible to use the 833AS Manager to change settings. However, if for some reason the Manager cannot access the unit, it will not be possible to reset the unit without the Front Panel password. There is no "secret method" to circumvent this.*

Static Routing

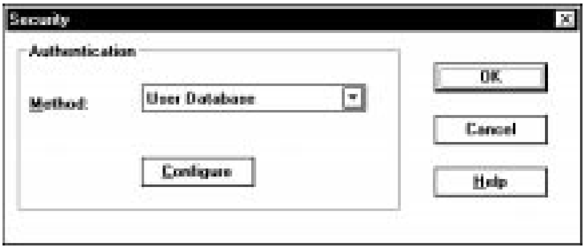
A server in an IPX network learns which networks and servers it can see. However, by using the Static Routing Table feature of the 833AS, you can explicitly specify which IPX servers and networks can be accessed. See “IPX Static Routing” on page 135.

You can use the IP Static Routing Table feature to restrict which IP networks and hosts that remote users can access. See “IP Static Routing” on page 130. Note that if you specify an IP Default Gateway in the configuration, the 833AS will attempt to use it to route to any addresses not specified in the Static Routing Table.

Configuring User Authentication Security

To access the Security Screen:

1. From the Configuration File screen, click on **Server**.
2. From the Server Screen, click on **Security**. The Security main screen will appear.

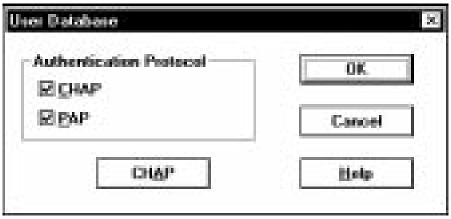


Method: User Database

3. Choose the Authentication method from the drop list. Click **Configure** to edit the configuration.

User Database

User Database Security uses the user ID and password stored within an 833AS User database. This database could be configured on the Local 833AS or on a remote 833AS. When the remote Client connects, it communicates with the 833AS using either the CHAP or PAP security protocols. If the user ID and password provided by the client matches the user ID and password within a Perle User database, the user will be granted access. The User Database Security configuration screen is as follows:



☑ CHAP
☑ PAP

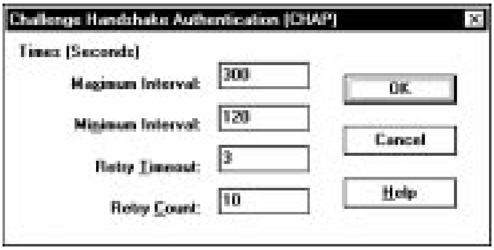
Authentication Protocol

Click on the check box to enable CHAP or PAP authentication protocols. If both are checked, the 833AS will first attempt to authenticate using CHAP. If CHAP is not supported by the client, the 833AS will then use PAP.

CHAP

CHAP (Challenge Handshake Authentication Protocol) is one of two protocols used in PPP security. It provides a higher level of security than PAP to authenticate a user name and password.

To configure the parameters for CHAP for the 833AS, click this button. The **CHAP** window appears. The fields are as follows:



Challenge Handshake Authentication (CHAP)

Times (Seconds)

Maximum Interval: 300

Minimum Interval: 120

Retry Timeout: 3

Retry Count: 10

Maximum Interval

This is the maximum amount of time that PPP will wait before sending out a CHAP challenge.

Minimum Interval

This is the minimum amount of time the PPP will wait before sending out a CHAP challenge.

Retry Timeout

This is how long CHAP will wait for a response before retrying.

Retry Count

This is how many times CHAP will retry before disconnecting the client.

Netware Bindery

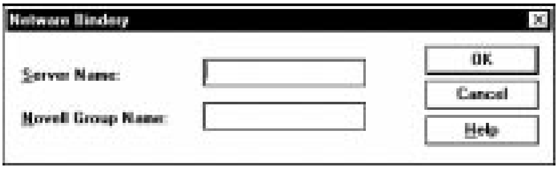
The Netware Bindery is a user profile database that is stored on a Novell Netware server. The Bindery controls access to resources on the Netware network. A user defined on the Bindery is granted privileges for access to specific servers, file directories on the servers, etc. The Bindery also has the concept of a user group. A user belonging to a group is granted all access privileges given to that group.

833AS Bindery support can also be used with Novell Directory Service (NDS) to control password access to the 833AS. NDS supports Bindery requests if the Bindery option is enabled within the NDS configuration. Consult the appropriate Novell documentation for details. Please note that the 833AS does not support native NDS messages.

The 833AS can use the Bindery to control password access to the 833AS. On the Bindery server, a group is created containing all users that can access the 833AS. When the remote Client connects, it will communicate with the 833AS using the PAP protocol (Bindery does not support CHAP). If the user ID and password provided by the client matches the user ID and password within the Bindery, the 833AS will grant access.

Users will be given the privileges granted in the Standard User Profile. See “Configuring the Standard Profile” on page 164. However, you can add a user record to the Internal 833AS User database to define unique privileges. The User ID field must match the user ID stored in the Bindery. The password in the Internal User database will not be used unless the user is requesting administration privileges.

The Netware Bindery screen contains the following:



Server Name

The name of the Netware server where the Bindery resides.

Netware Group Name

The name of the Netware group to which the authorized users belong.

This field is optional. If left blank, a user will be granted access based solely on the user ID and password.

ARA clients are not supported in this mode.

RADIUS

RADIUS (Remote Authentication Dial-In Users Services) is an open standard network security protocol. It can be used to centralize the authentication and accounting functions for any number of RAS (Remote Access Server) units. A RADIUS server authenticates users by matching the user name and password with a user record in its internal database.

When the remote client connects, it will communicate with the 833AS using the CHAP or PAP protocol. Regardless of the protocol used to exchange the password information with the client, the 833AS will always ensure that the password is encrypted before it is sent to the RADIUS server. If the user ID and password provided by the client matches the user ID and password within the RADIUS server, the user will be granted access to the 833AS. If any additional parameters were specified for the user on the RADIUS server, they will be forwarded to the 833AS at this time.

If RADIUS authentication has been configured on the 833AS, all users who attempt to gain access to the 833AS will have to have records on the RADIUS server. The local user database will not be used to authenticate users. This includes users who have administrator privileges. You can add a user record to the internal 833AS user database to define attributes not supported within RADIUS. The user ID field must match the user IS stored in RADIUS, the password in the internal user database will not be used. If a local user database entry exists for a user, it will only be used after the user has been successfully authenticated by the RADIUS server.

Sequence of events for RADIUS authentication:

1. PC dials in and is prompted for a user name and password. User enters the information which is then forwarded to the 833AS.
2. The 833AS will forward the user name and password to the RADIUS authentication server. If necessary, the password is first encrypted by the 833AS.
3. The RADIUS authentication server indicates to the 833AS if the user is authenticated. If authentication is rejected, the 833AS will notify the user.
4. If the user is authenticated, the 833AS looks for a local user record for the user. If one is found, it is loaded into the working user record. If no local user is found, the *standard* user record will be used.
5. The RADIUS server may return some configured parameters for the user. If it does, these parameters will take precedence over existing parameters in the working user record.

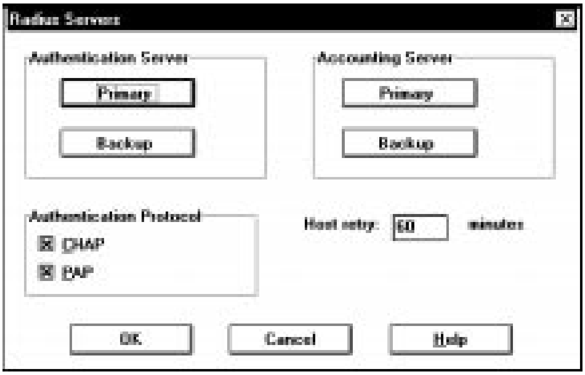
A backup RADIUS authentication server can be optionally configured on the 833AS. This server will be used if the main authentication server is not available.

A RADIUS accounting server can be optionally configured on the 833AS. This server can be used to keep accounting information for sessions. The type of information collected by a RADIUS server includes items such as:

- Indication that the user has logged on
- Number of bytes, packets sent by the user
- Number of bytes, packets received by the user
- Total amount of time for which the user was logged on
- Indication that the user had been logged off
- Reason why the user was logged off

A backup RADIUS accounting server can be optionally configured on the 833AS. This server would be used if the main if the main RADIUS accounting server was not available. If no RADIUS accounting server is defined, the accounting information will be sent to the RADIUS authentication server.

The RADIUS configuration screen contains the following:



☒ CHAP
☒ PAP

Host retry: 60 minutes

Authentication server

Click on the **Primary** button to configure the main RADIUS authentication server. Click on the **Backup** button to configure the backup RADIUS authentication server.

Accounting server

Click on the **Primary** button to configure the main RADIUS accounting server. Click on the **Backup** button to configure the backup RADIUS accounting server.

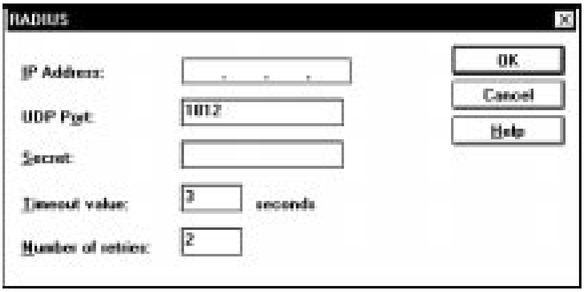
Host Retry

The length of time in minutes after which the 833AS should retry a RADIUS host which had previously become unreachable. At the expiration of this retry time, the 833AS will attempt to communicate with the RADIUS host. If no response is received, the RADIUS will remain in an off-line state. The next attempt by the 833AS to re-establish communications with this RADIUS host will occur when the time specified by the parameter elapses. The default value is 60 minutes.

Authentication Protocol

Selects the Authentication protocol to be used between the 833AS and the RADIUS server. Click on the check box to enable CHAP or PAP authentication protocols. If both are checked, the 833AS will first attempt to retrieve the user name and password using CHAP. If CHAP is not supported by the client, it will then use PAP.

Conifguring the RADIUS server parameters:IP Address



RADIUS

IP Address: . . .

UDP Port: 1812

Secret:

Timeout value: 3 seconds

Number of retries: 2

IP Address

The Internet Protocol address of the RADIUS server.

UDP port

The UDP port to be used to communicate with the RADIUS server. The default is 1812 for an authentication server and 1813 for an accounting server.

Secret

The secret key that is shared between the 833AS and the RADIUS server to encrypt the data. This key must match the key configured on the RADIUS server.

Response Timeout

The length of time in seconds for the 833AS to wait for a reply from the RADIUS server. The default is 3 seconds.

Number of Retries

The number of times the 833AS will retry a request if no answer is received from the RADIUS server. The default value is 2.

The user is not required to configure a backup RADIUS authentication server, a RADIUS accounting server or a backup RADIUS accounting server. If an accounting RADIUS server is not configured, the accounting information will be forwarded to the authentication RADIUS server.

For a complete list of the RADIUS server attributes supported by the 833AS, please refer to “Appendix 4: RADIUS Server Attributes”.

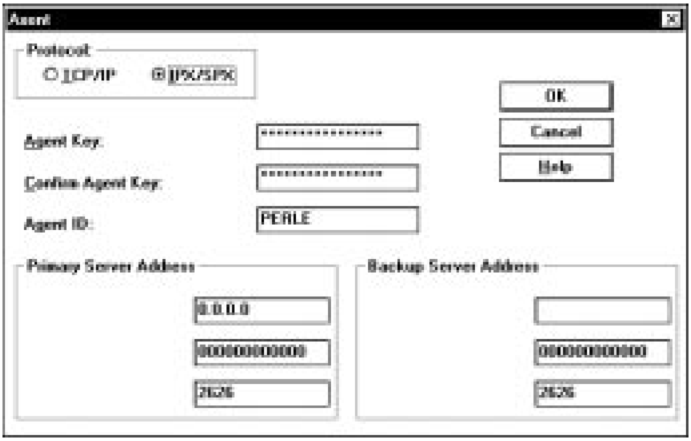
Axent

Axent (previously known as Assurenet or Digital Pathways) is a software based security server that provides user authentication with SecureNet Key cards. When the remote Client connects, the 833AS will ask the Axent server to start the authentication process. The 833AS then acts as a path between the remote Client and the Axent server. The remote Client enters a TTY or terminal mode. The Axent server will then prompt the Dial-In user for their user ID and security token from the key card. If the user ID and token are authenticated by the Axent server, the user will be granted access.

A remote Client must support terminal mode to use Axent security. Client configuration may be required to enable this mode.

Users will be given the privileges granted in the Standard User Profile. See “Configuring the Standard Profile” on page 164. However, you can add a user record to the Internal 833AS User Database to define unique privileges. The User ID field must match the user ID in the Axent server. The password in the Internal User Database will not be used unless the user is requesting administration privileges.

The **Axent** screen contains the following:



Protocol
○ TCP/IP ● IPX/SPX

Agent Key: ****************

Confirm Agent Key: ****************

Agent ID: PERLE

Primary Server Address
0.0.0.0
000000000000
2626

Backup Server Address

000000000000
2626

Protocol

Select **IPX/SPX** or **TCP/IP** as the protocol used to communicate with the Axent server. The protocol chosen will change the **Primary** and **Backup Server Address** fields described below.

Agent Key

Enter the **Agent Key** for the 833AS. This is a 1 to 16 digit hexadecimal value and must match the Agent Key configured on the Axent server. This key is used to authenticate the 833AS as a valid Axent agent.

Confirm Agent Key

Re-enter the **Agent Key** in this field for confirmation.

Agent ID

Enter the **Agent ID** for the 833AS. This is a 1 to 16 digit hexadecimal value and must match the **Agent ID** configured on the Axent server. This key is used to identify the 833AS as a valid Axent agent.

Primary Server Address (IPX/SPX)

These fields specify the address for the Primary Axent server connected via IPX/SPX:

Network

The Network number is an 8 digit hexadecimal value which identifies the network to which the Axent server is connected.

Node

The network node is a 12 digit hexadecimal value which identifies the network node to which the Axent server is connected.

Socket

The socket number for the Axent Security service. This is a 4 digit hexadecimal number. The default is 4545.

Primary Server Address (TCP/IP)

These fields specify the address for the Primary Axent server connected via TCP/IP:

IP address

The IP address of the Axent server.

TCP port

The TCP port number of the Axent Security Service. This is a 4 digit hexadecimal number. The default is 2626.

Backup Server Address

If you have a backup Axent server, configure the address using these fields.

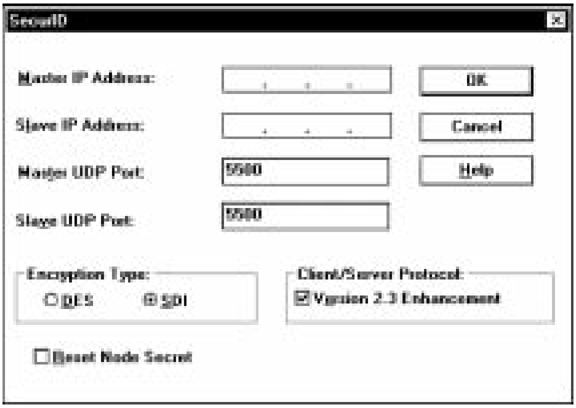
SecurID

SecurID enables the 833AS to use the ACE/Server from Security Dynamics for user authentication. The ACE/Server is a software based security server that provides user authentication with a memorized personal identification number (PIN) and a code generated by the SecurID token. When the remote Client connects, the 833AS will ask the ACE/Server to start the authentication process. The 833AS then acts as a path between the remote Client and the ACE/Server. The remote Client enters a TTY or terminal mode. The ACE/Server will then prompt the Dial-In user for their user ID and passcode from the SecurID token. If the user ID and token are authenticated by the ACE/Server, the user will be granted access.

A remote Client must support terminal mode to use SecurID security. Client configuration may be required to enable this mode.

Users will be given the privileges granted in the Standard User Profile. See “Configuring the Standard Profile” on page 164. However, you can add a user record to the Internal 833AS User Database to define unique privileges. The User ID field must match the user ID in the ACE/Server. The password in the Internal User Database will not be used unless the user is requesting administration privileges.

The ACE/Server screen contains the following:



Master IP Address: . . .

Slave IP Address: . . .

Master UDP Port: 5500

Slave UDP Port: 5500

Encryption Type: ○ DES ● SDI

Client/Server Protocol: ☑ Version 2.3 Enhancement

☐ Reset Node Secret

Master IP Address

The IP address of the Master SecurID server.

Master UDP Port

The UDP port number of the SecurID service on the Master server. This is a 4 character decimal number. The default is 5500.

Slave IP Address

The IP address of the Slave SecurID server.

Slave UDP Port

The UDP port number of the SecurID service on the Slave server. This is a 4 character decimal number. The default is 5500.

Encryption Type

Click the type of data encryption to be used when communicating with the SecurID server. The choices are DES or SDI.

Client/Server Protocol

Version 2.3 Enhancement

Check this box to enable the 833AS to use the Security enhancements of the Client/Server communication protocol offered in Version 2.3 of the ACE/Server software. This is the default setting.

If you are using an ACE/Server with Version 2.2 software then remove the check from this box.

Reset Node Secret

The Node Secret is a pseudo-random string that is sent to the 833AS server by the SecurID server the first time the 833AS sends an authorization request. The Node Secret is used to encrypt the data that is sent between the 833AS and the SecurID Server.

Do not check this box unless there is a mismatch between the node secret in the 833AS and the SecurID server and you must reset the Node Secret to blank. This would occur if a 833AS is moved to another network with a new SecurID server.

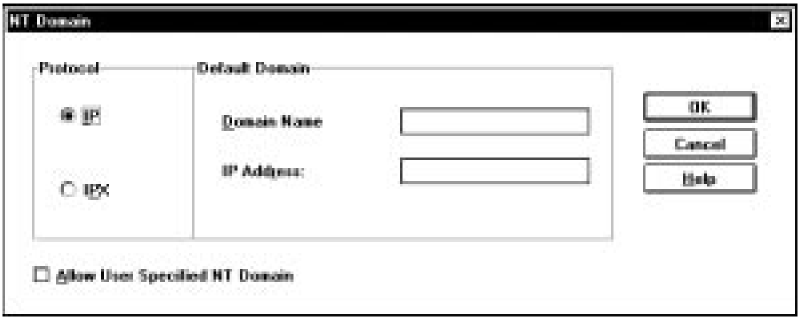
If the Node Secret is reset, or the 833AS is reset to factory defaults, then the SecurID server must be configured to resend the Node Secret to the 833AS.

NT Domain

NT Domain enables the Perle 833AS to use a Windows NT’s domain user database for dial-in user authentication. The Perle 833AS server will collect the userid and password from the dial-in client and will forward an authorization request to the Primary Domain Controller (PDC). This feature will work with the Perle Remote Client as well as other PPP clients such as Windows 95 and NT. The clients must support the Password Authentication Protocol (PAP).

Users will be given the privileges granted in the Standard User Profile. See “Configuring the Standard Profile” on page 164. However, you can add a user record to the Internal 833AS User Database to define unique privileges. The User ID field must match the user ID in the NT Domain Server. The password in the Internal User Database will not be used unless the user is requesting administration privileges.

The NT Domain dialog box contains the following:



Protocol

Select the network protocol which will be used to communicate with the PDC. The choices are IPX and IP.

Default Domain Name

Identify the NT domain by entering the Domain Name. The Domain name can be up to 16 characters long.

IP Address

If the network protocol used to communicate with the PDC is IP then enter the PDC’s IP address. This value must be configured if the PDC is not on the same IP subnet as the Perle 833AS.

Allow User Specified NT Domain

Click the check box to allow a dial-in user to specify a domain to which they belong. The Perle 833AS server will send the authorization request to this domain instead of the default domain. A user would enter their userid in the format “domain\userid”.

Group Settings

The powerful grouping feature of the 833AS lets you select specific channels and modems and give them their own configuration. Some examples of uses for grouping include:

- Allocate connections for specific departments or have a connection always available for the MIS department.
- Set up a group of modems that are compatible with older Dial-In modems that require special settings.
- Set one group of users with a maximum Dial-In time of one hour, and another with unlimited access time.

The 833AS treats channels and modems as pools of channels and modems. A channel, by default, appears in the main channel pool. The channel can be enabled for Dial-In, Dial-Out, and/or call back. (Note that by default Dial-In, Dial-Out and call back are enabled, but any of these functions can be disabled in the T1/PRI or E1/PRI configuration).

When a Dial-In call comes in, the 833AS will allocate the next available modem from the main modem pool.

For a discussion on the main channel and modem pool, please See “Channels” on page 196.

If a channel is added to a group, that channel is removed from the main pool. A channel can appear within only one group.

If a modem is added to a group, that modem will be removed from the main pool. However, a modem can appear in multiple groups.

How a group is selected is based on the mode of operation.

Dial-In

When a call comes in, the 833AS checks to see if the channel is assigned to a group. If it is, the group profile for that call is used. Based on this profile, the 833AS will allocate one of the modems assigned to the group. Also, other settings can optionally be defined for this group:

- User standard profile.
- PPP protocol settings.
- Bridge filter.

Dial-Out

Groups enabled for Dial-Out will appear in the "Available Pools" list of the Perle 833 Dial-Out client. A user selects a group from the list and is then assigned a channel and modem that is defined to the group. Also, Dial-Out settings for flow control, autodial, and packet forwarding can be customized for this group.

Call Back

The Call Back group is determined by an entry in the user record. A channel and modem assigned to the group will be used when call back is required. There are no optional group settings for Call Back.

It is possible to enable a group for more than one mode of operation. That is, one group can be enabled for Dial-In, Dial-Out, and Call Back.

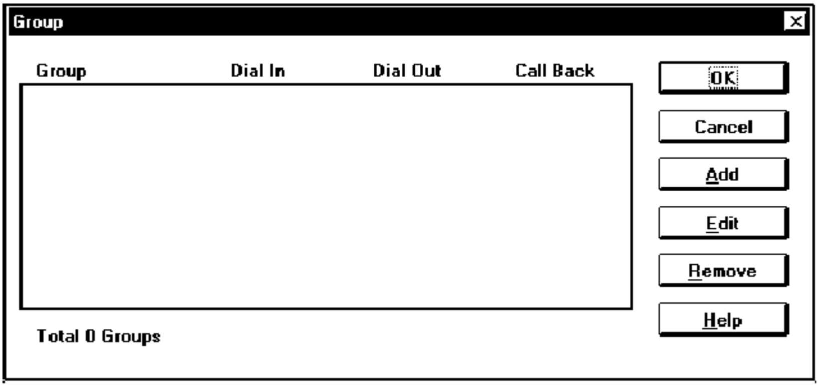
If a group is enabled for multiple modes, it will behave...

- as a Dial-In group if a Dial-In call is received.
- as a Dial-Out group if selected from the Dial-Out client.
- as a Call Back group if call back is required.

...if Dial-In, Dial-Out, and call back are enabled.

Group Main

The group main screen lists all the currently defined groups and whether a group is enabled for Dial-In, Dial-Out, or call back. Fields are as follows:



Group

Name of the group.

Dial-In

Displays whether this group is enabled for Dial-In.

Dial-Out

Displays whether this group is enabled for Dial-Out.

Call Back

Displays whether this group is enabled for call back.

Add

To create a new group, click on **Add**.

Edit

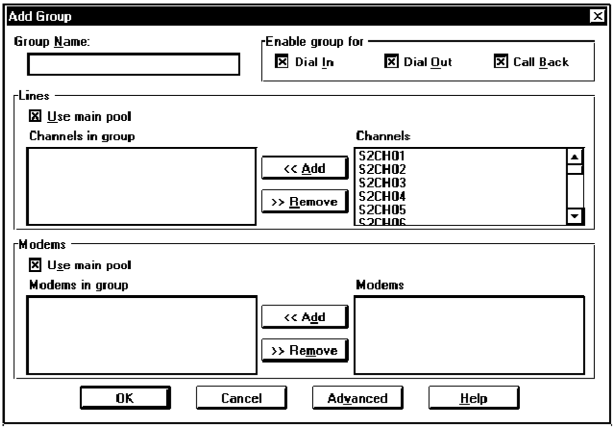
To edit an existing group, highlight that group and click on **Edit**.

Remove

To remove an existing group, highlight that group and click on **Remove**.

Add/Edit Group

The Add Group and Edit Group screens allow you to set the parameters for the group. Fields are as follows:



Add Group

Group Name:

Enable group for: ☒ Dial In ☒ Dial Out ☒ Call Back

Lines

☒ Use main pool

Channels in group

Channels: S2CH01, S2CH02, S2CH03, S2CH04, S2CH05, S2CH06

Modems

☒ Use main pool

Modems in group

Modems

Group Name

Enter the name you want to assign to the Group. Maximum length is 16 characters.

Enable Group For

These settings allow you to enable a group for:

- Dial-In.
- Dial-Out.
- Call back.

The enable group settings override the settings for any channels and modems explicitly included in the group.

Channels

Use Main Pool

When enabled, the channels for this group will be allocated from the main channel pool. If a channel is required for Dial-Out or call back, the channel attributes that were defined in the T1/PRI or E1/PRI configuration will be used. For example, if a channel is required for Dial-Out for this group, the 833AS will select the next available channel from the main pool that has been enabled for Dial-Out.

When disabled, the next available channel that appears in the **Channels In Group** box will be used.

Channels In Group

Lists the channels by name that have been allocated to this group. If a channel appears in this group, it will not appear in either the main pool or any other group. To remove a channel from this group, click on the **Remove** button.

Channels

Lists the channels that are available to be added to this group. To add a channel to this group, click on the **Add** button. The name of the channel is defined in the channel section of the T1/PRI or E1/PRI configuration. Note that if a T1/PRI or E1/PRI card has been disabled in configuration, the associated channels will still appear in the list to permit pre-configuration.

Modems

Use Main Pool

When enabled, the modems for this group will be allocated from the main modem pool. If a modem is required for Dial-In, Dial-Out, or call back, the modem attributes defined in the Modem configuration will be used. For example, if a modem is required for Dial-In for this group, the 833AS will select the next available modem from the main modem pool that has been enabled for Dial-Out.

Modems In Group

Lists the modems that have been allocated to this group by name. If a modem appears in this group, it will not appear in the main pool. It may, however, be allocated to another group. To remove a modem from this group, click on the **Remove** button.

Modems

Lists the modems that are available to be added to this group. To add a modem to this group, click on the **Add** button. The name of the modem is defined in the modem section of the Modem configuration. Note that if a Modem card has been disabled in configuration, the associated modems will still appear in the list to permit pre-configuration.

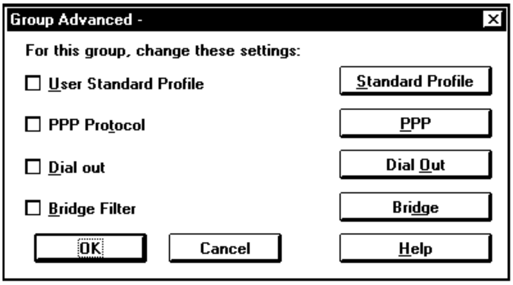
Advanced

To access the Advanced group settings, click on this button.

Group Advanced

The advanced settings allow you to customize these settings on a per group basis:

- User standard profile.
- PPP protocol settings.
- Dial-Out settings.
- Bridge filter settings.



Group Advanced -

For this group, change these settings:

□ User Standard Profile

□ PPP Protocol

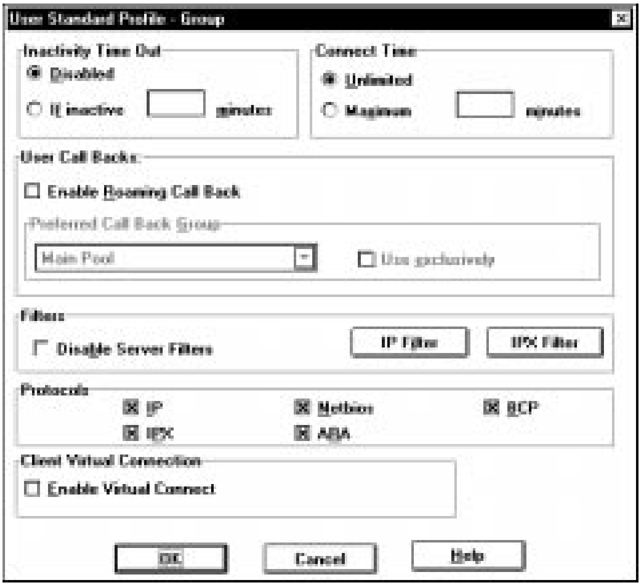
□ Dial out

□ Bridge Filter

Click the checkbox for any settings that you wish to modify. If you do not modify a setting, the system settings for these values will be used.

User Standard Profile - Group

If enabled, this Group Standard Profile will replace the system Standard Profile for any Dial-In calls received on this group. If a user record is set to not use the Standard profile, the Group Standard Profile will not be used.



User Standard Profile - Group

Inactivity Time Out
● Disabled
○ If inactive [ ] minutes

Connect Time
● Unlimited
○ Maximum [ ] minutes

User Call Backs
□ Enable Roaming Call Back
Preferred Call Back Group: Main Pool
□ Use exclusively

Filters
□ Disable Server Filters

Protocols
☒ IP ☒ Netbios ☒ BCP
☒ IPX ☒ ARA

Client Virtual Connection
□ Enable Virtual Connect

Inactivity Time Out

This feature will disconnect a Dial-In user if there has been no activity on the link during a time out interval. The default disables this feature and lets the user stay connected until they disconnect. To configure an Inactivity time out, click the **If inactive** button, and enter a **time value** in minutes.

Use caution when setting this option. The operation of certain applications may be adversely effected when a user connected to the network is disconnected when the time expires.

Bridged protocols may generate data traffic even though the user may not be performing any functions. This may cause the connection to remain open even when the user is inactive.

Connect Time

This feature will disconnect a Dial-In user after a preset time limit, regardless of activity. The default is to allow the user Unlimited connect time. To configure a time limit, click the **Maximum radio button** and enter a **value** for connect time in minutes.

User Call Backs

For a complete discussion on call back, see “User Call Backs” on page 160.

Enable Roaming Call Back

When checked, this option will enable **Roaming Call Back**. If a client asks for roaming call back during connect, the 833AS will call back with the number supplied by the client. If a client does not request roaming call back, the session will be established as if roaming call back was not checked.

If this option is not checked, any roaming call back requests will be rejected at connect time. Client behavior will be dependent on the client – the client may either continue the session without call back, or end the session.

Preferred Call Back Group

By default, a call back will be done on the next available line that has been enabled for call back. If you wish to allocate a specific group of channels for call back by this user, select the group in the drop box. The call back group must have been previously defined.

If you check **Use Exclusively**, the call back will occur only if there is a free channel available in the selected group. If **Use Exclusively** is not checked, the call back will use another channel enabled for call back if a channel from the preferred group is not available.

Filters

Disable Server Filters

To override the server filters and only use the user-assigned filters, click on this box in the Disable Server Filters field.

IP Filters

To assign IP filters, click the **IP Filters** button. See “Filter Definition” on page 124 for more details.

IPX Filters

To assign IPX filters, click the **IPX Filters** button. See “Filter Definition” on page 124 for more details.

Protocols

Disable any **Protocols** that the user should not have access to by removing the check in the check box. All protocols are enabled by default. However, if the server has any protocols disabled, then that protocol will show as disabled for the User.

Client Virtual Connection

This feature is used by remote Dialin clients to save packet charges. The client drops the physical link to the 833AS when the line is idle but maintains the logical end-to-end connection (IP/IPX). The client reestablishes the physical link whenever there is end-to-end data to send. This feature must be supported by the Dial-In Clients.

PPP - Group

If enabled, these PPP settings will replace the system PPP settings for any Dial-In calls received on this group. This may be useful for providing compatibility with older PPP clients. Some older clients may have restrictions in their PPP protocol implementation and may require specific settings for the compression and maximum counts parameters.

The parameters for the PPP Group settings are the same as the main PPP settings. For details on these settings, see “Configuring PPP” on page 146.

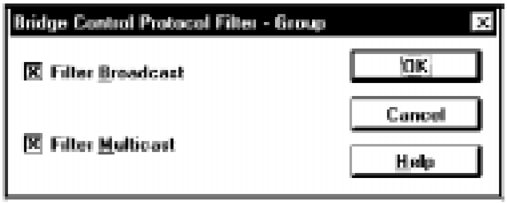
Dial-Out - Group

If enabled, these Dial-Out settings will replace the system Dial-Out settings for any Dial-Out sessions using this group. The parameters for the Dial-Out Group settings are the same as the main Dial-Out settings. For details on these settings, see “Dial-Out” on page 176.

Bridge Filter - Group

If enabled, these protocol settings will replace the system Bridge Control Protocol (BCP) protocol settings for any Dial-In calls received on this group. This option can be used to independently filter out LAN broadcasts and multicast frames so they are not passed on to the WAN client. With LLC2 protocol, no filtering should be set. See “Chapter 7: Configuring the Protocols” on page 111.

Fields are as follows:



Bridge Control Protocol Filter - Group

☒ Filter Broadcast

☒ Filter Multicast

Filter Broadcast

When checked, the 833AS will not pass any broadcast messages received from the LAN to the WAN client.

Filter Multicast

When checked, the 833AS will not pass any multicast messages received from the LAN to the WAN client.

SNMP

SNMP, or Simple Network Management Protocol, is a command/response protocol used for managing IP devices on a network.

An SNMP Manager such as HP OpenView© is used to issue requests for status, performance, and configuration information to an IP device on the network.

An SNMP compliant IP device responds to commands issued by the SNMP Manager. The code that responds to the SNMP request is known as an SNMP Agent. Depending on the source and access privileges of the request, the Agent may or may not issue the requested information. Access levels range from:

- No Access - the SNMP Manager does not have access privileges.
- Read-only - the SNMP Manager can read the information only, but cannot modify it.
- Read/Write - the SNMP Manager can read and edit the information.

SNMP is an open standard and the capabilities are defined in specifications known as RFCs. The 833AS supports the following RFCs:

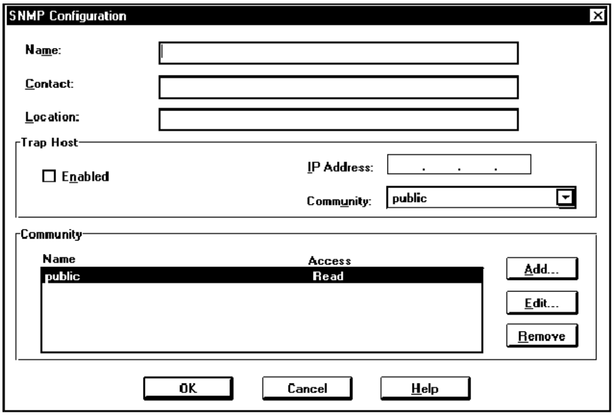
- RFC 1157 - A Simple Network Management Protocol. (SNMP)
- RFC 1213 - Management Information Base for Network Management of TCP/IP Internets: MIB II.
- RFC 1406 - Definitions of Managed Objects for the DS1 and E1 Interface Types.
- RFC 1471 - The Definitions of Managed Objects for the Link Control Protocol of Point-to-Point Protocol.
- RFC 1573 - Evolution of the Interface Groups of MIB-II.
- RFC 1643 - Definitions of Managed Objects for Ethernet-like Interface Types.
- RFC 1659 - Definitions of Managed Objects for RS-232-like Hardware Devices using SMIv2.
- RFC 1696 - Modem Management Information Base (MIB) using SMIv2.
- RFC 1742 - AppleTalk Management Information Base II.
- RFC 1743 - IEEE 802.5 MIB using SMIv2.
- RFC 2127 - ISDN Management Information Base using SMIv2.

The 833AS Agent supports read access of the SNMP information only. Configuration and control is performed via the 833AS Manager.

The 833AS can be controlled by an SNMP Manager that has dialed in to the 833AS.

SNMP Configuration

The **SNMP Configuration** screen is used to set parameters related to SNMP. Fields are as follows:



☐ Enabled

IP Address: . . .

Community: public

Name	Access
public	Read

Name

Enter the name that the **Server** will be known as to the SNMP network. This name is not tied to the Server name that is defined on the main **Server** configuration screen. Maximum length is 255 characters.

Contact

Enter the name of the person responsible for managing the 833AS. Maximum length is 255 characters.

Location

Enter a description of the physical location of the 833AS.

Trap Host

When the SNMP Agent in the 833AS detects a serious condition or activity, it will send a message known as a trap. A **Trap Host** is an IP workstation that is set up to receive SNMP trap messages. The **Trap Host** must be a member of a community which is known to the SNMP Agent.

The 833AS sends trap messages:

- When the unit restarts.
- When an invalid login is detected.

Enabled

Click on the box to enable the **Trap Host**.

IP Address

Enter the **IP address** of the **Trap Host** in dotted decimal format.

Community

Select a community that the **Trap Host** belongs to from the drop box.

Community and Community Tables

Not everyone on the IP network should be permitted to access the information controlled by an SNMP Agent. SNMP access to the 833AS is restricted through the use of communities and community tables.

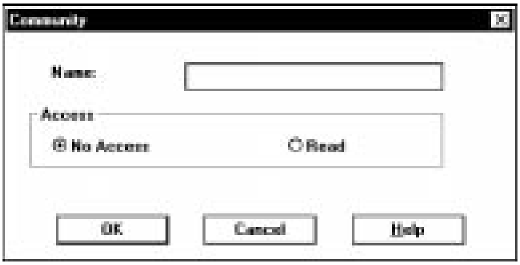
A community is a group of users having a defined Name and a defined Access level. The 833AS supports up to five SNMP communities. The default community is "**public**".

Community tables act like passwords by controlling SNMP access. They list all SNMP communities and their corresponding access levels.

When the SNMP Agent on the 833AS receives a request for information, it looks for the name of the requester in the community table. If it is not found, the request is denied and an error is returned to the user. If the access level of the community is equivalent to or greater than the access level of the request, it is accepted.

The list of currently defined communities is displayed in the Community table. To add a new community, click **Add**. To edit an existing community, highlight the community and click **Edit**. The Community configuration screen will appear.

To delete an existing community, highlight the community and click **Delete**. You cannot delete the "public" SNMP community. However, its access level can be changed.



Access

● No Access ○ Read

Name

Enter the **SNMP community name** in this field.

Access

Click on **No Access** if you want to prevent members of this community from receiving responses to their SNMP requests. Click on **Read** if you wish to grant Read access permission to members of this community.

Section 3: Management

Chapter 10: Managing the Perle 833AS

About Managing the Perle 833AS

This chapter provides information related to managing the 833AS. You will read about:

- 833AS Manager Statistics
- 833AS Front Panel
- 833AS Event Log

833AS Manager Statistics

Built into your 833AS Manager is a facility that provides information about the:

- Operational status of the Feature Cards in the unit.
- Number of LAN transmission and receive errors encountered.
- Networks and Servers that can be reached by the 833AS on an IPX connection.
- Status of current calls, and what modems and lines are used by those calls.
- Quality of the T1 or E1 line.

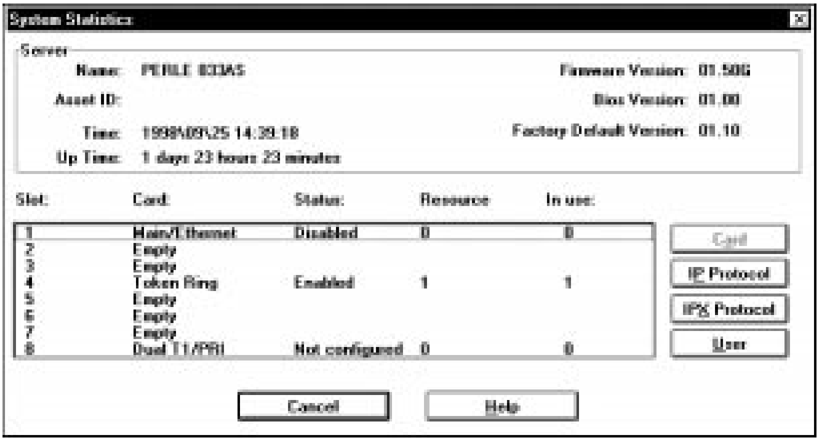
Viewing Statistics

To view the statistics of an 833AS, connect to the server and choose **Get Statistics** from the Statistics menu. Please See “Connecting to the Server” on page 57 for details on how to connect to a server.

The main System Statistics screen will appear. This screen provides a high level view of the status of the server. It also allows you to access more detailed information about a Feature Card or protocol.

Server Information

The following general information about the Server is displayed:



Server

Name: PERLE 833AS

Asset ID:

Time: 1998\09\25 14:39:18

Up Time: 1 days 23 hours 23 minutes

Firmware Version: 01.50G

Bios Version: 01.00

Factory Default Version: 01.10

Slot:	Card:	Status:	Resource	In use:
1	Main/Ethernet	Disabled	0	0
2	Empty			
3	Empty			
4	Token Ring	Enabled	1	1
5	Empty			
6	Empty			
7	Empty			
8	Dual T1/PRI	Not configured	0	0

Name

Name of this 833AS as defined in the Server configuration.

Asset ID

Asset ID of this 833AS as defined in the Server configuration.

Time

The current time as set within this 833AS.

Up time

Time elapsed since the 833AS was last started or reset.

Firmware Version

Version number of the 833AS operating Firmware.

BIOS version

Version number of the 833AS BIOS.

Feature Card Display

The Feature Card display provides basic information about each Feature Card installed in the 833AS. The following information is displayed for each Feature card:

Slot

Slot number of the Feature Card.

Card

Type of card installed in the slot. Valid card types are:

- System/Ethernet
- Token Ring
- T1/PRI
- Dual T1/PRI
- E1/PRI
- Dual E1/PRI
- PerleDSP Modem Feature Cards
- Perle 12 HD Modem Feature Card
- Perle 18 HD Modem Feature Card
- Perle 24 HD Modem Feature Card
- Perle 30 HD Modem Feature Card
- Empty (no card)

Status

Displays whether the card is enabled or has been disabled via configuration.

Resources

The total number of resources available for this card. A resource is a general term for the number of enabled modems or channels available on a card. If a channel or modem has been disabled via configuration, that resource will not be included in the total.

In Use

The number of resources for the card that are currently in use.

Card

Click on this button to access the **Statistics** for this card.

IP Protocol

Click on this button to access the **IP Protocol Statistics**.

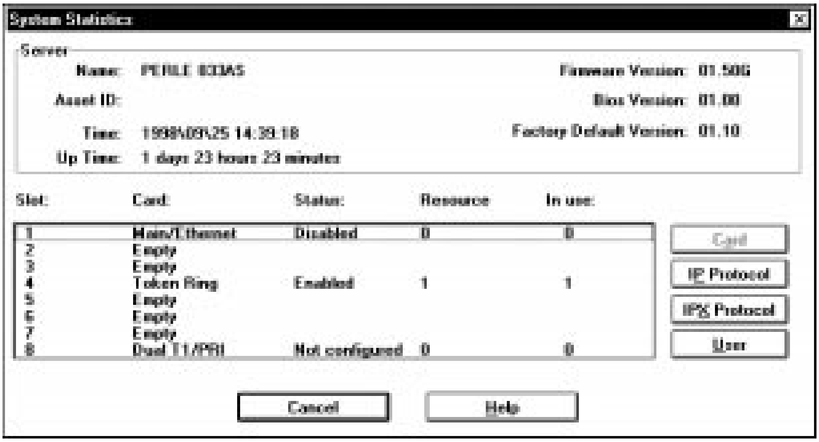
IPX Protocol

Click on this button to access the **IPX Protocol Statistics**.

Accessing Card Statistics

To access the statistics for a Feature Card:

1. Bring up the main **System Statistics** screen.
2. Highlight the **Feature Card** in the **Feature Card window**, and click on **Card**. The next screen displayed will be based on the card selected.



System Statistics

Server

Name: PERLE 833AS

Asset ID:

Time: 1998\09\25 14:39:18

Up Time: 1 days 23 hours 23 minutes

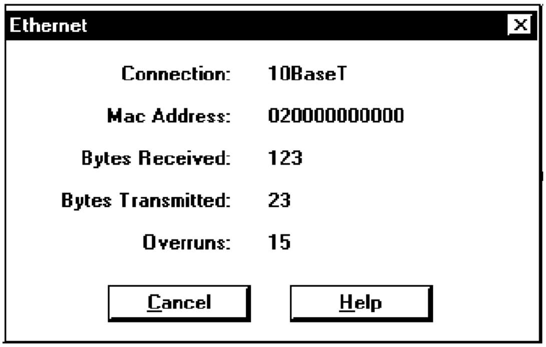
Firmware Version: 01.50G

Bios Version: 01.00

Factory Default Version: 01.10

Slot:	Card:	Status:	Resource	In use:
1	Main/Ethernet	Disabled	0	0
2	Empty			
3	Empty			
4	Token Ring	Enabled	1	1
5	Empty			
6	Empty			
7	Empty			
8	Dual T1/PRI	Not configured	0	0

System/Ethernet



Ethernet

Connection: 10BaseT

Mac Address: 020000000000

Bytes Received: 123

Bytes Transmitted: 23

Overruns: 15

Connection

The physical connection used for the Ethernet on the 833AS.

MAC Address

The MAC address configured for this Ethernet connection.

Bytes Received

The total number of bytes received by this Ethernet connection for the 833AS since last start or reset.

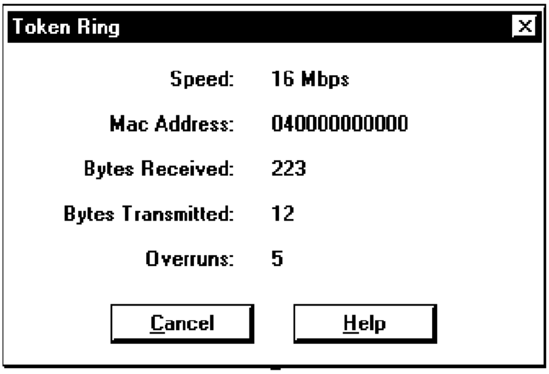
Bytes Transmitted

The total number of bytes transmitted by the 833AS on this Ethernet connection since last start or reset.

Overruns

The number of times that heavy LAN traffic caused a frame to be lost by the Ethernet interface. Overruns result in frames having to be retransmitted.

Token Ring



Speed: 16 Mbps

Mac Address: 040000000000

Bytes Received: 223

Bytes Transmitted: 12

Overruns: 5

Speed

The speed configured for this Token Ring interface.

MAC Address

The MAC address configured for this Token Ring interface.

Bytes Received

The total number of bytes received by this Token Ring connection for the 833AS since last start or reset.

Bytes Transmitted

The total number of bytes transmitted by the 833AS on this Token Ring connection since last start or reset.

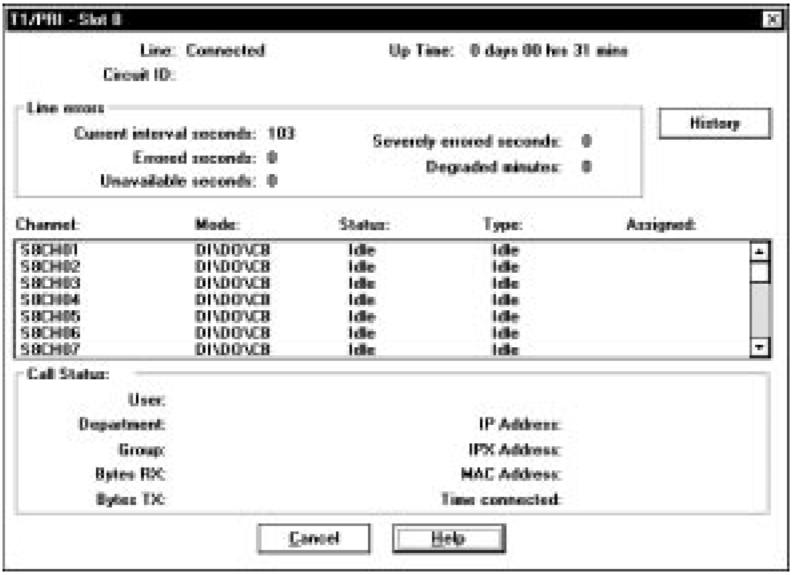
Overruns

The number of times that heavy LAN traffic caused a frame to be lost by the Token Ring interface. Overruns result in frames having to be retransmitted.

T1/PRI and E1/PRI and Dual T1/PRI and Dual E1/PRI

The statistics screen displayed is identical for both the T1/PRI interface card and the E1/PRI interface card.

If the selected card is a Dual T1/PRI or a Dual E1/PRI, you will be prompted to select the line interface before being presented with the statictics screen.



Line: Connected

Up Time: 0 days 00 hrs 31 mins

Circuit ID:

Line errors

Current interval seconds: 103

Errored seconds: 0

Unavailable seconds: 0

Severely errored seconds: 0

Degraded minutes: 0

Channel:	Mode:	Status:	Type:	Assigned:
S8CH01	DI\DO\CB	Idle	Idle	
S8CH02	DI\DO\CB	Idle	Idle	
S8CH03	DI\DO\CB	Idle	Idle	
S8CH04	DI\DO\CB	Idle	Idle	
S8CH05	DI\DO\CB	Idle	Idle	
S8CH06	DI\DO\CB	Idle	Idle	
S8CH07	DI\DO\CB	Idle	Idle	

Call Status:

User:

Department:

Group:

Bytes RX:

Bytes TX:

IP Address:

IPX Address:

MAC Address:

Time connected:

Line

Displays whether the T1 line is communicating with the Carrier Central Office. Valid statuses are:

- Connected
- Disconnected

Circuit ID

The configured Circuit ID for this line.

Up Time

The time elapsed since this Feature Card was started or reset.

Line Errors

This section displays the line error status for the current interval. By convention, line errors are counted for a 15 minute interval, after which all counts revert to 0. The errors below are calculated as defined in the SNMP RFC 1406 (Definition of Managed Objects for the DS1 and E1 Interface Types). Line error information for the previous 24 hours is available by clicking on the History button.

Current Interval Seconds

The number of seconds elapsed in the current 15 minute interval. It will be reset to 0 every 15 minutes.

Errored Seconds

Number of seconds within the current interval that any of the following error conditions occurred on the line:

- Path code violation.
- Out of frame detect.
- Controlled slip event.
- AIS defect.
- Bipolar Violation (D4, E1-no CRC links only).

Severely Errored Seconds

Number of seconds within the current interval that any of the following error conditions occurred on the line:

D4 framing

- One or more Out of frame detects.
- More than 1544 Line code violations.

ESF framing

- More than 320 Path code violations.
- One or more Out of frame detects.
- One or more AIS defects.

E1-CRC framing

- More than 832 Path code violations.
- One or more Out of frame detects.

E1-no CRC framing

- More than 2048 Line code violations.

Unavailable Seconds

Number of seconds within the current interval that the interface is unavailable.

Degraded Minutes

Number of minutes in the current interval that the estimated error rate is greater than 1E-6, but does not exceed 1E-3.

Channel Status

This area displays detailed status for each channel on the line. For each channel, the following information is displayed:

Channel

Displays channel number, and channel name as defined by configuration.

Mode

Displays the current mode for the selected channel.

If the channel is idle, the configured values for the channel will be displayed:

- DI - Dial-In.
- DO - Dial-Out.
- CB - Call Back.
- Disabled.

If the channel is in use, the valid modes are:

- Dial in.
- Dial out.
- Call back.

Status

Displays the current status for the selected channel. Valid statuses are:

Idle

Channel is not in use.

Connecting

Channel is attempting to connect.

Active

Channel is connected.

Disabled

Channel is disabled in configuration.

Type Displays the type of call for the selected channel. Valid types are:

Idle
Channel is not in use

Analog
Call is an analog call, received on a channelized T1. A modem is required.

ISDN Digital
Call is an ISDN digital call. A modem is not used.

ISDN Analog
Call is an ISDN analog (also known as ISDN voice) call. A modem is required.

Disabled
Channel is disabled in configuration.

Assigned
If the current call is an Analog or ISDN analog call, this field will display the name of the modem assigned.

Call Status This area displays User and Session information for the current call.

User

The name of the user dialed into the 833AS. Valid for dial in only.

Department

The department as configured in the User record. Valid for dial in only.

Group

If this channel has been configured to be part of a group, the group name is displayed here.

Bytes RX

The number of bytes received on this channel.

Bytes TX

The number of bytes transmitted on this channel.

IP Address

If IP protocol is being used in this connection, the IP address of the client is displayed here. Valid for dial in only.

IPX Address

If IPX protocol is being used for this connection, the IPX address of the client is displayed here. Valid for dial in only.

MAC Address

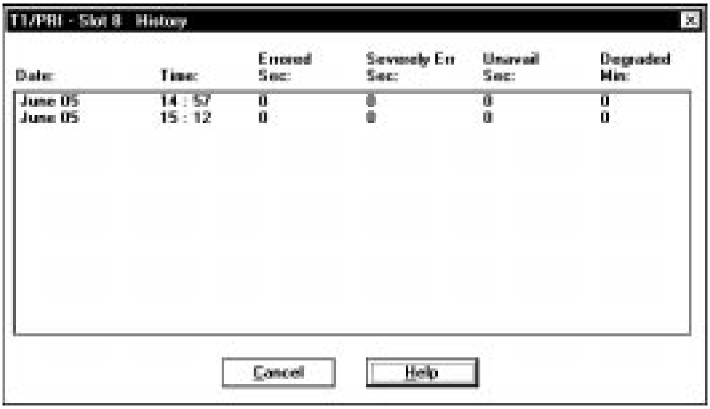
The MAC address used by the client. Valid for dial in only.

Time Connected

The time since the start of the current call.

History

This screen displays the line errors for the T1/PRI line or E1/PRI line for all the 15 minute intervals during the previous 24 hours.



T1/PRI - Slot 8 History

Date:	Time:	Errored Sec:	Severely Err Sec:	Unavail Sec:	Degraded Min:
June 05	14 : 57	0	0	0	0
June 05	15 : 12	0	0	0	0

Fields are as follows:

Date, Time

The date and time of the start of the 15 minute interval.

Errored Sec

The number of errored seconds in this interval.

Severely Err Sec

The number of severely errored seconds in this interval.

Unavail Sec

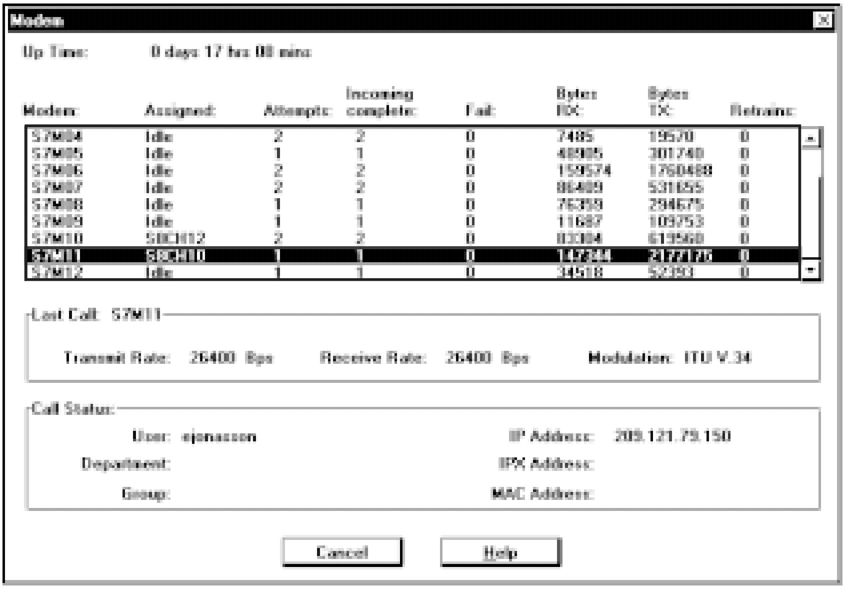
The number of unavailable seconds in this interval.

Degraded Min

The number of degraded minutes in this interval.

Modem

This screen displays statistics for the Modem Feature Card.



Up Time: 0 days 17 hrs 08 mins

Modem:	Assigned:	Attempts:	Incoming complete:	Fail:	Bytes RX:	Bytes TX:	Retrains:
S7M04	Idle	2	2	0	7485	19570	0
S7M05	Idle	1	1	0	48905	301740	0
S7M06	Idle	2	2	0	159574	1760488	0
S7M07	Idle	2	2	0	86409	531655	0
S7M08	Idle	1	1	0	76359	294675	0
S7M09	Idle	1	1	0	11687	109753	0
S7M10	S0CH12	2	2	0	83304	619560	0
S7M11	S0CH10	1	1	0	147344	2177176	0
S7M12	Idle	1	1	0	34518	52393	0

Last Call: S7M11

Transmit Rate: 26400 Bps Receive Rate: 26400 Bps Modulation: ITU V.34

Call Status:

User: ejonasson IP Address: 209.121.79.150

Department: IPX Address:

Group: MAC Address:

Up Time

The time elapsed since this Feature Card was started or reset.

Modem Status

This area displays a detailed status for each modem on the Feature Card. For each modem, the following information is displayed:

Modem

Displays modem number and name as defined by configuration.

Assigned

The following statuses are valid:

- Channel: The name of the channel to which the modem is currently assigned.
- Idle: The modem is not currently assigned to a call.
- Disabled: The modem is disabled via configuration.

Attempts

Number of incoming call attempts for this modem since card start or reset.

Incoming Complete

Number of successful incoming attempts for this modem since card start or reset. The count is incremented when the modem has completed the training sequence successfully and has indicated to the 833AS that the carrier is active.

Fail

Number of unsuccessful incoming attempts for this modem since card start or reset. The count is incremented if the modem does not complete its training sequence. This could be due to modem incompatibility, an incorrect call type (voice, fax), or a line disconnect before the training sequence completes.

Bytes RX

Number of bytes presented to the modem since card start or reset.

Bytes TX

Number of bytes transmitted by this modem since card start or reset.

Retrains

Number of retrains experienced on connections with this modem since card start or reset.

Last Call Status

This area displays status for the last call received by the modem currently selected in the Modem status window.

Transmit Rate

The transmit speed used by the modem for the last call in bits per second.

Receive Rate

The receive speed used by the modem for the last call in bits per second.

Modulation

The modulation scheme used by the modem for the last call.

Call Status

This area displays User and Session information for the selected modem in the modem status window.

User

The name of the user dialed into the 833AS. Valid for dial in only.

Department

The department as configured in the User record. Valid for dial in only.

Group

If this modem has been configured to be part of a group, the group name is displayed here.

IP Address

If IP protocol is being used in this connection, the IP address of the client is displayed here. Valid for dial in only.

IPX Address

If IPX protocol is being used for this connection, the IPX address of the client is displayed here. Valid for dial in only.

MAC Address

The MAC address used by the client. Valid for dial in only.

Time Connected

The time since the start of the current call.

Bytes RX

The number of bytes received on this modem during the current call.

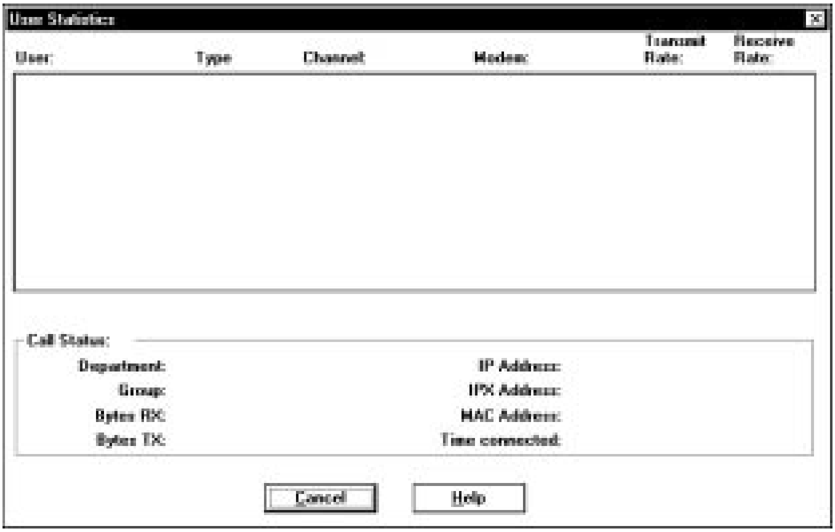
Bytes TX

The number of bytes transmitted on this modem during the current call.

User Statistics

From the statistics screen of the manager, the administrator will be able to view the session statistics on a per user basis.

The **User Statistics** screen is as follows:



User

The name of the user dialed into the 833AS. Valid for dial in only.

Modem

Displays modem number and name as defined by configuration.

Type

Displays the type of call for the selected channel.

Idle

Channel is not in use

Analog

Call is an analog call, received on a channelized T1. A modem is required.

ISDN Digital

Call is an ISDN digital call. A modem is not used.

ISDN Analog

Call is an ISDN analog (also known as ISDN voice) call. A modem is required.

Channel

Displays channel number, and channel name as defined by configuration.

Department

The department as configured in the User record. Valid for dial in only.

Group

If this modem has been configured to be part of a group, the group name is displayed here.

Bytes RX

The number of bytes received on this modem during the current call.

Bytes TX

The number of bytes transmitted on this modem during the current call.

IP Addr

If IP protocol is being used in this connection, the IP address of the client is displayed here. Valid for dial in only.

IPX Addr

If IPX protocol is being used for this connection, the IPX address of the client is displayed here. Valid for dial in only.

MAC Addr

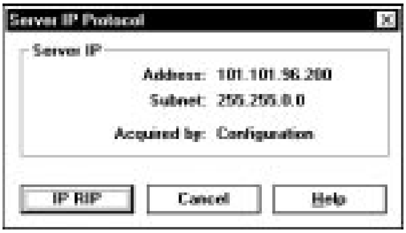
The MAC address used by the client. Valid for dial in only.

Time Connected

The time since the start of the current call.

IP Protocol

To access the statistics for the **IP protocol**, from the main System Statistics screen, click on **IP Protocol**. The following screen is displayed:



Server IP Protocol

Server IP

Address: 101.101.96.200

Subnet: 255.255.0.0

Acquired by: Configuration

Address

The IP address of the Server.

Subnet

The subnet of the Server.

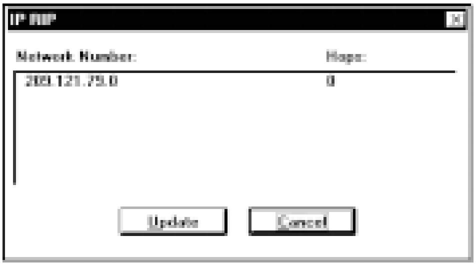
Acquired By

The method used to acquire the IP address. Valid values are:

- BOOTP: Address was acquired from a BOOTP server.
- RARP: Address was acquired from a RARP server.
- Configuration: Address was configured in the 833AS.

IP RIP

To display the contents of the **IP RIP** table, click on the **IP RIP** button on the **IP Protocol** screen. The **IP RIP** screen will be displayed.



IP RIP

Network Number:	Hops:
200.121.75.0	0

Fields are as follows:

Network Number

The network number of the network that can be accessed.

Hops

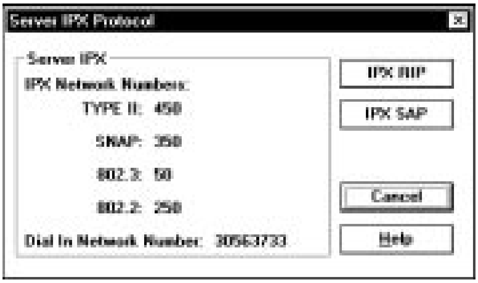
The number of routers that are between this network and the network that the 833AS is on.

Update

This button will display the updated number of RIPS in the table.

IPX Protocol

To access the statistics for the **IPX protocol**, from the main System Statistics screen, click on **IPX Protocol**. The following screen is displayed



Server IPX

IPX Network Numbers:

TYPE II: 450

SNAP: 350

802.3: 50

802.2: 250

Dial In Network Number: 30563733

Type II

The network number for Ethernet Type II frames. Field is blank if Ethernet Type II frames are not used.

SNAP

The network number for Ethernet or Token Ring SNAP frames. Field is blank if Ethernet or Token Ring SNAP frames are not used.

802.2

The network number for Ethernet or Token Ring 802.2 frames. Field is blank if Ethernet or Token Ring 802.2 frames are not used.

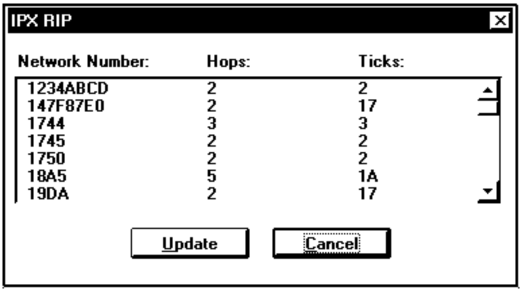
802.3

The network number for Ethernet 802.3 frames. Field is blank if Ethernet 802.3 frames are not used.

Dial In Network Number

The network number of the Dial In network.

IPX RIP To display the contents of the **IPX RIP** table, click on the **IPX RIP** button on the IPX **Protocol** screen. The **IPX RIP** screen will be displayed.



Network Number:	Hops:	Ticks:
1234ABCD	2	2
147F87E0	2	17
1744	3	3
1745	2	2
1750	2	2
18A5	5	1A
19DA	2	17

Fields are as follows:

Network Number

The network number of the network that can be accessed.

Hops

The number of routers that are between this network and the network that the 833AS is on.

Ticks

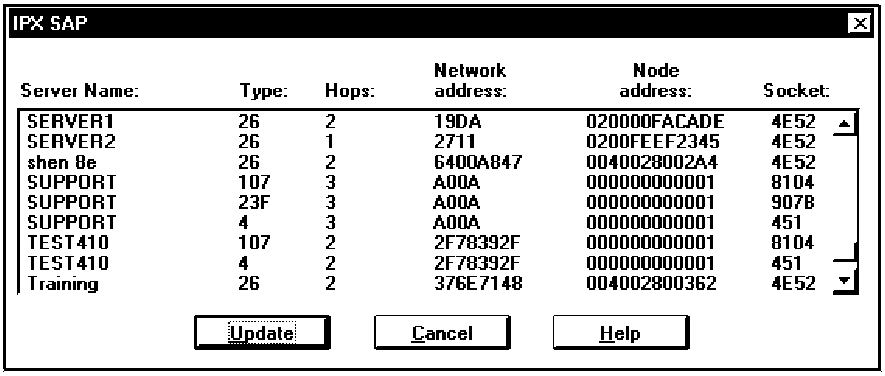
The amount of time in ticks to reach the network. A tick is equal to 55 milliseconds.

Update

This button will display the updated number of RIPS in the table.

IPX SAP

To display the contents of the **IPX SAP** table, click on the **IPX SAP** button on the main **Protocol** screen. The **IPX SAP** screen will be displayed.



Server Name:	Type:	Hops:	Network address:	Node address:	Socket:
SERVER1	26	2	19DA	020000FACADE	4E52
SERVER2	26	1	2711	0200FEEF2345	4E52
shen 8e	26	2	6400A847	0040028002A4	4E52
SUPPORT	107	3	A00A	000000000001	8104
SUPPORT	23F	3	A00A	000000000001	907B
SUPPORT	4	3	A00A	000000000001	451
TEST410	107	2	2F78392F	000000000001	8104
TEST410	4	2	2F78392F	000000000001	451
Training	26	2	376E7148	004002800362	4E52

The fields are as follows:

Server Name

The name of the Novell Server described in this entry.

Type

Type of Novell Server. These numbers are defined by Novell. Some common types of servers are:

- 3 - Print Queue
- 4 - File Server
- 5 - Job Server
- 7 - Print Server
- 9 - Archive Server
- 24h - Remote Bridge Server
- 47h - Advertising Print Server

The Perle 833AS server uses the number “26h” as its server type.

Hops

The number of routers that are between this Server and the network that the 833AS is on.

Network Address

The network address of this Server.

Node Address

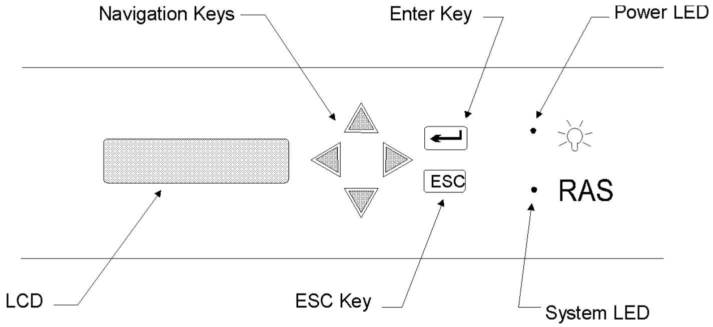
The node address of this Server.

Socket

The IPX socket number that is used to communicate with this Server.

833AS Front Panel

The Front Panel consists of a keypad and LCD display at the front of the 833AS. It is used for the initial setup of the 833AS and monitoring the operational status.



▲ 833AS Front Panel

The elements of the Front Panel are:

- 2 x 16 character backlit LCD display
- 6 key keypad. Keys are:
  - Navigation keys (left, right, up, down)
  - Enter key
  - ESC key

Power LED

Indicates that the 833AS is powered up.

System LED

Blinks continuously when the 833AS is operational.

Front Panel Modes

The Front Panel operates in two different modes, Factory Default and Normal.

If the 833AS has not yet been configured, the Front Panel is in Factory Default mode. In Factory Default mode, you have access to commands and statuses that you may require to communicate with the 833AS Manager.

Once the 833AS has been fully configured, the Front Panel is in Normal mode. In this mode, many of the statistics that are available from the 833AS Manager can be displayed on the Front Panel. You also have access to these control functions:

- Reset the entire 833AS.
- Reset a single Feature Card.
- Reset the 833AS to Factory Default mode.
- Set the IP and IPX address of the 833AS.

These control functions can be password protected to prevent unauthorized access.

Display Language

In Normal mode, the display will be in the same language as the 833AS Manager that was used to configure the unit. In Factory Default mode, the display will initially be in English. However, the display language can be changed. Available languages are:

- English
- French
- German
- Italian
- Japanese (Katakana)
- Spanish

To change the language, from the main factory default screen:

```
Perle 833AS
```

Press ▶ One of the following screens will appear:

```
No Manager
```

Or

```
Manager IP
```

Or

```
Manager IPX
```

Press **Enter**. Use ▲ ▼ keys to scroll through the languages.

Press **Enter** to confirm your choice.

Navigating the Front Panel

The keypad is used to navigate through the Front Panel displays, and edit a Front Panel field.

The front panel menu structure is provided in Appendix 2. For navigation, the keys behave as follows:

Left ◀ , ▶ Right Keys

Selects a menu.

Up ▲ , ▼ Down Keys

View entries within a menu.

Enter Key

If an item can be edited, enables the item to be edited.

ESC

Return to the previous screen.

Editing Fields

When editing a field, the keys behave as follows:

Left ◀ , ▶ Right Keys

Position the cursor to the correct editing position.

Up ▲ , ▼ Down Keys

View selections or change values at the cursor position.

Enter Key

Accept changes and exit edit mode.

ESC Key

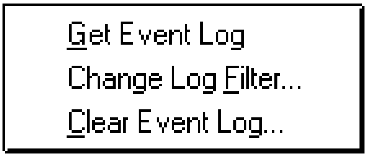
Discard changes and exit edit mode.

Event Log

The 833AS has a non-volatile Event Log that is used to track key activities in the 833AS. This user log can be uploaded to the 833AS Manager for display or printing. The following types of events are recorded:

- User access (log on, log out, and failed log on activity)
- Configuration changes through the Manager or Front Panel
- System and Feature card restarts
- Internal 833AS errors

To access the Event Log, the 833AS Manager must connect to an 833AS Server. The following operations are supported and are accessed through the Manager's Event Log menu.



Get Event Log

This will get the event log from the connected 833AS and display the data in a scrollable window. The columns in the table are date, time, event and user ID if applicable.

Change Log Filter

This command will allow you to filter the type of events recorded by the 833AS.

Clear Event Log

This will clear all the log data from the connected 833AS.

Appendix 1: Menu Descriptions and Maps

About Menu Descriptions and Maps

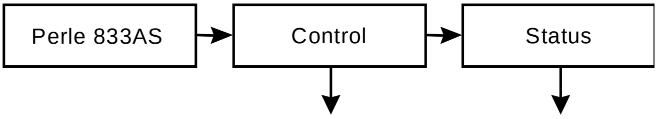
In this chapter you will read about:

- Front Panel Main Screen
- Control
- Status
- Card Type
- Network Status Display
- Factory Default Mode
- Factory Default Status

Front Panel Main Screen

Menu	Description
Control	Indicates the start of Control displays. Control is organized into System, Card, and Network control displays.
Status	Indicates the start of Status displays. Status is organized into System, Card, and Network Status displays.

Front Panel Main Screen Map



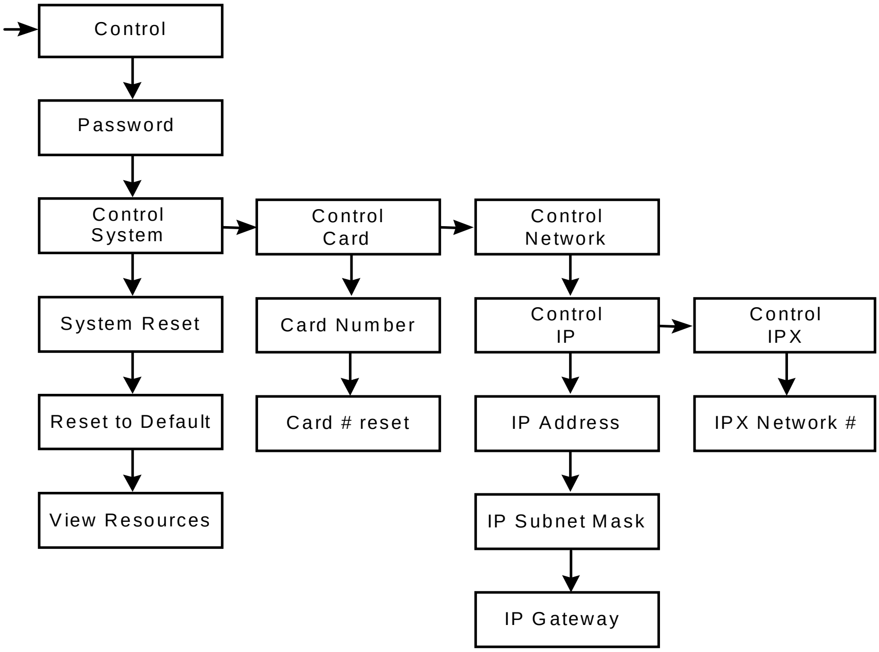
Control Menu Descriptions on page 236.
Status Menu Descriptions on page 238.

Control

Indicates the start of control displays. Control is organized into System, Card, and Network control displays.

Menu	Description
Control	**Indicates the start of Control displays. Control is organized into System, Card, and Network control displays.**
Password	If the panel lock has been defined in the Manager, the password must be entered here to access further control screens.
System	**System Control Displays**
System Reset	Causes system to restart same as the power up.
Reset to Default	Deletes current configuration, sets server to factory default mode.
View Resources	Enables display of internal resources.
Card	**Control Card Displays.**
Card Number	Select card.
Card #	Caused selected card to restart same as a power up.
Network	**Network Control Displays.**
IP	Select IP Settings.
IP Address	Set IP address of unit.
IP Subnet Mask	Set IP Subnet Mask of unit.
IP Router	Set address of IP Router if used.
IPX	Select IPX Settings.
IPX Network Number	Set IPX Network Number of unit.

Control Menu Map

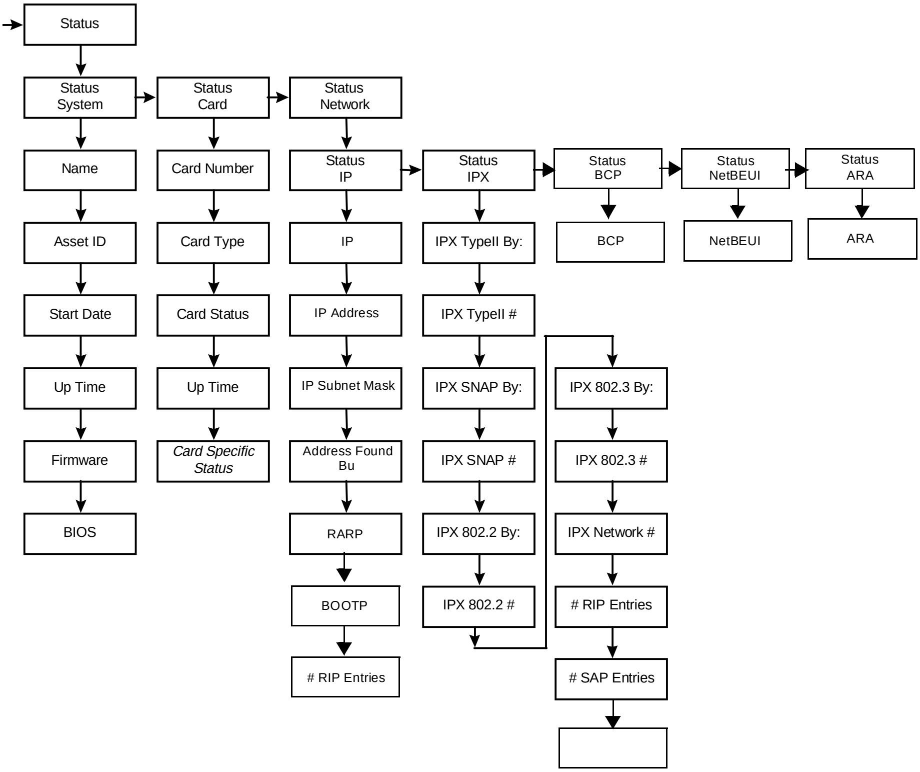


Status

Indicates the start of the Status Displays. Status is organized into System, Card, and Network Status Displays.

Menu	Descriptions
Status	**Indicates the start of Status displays. Status is organized into System, Card, and Network Status displays.**
Name	Server name as defined in configuration.
Asset ID	Asset ID as defined in configuration.
Start Date	Date unit last Start-up.
Up Time	Elapsed time since last Start-up.
Firmware	Revision of operational Firmware.
BIOS	Revision of BIOS.
Card	**Card Status Displays.**
Select Card	Choose among a range of cards.
Card Type (common)	■ System/Ethernet ■ Token Ring ■ T1/PRI ■ E1/PRI ■ Dual E1/T1 ■ PerleDSP Modem 56k ■ Perle HD 12, 18, 24, and 30 Modem For menus specific to each of the common cards see the following menu description - Card Type.
Card Status	■ Active ■ Disabled ■ No configuration ■ Configuration mismatch ■ Diagnostic failed (error code)
Card Uptime	Elapsed time since last card Start-up.

Status Menu Map



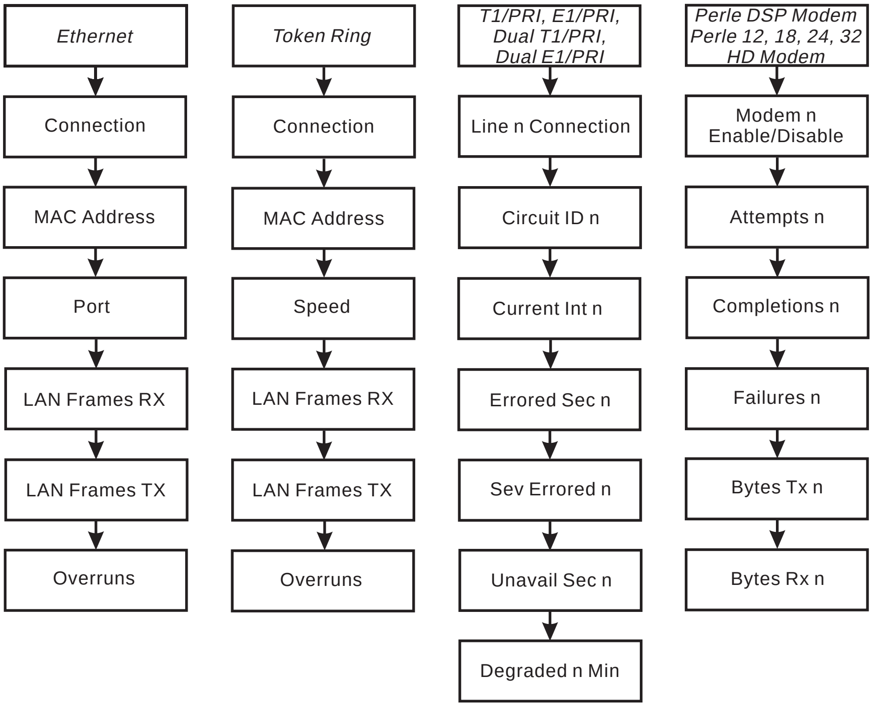
Card Type

Status specific to each card type is detailed below.

Menu	Description
Card Type	**Each of the Common Type Cards can be uniquely configured using the menu specific to that card.**
Ethernet	**Common Status.**
Connection	Indicates if the card is connected to the Ethernet network.
MAC Address	MAC address of Ethernet card.
Port	■ BNC ■ RJ-45
Frames RX	Number of frames received since last Start-up.
Frames TX	Number of frames transmitted since last Start-up.
Overruns	Number of receive overruns since last Start-up.
Token Ring	**Common Status.**
Connection	Indicates if card is connected to Token Ring network.
MAC Address	MAC address of Token Ring card.
Speed	■ 4 Mbps ■ 16 Mbps
Frames RX	Number of frames received since last Start-up.
Frames TX	Number of frames transmitted since last Start-up.
Overruns	Number of receive overruns since last Start-up.

Card Type Menu Description continues on page 242.

Card Type Menu Map



Card Type continued

Menu	Description
T1/PRI, E1/PRI, Dual T1/PRI, Dual E1/PRI	**Common Status**
Line n Connection	Indicates if card is connected to the telephone network.
Circuit ID n	Configured Circuit ID of line.
Current Int n	The following line card statistics are based on occurrences within a 15 minute interval as defined in the SNMP RFC 1406. (Definition of Managed Objects for the DS1 and E1 Interface Types. This screen displays the number of seconds elapsed in the current 15-minute interval. It will be reset to 0 every 15 minutes.
Errored Sec n	Number of seconds within the current interval that any of the following error conditions occurred: ■ Path Code Violation. ■ Out of Frame Detect. ■ Controlled Slip Event. ■ AIS Defect. ■ Bipolar Violation. (D4, E1-no CRC links only)
Sev. Errored n	Number of seconds within the current interval that any of the following error conditions occurred: D4 ■ One or more Out of frame detects. ■ More than 1544 Line code violations. ESF: ■ More than 320 Path Code Violations. ■ One or more Out of frame detects. ■ One or more AIS defects. E1-CRC ■ More than 832 Path Code Violations. ■ One or more Out of frame detects. E1-no CRC ■ More than 2048 Line code violations.

Card Type continued

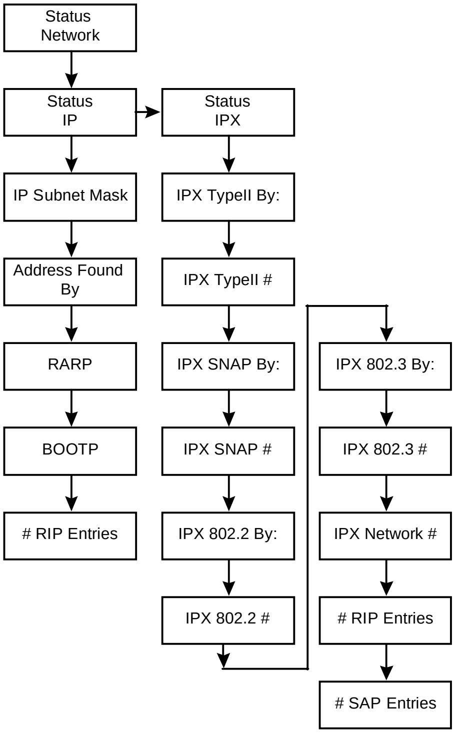
Menu	Description
Unavail Sec n	Number of seconds within the current interval that the interface is unavailable.
Degraded n Min	Number of minutes in the current interval that the estimated error rate is greater than 1E-6, but does not exceed 1E-3.
PerleDSP Modem	**Common Status.**
Modem n Enabled/ Disabled	Indicates whether the modem is enabled or disabled via configuration. The left and right keys will select the modem for the following: (n= the modem chosen)
Attempts n	Number of incoming call attempts for this modem since card Start-up.
Completions n	Number of successful incoming attempts for this modem since card Start-up. The count is incremented when the modem has completed the training sequence successfully, and has indicated to the router that carrier is active.
Failures n	Number of unsuccessful incoming attempts for this modem since card Start-up. The count is incremented if the modem does not successfully complete its training sequence. This could be due to the modem incompatibility or an incorrect call type (voice, fax).
Retrains n	Number of retrains experienced on connections with this modem since card Start-up.
Bytes Tx n	Number of bytes presented to the modem since Start-up.
Bytes Rx n	Number of bytes received from this modem since Start-up

Network Status Display

Menu	Description
IP	
IP Address	IP address of the 833AS.
IP Subnet Mask	IP subnet mask of the 833AS.
Address found by	Indicates how the IP address was determined: ■ BOOTP ■ RARP ■ Configured
RARP	Indicates whether RARP will be sent at startup to attempt to acquire the 833AS IP address.
BOOTP	Indicates whether a BOOTP request will be sent at startup to attempt to acquire the 833AS IP address.
# RIP entries	Current number of IP RIP entries.
IPX	
IPX Type II By:	Indicates how the Network Number for Type ll IPX frames was determined: ■ Automatically from network. ■ Configured ■ None (Type ll disabled)
IPX Type II #	Type ll IPX frame network number.
IPX SNAP by:	Indicates how the Network Number for SNAP IPX frames was determined: ■ Automatically from Network. ■ Configured ■ None (SNAP disabled)
IPX SNAP #	SNAP IPX frame network number.
IPX 802.2 by:	Indicates how the Network Number for the 802.2 IPX frames was determined: ■ Automatically from Network. ■ Configured ■ None (802.2 disabled)
IPX 802.2 #	802.2 IPX frame network number.

Menu	Description
IPX 802.3 by:	Indicates how the Network Number for the 802.3 IPX frames was determined: ■ Automatically from Network. ■ Configure ■ None (802.3 disabled)
IPX 802.3 #	802.3 IPX frame network number.
IPX Network Number	WAN (internal) Network Number.
#RIP entries	Current number of IPX RIP entries.
#SAP entries	Current number of IPX SAP entries.

Network Status Display Menu Map



Factory Default Mode

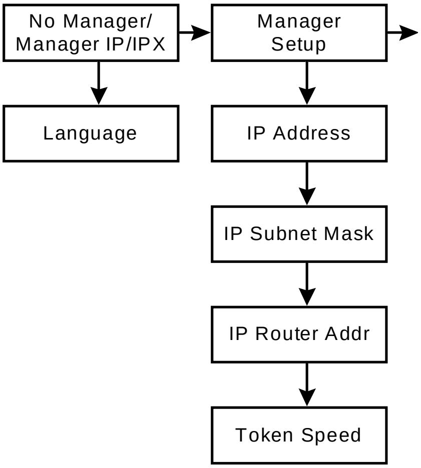
Menu	Description
Perle 833AS	Appears for 5 seconds on power up.
No Manager/ Manager IP/ Manager IPX	Indicates whether the Perle 833AS Manager is communicating with the server and which protocol is used for communication.
Language	Lets you select the language for Front Panel in Factory Mode. Choices are English, French, German, Italian, Spanish, and Japanese (Katakana).

Factory Default Setup

Provides the base configuration for the 833AS so that it can communicate with the Manager.

Menu	Description
Manager Setup	**Indicates the start of the Factory Mode Setup displays.**
IP Address	Set IP address of the unit. Will indicate “none” if none has been configured. When none appears, the 833AS will attempt to acquire an IP address by BOOTP or RARP.
IP Subnet Mask	Set IP subnet mask of unit. Will indicate “none” if none has been configured. When none appears, the 833AS will use a subnet mask of 255.255.255.0
IP Gateway Addr	Set IP default router address for the 833AS. This will be required if the 833AS is not on the same segment s the 833AS Manager.
Token Speed	Options are 4 Mbps, 16 Mbps. Will indicate “not set” if the speed has not been set by this configuration. If the speed has not been set, the 833AS will not attempt to get on the ring.

Factory Default Mode and Setup Map



.

Continues with “Factory Default Mode Menu Map” on page 250.

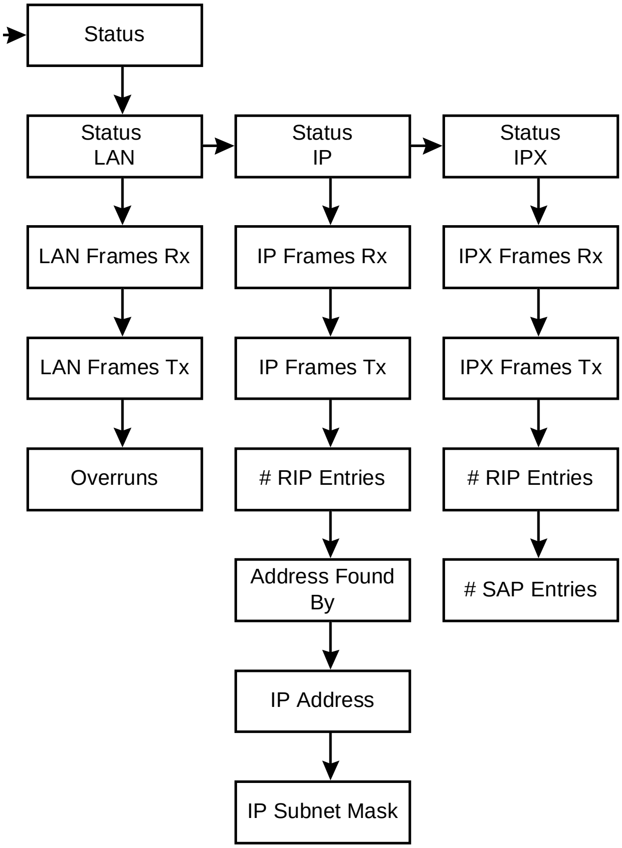
Factory Default Mode

Indicates start of Factory Default Mode Displays.

Menu	Description
LAN	
MAC address	MAC Address of the LAN adapter.
LAN Frames Rx	Number of frames received by the LAN adapter since last Start-up.
LAN Frames Tx	Number of frames transmitted by the LAN adapter since last Start-up.
Overruns	Number of receive overruns detected by the LAN adapter since last Start-up.
IP	
IP Frames Rx	Number of IP frames received since last Start-up.
IP Frames Tx	Number of IP frames transmitted since last Start-up.
# RIP Entries	Current number of IP RIP entries.
Address Found By	Indicates how the IP address was determined: ■ BOOTP ■ RARP ■ Configured ■ Default
IP Address	IP address of the 833AS.
IP Subnet Mask	IP subnet mask of the 833AS.
IPX	
IPX Frames Rx	Number of IPX frames received since last start-up.
IPX Frames Tx	Number of IPX frames transmitted since last Start-up.
# RIP entries	Current number of IPX RIP entries.
# SAP entries	Current Number of the IPX SAP entries.

Factory Default Mode Menu Map

Continued from“Factory Default Mode and Setup Map” on page 248



Appendix 2: AT Command Set

About AT Command Set

In this chapter you will read about:

- AT Commands
- Error Detection and Data Compression Commands
- S - Registers
- S - Register Definitions
- AT Command Set Summary

The modem will respond to the commands detailed below. Parameters applicable to each command are listed with the command description.

A single command string can be up to 40 characters in length, including the “AT”.

The modem behaves differently from a stand-alone modem because it does not directly interface to the telephone line. Phone call handling is by the Line card (T1/PRI or E1/PRI). Once the call is established it is switched to the modem. Therefore, modem commands that do line control (such as ATA, ATH) are not handled solely by the modem. Although there are significant differences between making a call on a T1/E1 line and a standard phone line, the 833AS will make all the necessary conversions.

AT Commands

A/ - Re-execute Command

The modem behaves as though the last command line had been re-sent by the DTE. "A/" will repeat all the commands in the command buffer.

The principal application of this command is to place another call (using the Dial command) that failed to connect due to a busy line, no answer, or a wrong number. This command must appear alone on a command line. This command should not be terminated by a carriage return.

AT= x - Write to Selected S-Register

This command writes the value x to the currently selected S-Register. An S-Register can be selected by using the ATSn command. All of the S-Registers will return the OK response if x is a number. Some registers may not be written due to country specific PTT limitations.

Result Codes

OK	For all arguments.

AT? - Read Selected S-Register

This command reads and displays the selected S-Register. An S-Register can be selected by using the ATSn command.

Result Codes:

OK	For all arguments.

A - Answer

The modem will go off-hook and attempt to answer an incoming call if correct conditions are met. Upon successful completion of answer handshake, the modem will go on-line in answer mode. Operation is also dependent upon +FCLASS command and country-specific requirements.

Bn - CCITT or Bell

When the modem is configured to allow either option, the modem will select Bell or CCITT modulation for a line speed connection of 300 or 1200 bps according to the parameter supplied. Any other line speed will use a CCITT modulation standard.

B0 Selects CCITT operation at 300 or 1200 bps during Call Establishment and a subsequent connection. (Default for W-class models.)

B1 Selects BELL operation at 300 or 1200 bps during Call Establishment and a subsequent connection. (Default for US models.)

Result Codes:

OK	n = 0 or 1.
ERROR	Otherwise.

Cn - Carrier Control

This command is included for compatibility only, and has no effect other than returning a result code. The only valid parameter is 1.

Result Codes:

OK	n = 1.
ERROR	Otherwise.

Dn - Dial

This command directs the modem to go on-line, dial according to the string entered and attempt to establish a connection. The dial process can be split into two parts.

In the first part, the call is made. Phone call handling is done by the Line card (T1/PRI or E1/PRI). The dial characters are sent to the Line card for processing. Therefore, the type of dialing done (tone, pulse, or ISDN) is under control of the Line card. The call process will be the same regardless if tone dialing (ATDT) or pulse dialing (ATDP) is specified.

Once the connection is established, the Line card notifies the Modem card. The “post dial” character can be used to have the modem send characters after the connection using tone (DTMF) signaling.

Dial Modifiers

The valid dial string parameters are described below. Punctuation characters may be used for clarity, with parentheses, hyphen, and spaces being ignored.

0-9 DTMF digits 0 to 9.

A-D DTMF digits A, B, C, and D. Some countries may prohibit sending of these digits during dialing.

T Select dialing: dial the numbers that follow until the next command is encountered. Method of dialing (tone, pulse) will be based on the configuration of the 833AS.

P Select dialing: dial the numbers that follow until the next command is encountered. Method of dialing (tone, pulse) will be based on the configuration of the 833AS.

R This command will be accepted, but not acted on.

, Dial pause: the modem will pause for a time specified by S8 before dialing the digits following ",".

; Return to command state. Added to the end of a dial string, this causes the modem to return to the command state after it processes the portion of the dial string preceding the ";". This allows the user to issue additional AT commands while remaining off-hook. The additional AT commands may be placed in the original command line following the ";" and/or may be entered on subsequent command lines. The modem will enter call progress only after an additional dial command is issued without the ";" terminator. Use "H" to abort the dial in progress, and go back on-hook.

( ) Ignored: may be used to format the dial string.

- Ignored: may be used to format the dial string.

<space> Ignored: may be used to format the dial string.

<i>	Invalid character: will be ignored.
/	The ‘post dial’ character. The modem will wait for a phone call connect before sending the characters following “/” using DTMF signaling.
*	The 'star' digit. Valid only after the post dial character.
#	The 'gate' digit. Valid only after the post dial character.
W	Wait for dial tone: the modem will wait for dial tone before dialing the digits following "W". If dial tone is not detected within the time specified, the modem will abort the rest of the sequence, return on-hook, and generate an error message. Valid only after the post dial character.
@	Wait for silence: the modem will wait for at least 5 seconds of silence in the call progress frequency band before continuing with the next dial string parameter. If the modem does not detect these 5 seconds of silence before the expiration of the call abort timer (S7), the modem will terminate the call attempt with a NO ANSWER message. If busy detection is enabled, the modem may terminate the call with the BUSY result code. If answer tone arrives during execution of this parameter, the modem handshakes. Valid only after the post dial character.
&	Wait for credit card dialing tone before continuing with the dial string. If the tone is not detected within the time specified by S7 (US models) or S6 (W-class models), the modem will abort the rest of the sequence, return on-hook, and generate an error message. Valid only after the post dial character.

En - Command Echo

The modem enables or disables the echo of characters to the DTE according to the parameter supplied.

E0	Disables command echo.
E1	Enables command echo. (Default.)

Result Codes:

OK	n = 0 or 1.
ERROR	Otherwise.

Hn - Disconnect (Hang-Up)

This command initiates a hang up sequence.

This command may not be available for some countries due to PTT restrictions.

H0 The modem will release the line if the modem is currently on-line, and will terminate any test (AT&T) that is in progress. Country specific, modulation specific, and error correction protocol specific processing is handled outside of the H0 command.

H1 If on-hook, the modem will go off-hook and enter command mode. For US models, the modem will remain off-hook. For W-class models, the modem will return on-hook after a period of time determined by S7.

Result Codes:

OK n = 0 or 1.

ERROR Otherwise.

Nn - Automode Enable

This command enables or disables automode detection.

N0 Automode detection is disabled (equivalent to setting the +MS <automode> subparameter to 0).

N1 Automode detection is enabled (equivalent to setting the +MS <automode> subparameter to 1). (Default.)

Result Codes:

OK n = 0 or 1.

ERROR Otherwise.

On - Return to On-Line Data Mode

This command determines how the modem will enter the on-line data mode. If the modem is in the on-line command mode, the enters the on-line data mode with or without a retrain. If the modem is in the off-line command mode (no connection), ERROR is reported.

00 Enters on-line data mode without a retrain. Handling is determined by the Call Establishment task. Generally, if a connection exists, this command connects the DTE back to the remote modem after an escape (+++).

01 Enters on-line data mode with a retrain before returning to on-line data mode.

Result Codes:

OK n = 0 or 1 and a connection exists.

ERROR Otherwise or if not connected.

Qn - Quiet Results Codes Control

The command enables or disables the sending of result codes to the DTE according to the parameter supplied.

Q0	Enables result codes to the DTE. (Default.)
Q1	Disables result codes to the DTE.

Result Codes:

OK	n = 0 or 1.
ERROR	Otherwise.

Sn - Read/Write S-Register

The modem selects an S-Register, performs an S-Register read or write function, or reports the value of an S-Register.

n	Establishes S-Register n as the last register accessed.
n=v	Sets S-Register n to the value v.
n?	Reports the value of S-Register n.

The parameter n can be omitted, in which case the last S-Register accessed will be assumed. The S can be omitted for AT= and AT?, in which case the last S-Register accessed will be assumed.

For example:

ATS7 establishes S7 as the last accessed register.

AT=40 sets the contents of the last register accessed to 40.

ATS=20 sets the contents of the last register accessed to 20.

Vn - Result Code Form

This command selects the sending of short-form or long-form result codes to the DTE.

V0	Enables short-form (terse) result codes. Line feed is not issued before a short-form result code.
V1	Enables long-form (verbose) result codes. (Default.)

Result Codes:

OK	n = 0 or 1.
ERROR	Otherwise.

Wn - Connect Message Control

This command controls the format of CONNECT messages.

W0 Upon connection, the modem reports only the DTE speed (e.g., CONNECT 19200). Subsequent responses are disabled. (Default.)

W1 Upon connection, the modem reports the line speed, the error correction protocol, and the DTE speed, respectively. Subsequent responses are disabled.

W2 Upon connection, the modem reports the DCE speed (e.g., CONNECT 14400). Subsequent responses are disabled.

Result Codes:

OK	n = 0, 1, or 2.
ERROR	Otherwise.

Xn - Extended Result Codes

This command selects which subset of the result messages will be used by the modem to inform the DTE of the results of commands.

Blind dialing is enabled or disabled by country parameters. If the user wishes to enforce dial tone detection, a "W" can be placed in the dial string (see D command). Note that the information below is based upon the default implementation of the X results Table 1. indicates the messages which are enabled for each X value.

If the modem is in facsimile mode the only message sent to indicate a connection is CONNECT without a speed indication.

X0 Disables monitoring of busy tones unless forced otherwise by country requirements; send only OK, CONNECT, RING, NO CARRIER, ERROR, and NO ANSWER result codes. Blind dialing is enabled/ disabled by country parameters. If busy tone detection is enforced and busy tone is detected, NO CARRIER will be reported. If dial tone detection is enforced or selected and dial tone is not detected, NO CARRIER will be reported instead of NO DIAL TONE.

X1 Disables monitoring of busy tones unless forced otherwise by country requirements; send only OK, CONNECT, RING, NO CARRIER, ERROR, NO ANSWER, and CONNECT XXXX (XXXX = rate). Blind dialing enabled/disabled by country parameters. If busy tone detection is enforced and busy tone is detected, NO CARRIER will be reported instead of BUSY. If dial tone detection is enforced or selected and dial tone is not detected, NO CARRIER will be reported instead of NO DIAL TONE.

X2 Disables monitoring of busy tones unless forced otherwise by country requirements; send only OK, CONNECT, RING, NO CARRIER, ERROR, NO DIALTONE, NO ANSWER, and CONNECT XXXX. If busy tone detection is enforced and busy tone is detected, NO CARRIER will be reported instead of BUSY. If dial tone detection is enforced or selected and dial tone is not detected, NO DIAL TONE will be reported instead of NO CARRIER.

X3 Enables monitoring of busy tones; send only OK, CONNECT, RING, NO CARRIER, ERROR, NO ANSWER, and CONNECT XXXX. Blind dialing is enabled/disabled by country parameters. If dial tone detection is enforced and dial tone is not detected, NO CARRIER will be reported.

X4 Enables monitoring of busy tones; send all messages.

Result Codes:

OK	n = 0 to 4.
ERROR	Otherwise.

Result Codes

Short Form	Long Form	n Value in ATXn Command				
		0	1	2	3	4
0	OK	x	x	x	x	x
1	CONNECT	x	x	x	x	x
2	RING	x	x	x	x	x
3	NO CARRIER	x	x	x	x	x
4	ERROR	x	x	x	x	x
5	CONNECT 1200	1	x	x	x	x
6	NO DIALTONE	3	3	x	x	x
7	BUSY	3	3	3	x	x
8	NO ANSWER	x	x	x	x	x
9	CONNECT 0600	1	x	x	x	x
10	CONNECT 2400	1	x	x	x	x
11	CONNECT 4800	1	x	x	x	x
12	CONNECT 9600	1	x	x	x	x
13	CONNECT 7200	1	x	x	x	x
14	CONNECT 12000	1	x	x	x	x
15	CONNECT 14400	1	x	x	x	x
16	CONNECT 19200	1	x	x	x	x
17	CONNECT 38400	1	x	x	x	x
18	CONNECT 57600	1	x	x	x	x
19	CONNECT 115200	1	x	x	x	x
20	CONNECT 230400	x	x	x	x	x
22	CONNECT 75TX/1200RX	1	x	x	x	x
23	CONNECT 1200TX/75RX	1	x	x	x	x
24	DELAYED	4	4	4	4	x
32	BLACKLISTED	4	4	4	4	x

Result Codes

Short Form	Long Form	n Value in ATXn Command				
33	FAX	x	x	x	x	x
35	DATA	x	x	x	x	x
40	CARRIER 300	x	x	x	x	x
44	CARRIER 1200/75	x	x	x	x	x
45	CARRIER 75/1200	x	x	x	x	x
46	CARRIER 1200	x	x	x	x	x
47	CARRIER 2400	x	x	x	x	x
48	CARRIER 4800	x	x	x	x	x
49	CARRIER 7200	x	x	x	x	x
50	CARRIER 9600	x	x	x	x	x
51	CARRIER 12000	x	x	x	x	x
52	CARRIER 14400	x	x	x	x	x
53	CARRIER 16800	x	x	x	x	x
54	CARRIER 19200	x	x	x	x	x
55	CARRIER 21600	x	x	x	x	x
56	CARRIER 24000	x	x	x	x	x
57	CARRIER 26400	x	x	x	x	x
58	CARRIER 28800	x	x	x	x	x
59	CONNECT 16800	1	x	x	x	x
61	CONNECT 21600	1	x	x	x	x
62	CONNECT 24000	1	x	x	x	x
63	CONNECT 26400	1	x	x	x	x
64	CONNECT 28800	1	x	x	x	x
66	COMPRESSION: CLASS 5	x	x	x	x	x
67	COMPRESSION: V.42 bis	x	x	x	x	x
69	COMPRESSION: NONE	x	x	x	x	x

Result Codes

Short Form	Long Form	n Value in ATXn Command				
70	PROTOCOL: NONE	x	x	x	x	x
77	PROTOCOL: LAPM	x	x	x	x	x
78	CARRIER 31200	x	x	x	x	x
79	CARRIER 33600	x	x	x	x	x
80	PROTOCOL: ALT	x	x	x	x	x
81	PROTOCOL: ALT-CELLULAR	x	x	x	x	x
84	CONNECT 33600	1	x	x	x	x
91	CONNECT 31200	1	x	x	x	x
150	CARRIER 32000	x	x	x	x	x
151	CARRIER 34000	x	x	x	x	x
152	CARRIER 36000	x	x	x	x	x
153	CARRIER 38000	x	x	x	x	x
154	CARRIER 40000	x	x	x	x	x
155	CARRIER 42000	x	x	x	x	x
156	CARRIER 44000	x	x	x	x	x
157	CARRIER 46000	x	x	x	x	x
158	CARRIER 48000	x	x	x	x	x
159	CARRIER 50000	x	x	x	x	x
160	CARRIER 52000	x	x	x	x	x
161	CARRIER 54000	x	x	x	x	x
162	CARRIER 56000	x	x	x	x	x
165	CONNECT 32000	x	x	x	x	x
166	CONNECT 34000	x	x	x	x	x
167	CONNECT 36000	x	x	x	x	x
168	CONNECT 38000	x	x	x	x	x
169	CONNECT 40000	x	x	x	x	x

Result Codes

Short Form	Long Form	n Value in ATXn Command				
170	CONNECT 42000	x	x	x	x	x
171	CONNECT 44000	x	x	x	x	x
172	CONNECT 46000	x	x	x	x	x
173	CONNECT 48000	x	x	x	x	x
174	CONNECT 50000	x	x	x	x	x
175	CONNECT 52000	x	x	x	x	x
176	CONNECT 54000	x	x	x	x	x
177	CONNECT 56000	x	x	x	x	x
+F4	+FCERROR	x	x	x	x	x

Notes:

An 'x' in a column indicates that the message (either the long form if verbose, or the value only for short form) will be generated when that particular value of 'n' (shown at the top of the column) has been selected by the use of ATXn. If the column is blank, then no message will be generated for that x option. A numeral indicates which less explicit message (verbose or short form) will be output for that X option.

AT& Commands

&Cn - RLSD (DCD) Option

The modem controls the RLSD output in accordance with the parameter supplied.

&C0 RLSD remains ON at all times.

&C1 RLSD follows the state of the carrier. (Default.)

Result Codes:

OK n = 0 or 1.

ERROR Otherwise.

&F - Restore Factory Configuration (Profile)

The modem loads the factory default configuration (profile). The factory defaults are identified for each command and in the S-Register descriptions. A configuration (profile) consists of a subset of S-Registers.

&FRestore Factory Configuration

Result Codes:

OK

ERRORIf the modem is connected.

&Rn - RTS/CTS Option

This selects how the modem controls CTS. CTS operation is modified if hardware flow control is selected (see &K command).

&R0	In sync mode, CTS tracks the state of RTS. In async mode, CTS is normally ON and will turn OFF only if required by flow control.
&R1	In sync mode, CTS is always ON (RTS transitions are ignored). tracks the state of RTS; In async mode, CTS is normally ON and will turn OFF only if required by flow control.

Result Codes:

OK	n = 0 or 1.
ERROR	Otherwise.

&V - Display Current Configuration and Stored Profiles

Reports the current (active) configuration. Note that there will be settings displayed that are reserved. You should not attempt to change the reserved settings.

Result Code:

OK

Example:

```
AT&V
ACTIVE PROFILE:
B0 E1 L1 M1 N1 QO T V1 W0 X4 Y0 &C0 &D0 &G2 &J0 &K3 &Q5 &R1 &S0
&T4 &X0 &Y0
S00:002 S01:000 S02:043 S03:013 S04:010 S05:008 S06:002 S07:030 S08:002
S09:006
S10:014 S11:255 S12:050 S18:000 S25:005 S26:001 S36:007 S37:000 S38:020
S46:138
S48:007 S95:000

OK
```

&V1 - Display Last Connection Statistics

Displays the last connection statistics in the following format (shown with typical results):

```
Termination Reason            Link Disconnect Or Local Request
LAST TX data rate             33600 BPS
HIGHEST TX data rate           33600 BPS
LAST RX data rate              28800 BPS
HIGHEST RX data rate            28800 BPS
Error correction PROTOCOL      LAPM
Data COMPRESSION                V42Bis
Line QUALITY                   030
Highest SPX RX state            068
Highest SPX TX state            067
```

AT% Commands

%En - Enable/ Disable Auto-Retrain or Fallback/ Fall Forward

Controls whether or not the modem will automatically monitor the line quality and request a retrain (%E1) or fall back when line quality is insufficient or fall forward when line quality is sufficient (%E2).

If enabled, the modem attempts to retrain for a maximum of 30 seconds.

%E0 Disable auto-retrain.
%E1 Enable auto-retrain.
%E2 Enable fallback/fall forward. (Default.)

Result Codes:

OK n = 0, 1, or 2.
ERROROtherwise.

AT\ Commands

\Kn - Break Control

Controls the response of the modem to a break received from the DTE or the remote modem or the \B command according to the parameter supplied.

The response is different in three separate states.

The first state is where the modem receives a break from the DTE when the modem is operating in data transfer mode:

\K0 Enter on-line command mode, no break sent to the remote modem.

\K1 Clear data buffers and send break to remote modem.

\K2 Same as 0.

\K3 Send break to remote modem immediately.

\K4 Same as 0.

\K5 Send break to remote modem in sequence with transmitted data. (Default.)

The second case is where the modem is in the on-line command state (waiting for AT commands) during a data connection, and the \B is received in order to send a break to the remote modem:

\K0 Clear data buffers and send break to remote modem.

\K1 Clear data buffers and send break to remote modem. (Same as 0.)

\K2 Send break to remote modem immediately.

\K3 Send break to remote modem immediately. (Same as 2.)

\K4 Send break to remote modem in sequence with data.

\K5 Send break to remote modem in sequence with data. (Same as 4.) (Default.)

The third case is where a break is received from a remote modem during a non-error corrected connection:

\K0 Clears data buffers and sends break to the DTE.

\K1 Clears data buffers and sends break to the DTE. (Same as 0.)

\K2 Send a break immediately to DTE.

\K3 Send a break immediately to DTE. (Same as 2.)

\K4 Send a break in sequence with received data to DTE.

\K5 Send a break in sequence with received data to DTE. (Same as 4.) (Default.)

Result Codes:

OK	n = 0 to 5.
ERROR	Otherwise.

\Nn - Operating Mode

This command controls the preferred error correcting mode to be negotiated in a subsequent data connection.

\N0 Selects normal speed buffered mode (disables error-correction mode).

\N1 Same as \N0.

\N2 Selects reliable (error-correction) mode. The modem will first attempt a LAPM connection and then an MNP connection. Failure to make a reliable connection results in the modem hanging up.

\N3 Selects auto reliable mode. This operates the same as \N2 except failure to make a reliable connection results in the modem falling back to the speed buffered normal mode.

\N4 Selects LAPM error-correction mode. Failure to make an LAPM error-correction connection results in the modem hanging up. Note: The -K1 command can override the \N4 command.

\N5 Selects MNP error-correction mode. Failure to make an MNP error-correction connection results in the modem hanging up.

Result Codes:

OK	n = 0 to 5.
ERROR	Otherwise.

AT+ Commands

+MS - Select Modulation

This extended-format command selects the modulation, optionally enables or disables automode, and optionally specifies the lowest and highest connection rates using one to three subparameters.

+MS= <od> [,[<automode>][,[<min_rate>][,[<max_rate>][,[ ]]]]]<CR>

Notes:

Subparameters not entered (enter a comma only or <CR> to skip the last subparameter) remain at their current values.

Reporting Selected Options

The modem can send a string of information to the DTE consisting of selected options using the following command:

+MS?

The response is:

+MS: <mod>,<automode>,<min_rate>,<max_rate>

There may be additional values displayed after the <max_rate> field, but they are not applicable.

For example,

+MS: 56,1,300,56000

Reporting Supported Options

The modem can send a string of information to the DTE consisting of supported options using the following command:

+MS=?

The response is:

+MS: (list of supported <mod> values), (list of supported <automode> values), (list of supported <min_rate> values),
(list of supported <max_rate> values)

For example,

+MS: (0,1,2,3,9,10,11,56, 64,69),(0,1),(300-33600),(300-56000)

There may be additional values displayed after the <max_rate> field, but they are not applicable.

Subparameter Definitions

1. <mod> = A decimal number which specifies the preferred modulation (automode enabled) or the modulation (automode disabled) to use in originating or answering a connection. The options are:

<mod>	Modulation	Possible Rates (bps) [1]	Notes
0	V.21	300	
1	V.22	1200	
2	V.22 bis	2400 or 1200	
3	V.23	1200	See Note 2
9	V.32	9600 or 4800	
10	V.32 bis	14400, 12000, 9600, 7200, or 4800	
11	V.34	33600, 31200, 28800, 26400, 24000, 21600, 19200, 16800, 14400, 12000, 9600, 7200, 4800, or 2400	
56	K56flex	56000, 54000, 52000, 50000, 48000, 46000, 44000, 42000, 40000, 38000, 36000, 34000, 32000	[default]
12	V.90	56000, 54667, 53333, 52000, 50667, 49333, 48000, 46667, 45333, 42667, 41333, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000	
64	Bell 103	300	
69	Bell 212	1200	

Notes:

1. See optional <automode>, <min_rate>, and <max_rate> subparameters.

2. For V.23, originating modes transmit at 75 bps and receive at 1200 bps; answering modes transmit at 1200bps and receive at 75 bps. The rate is always specified as 1200 bps.

The modem may also automatically switch to another modulation (automode), subject to the following constraints:

a. The modem may not be able to automatically switch from the current modulation (specified by <mod>) to some other modulation. For example, there is no standard way to automode from Bell 103 to V.23.

b. The DTE may disable automode operation (see <automode> below).

c. The DTE may constrain the range of modulations available by specifying the lowest and highest rates (see <min_rate> and <max_rate> below).

4. <automode> is an optional numeric value which enables or disables automatic modulation negotiation using V.8 bis/V.8 or V.32 bis Annex A. The options are:

<automode>	Option Selected	Notes
0	Automode disabled	
1	Automode enabled using V.8 bis/V.8 or V.32 Annex A	Default

The default value is 1, which enables automode. Note, however, there are modulations for which there is no automatic negotiation, e.g., Bell 212 (<mod> = 69).

For <automode> = 0 (automode disabled, i.e., fixed modulation):

a. If <max_rate> is within the rates supported by the selected modulation, the selected rate is that specified by <max_rate>. For example:

+MS=10,0,1200,4800 selects V.32 bis 4800 bps fixed rate.

b. If <max_rate> is greater than the highest speed supported by the modulation specified by <mod>, the starting rate is the highest rate supported by the selected modulation. For example:

+MS=10,0,2400,14400 selects V.32 bis 14400, 12000, 9600, 7200, or 4800 bps.

c. To select fixed mode operation, specify the <max_rate> and <min_rate> both to be the (same) requested speed, and <mod> to be the modulation for that speed. For example:

+MS=11,0,16800,16800 selects V.34 16800 bps fixed mode

+MS=10,0,12000,12000 selects V.32 bis 12000 bps fixed mode

For <automode> = 1 (automode enabled, i.e., automatically selected speed and modulation):

The modem connects at the highest possible rate in accordance with V.8 bis/V.8, or V.32 bis Annex A if V.8 bis/V.8 is not supported by the remote modem.

d. If <max_rate> is greater than the highest rate supported by the modulation specified by <mod>, the modem automodes down from the highest rate of the selected modulation. For example:

e. +MS=10,1,1200,24000 selects automoding down from V.32 bis 14400 bps.

6. <min_rate> is an optional number which specifies the lowest rate at which the modem may establish a connection. The value is decimal coded, in units of bps, e.g., 2400 specifies the lowest rate to be 2400 bps. The default is 300 for 300Êbps.

<max_rate> is an optional number which specifies the highest rate at which the

modem may establish a connection. The value is decimal coded, in units of bps, e.g., 14400 specifies the highest rate to be 14400 bps. The default is 28800 for 28800 bps.

Error Detection and Data Compression Commands

AT% Commands

%C - Enable/ Disable Data Compression

Enables or disables data compression negotiation. The modem can only perform data compression on an error corrected link.

%C0	Disables data compression.
%C1	Enables MNP 5 data compression negotiation.
%C2	Enables V.42 bis data compression.
%C3	Enables both V.42 bis and MNP 5 data compression. (Default.)

Result Codes:

OK	n = 0, 1, 2, or 3.
ERROR	Otherwise.

AT\ Commands

\An - Select Maximum MNP Block Size

The modem will operate an MNP error corrected link using a maximum block size controlled by the parameter supplied.

\A0	64 characters.
\A1	128 characters. (Default.)
\A2	192 characters.
\A3	256 characters.

Result Codes:

OK	n = 0 to 3.
ERROR	Otherwise.

\Bn - Transmit Break to Remote

In non-error correction mode, the modem will transmit a break signal to the remote modem with a length in multiples of 100 ms according to parameter specified. If a number in excess of 9 is entered, 9 is used. The command works in conjunction with the \K command.

In error correction mode, the modem will signal a break through the active error correction protocol, giving no indication of the length.

\B1-\B9Break length in 100 ms units. (Default = 3.) (Non-error corrected mode only.)

Result Codes:

OK If connected in data modem mode.

NO CARRIERIf not connected or connected in fax modem mode.

Note: When the modem receives a break from the remote modem, break is passed to the DTE as follows: In non-error correction mode direct, the break length is passed; in non-error correction mode normal and in error correction mode, a 300 ms break is passed.

-Kn - MNP Extended Services

Enables or disables conversion of a V.42 LAPM connection to an MNP 10 connection.

-K0 Disables V.42 LAPM to MNP 10 conversion. (Default.)

-K1 Enables V.42 LAPM to MNP 10 conversion.

-K2 Enables V.42 LAPM to MNP 10 conversion; inhibits MNP Extended Services initiation during V.42 LAPM answer mode detection phase.

Result Codes:

OK n = 0 or 2.

ERROR Otherwise.

–SEC=n - Enable/ Disable MNP10-EC

Enables or disables MNP10-EC operation. The command format is:

-SEC=n,[<tx level>]where <tx level> is the optional transmit level sub parameter.

-SEC=0 Disable MNP10-EC;

-SEC=1,[<tx level>]Enable MNP10-EC; the transmit level will be defined by the sub parameter <tx level> range 0 to 30 (0 dBm to -30 dBm)

Result Codes:

OK n=0, 1, or 1 and <tx level>=0 to 30

ERROR Otherwise

Example: AT-SEC=1,18 enables MNP10-EC and sets the transmit level to -18 dBm.

Note: If AT-SEC=0, the modem will automatically set AT-SEC=1 if the remote modem indicates Cellular in the V.8 bis/V.8 phase or if a Cellular Driver is loaded and the Cell Phone is attached.

Inquiries

AT-SEC?Retrieves the current -SEC command settings, e.g., 1,18.

S-Registers

The S-Registers are summarized in along with their default values. Registers or register fields quoted as “reserved” are reserved for current or future use by the Firmware, or are permanently overridden by PTT limitations.

Register Summary

Register	Function	Range	Units	Saved	Default**
S3	Carriage Return Character	0-127	ASCII		13
S4	Line Feed Character	0-127	ASCII		10
S5	Backspace Character	0-255	ASCII		8
S6	Wait Time for Dial Tone	2-255	s	*	2
S7	Wait Time for Carrier	1-255	s	*	50
S8	Pause Time for Dial Delay Modifier	0-255	s	*	2
S9	Carrier Detect Response Time	1-255	0.1 s	*	6
S10	Carrier Loss Disconnect Time	1-255	0.1 s	*	14
S11	DTMF Tone Duration	50-255	0.001 s	*	95
S12	Reserved				
S13	Reserved				
S14	Reserved				
S15	Reserved				
S16	Reserved				
S17	Reserved				
S18	Reserved				
S19	Reserved				
S20	Reserved				
S21	Reserved				
S22	Reserved				

Register Summary

Register	Function	Range	Units	Saved	Default**
S23	Reserved				
S24	Reserved				
S25	Reserved				
S26	Reserved				
S27	Reserved				
S28	Reserved				
S29	Reserved				
S30	Reserved				
S31	Reserved				
S32	Reserved				
S33	Reserved				
S34-S35	Reserved				
S36	LAPM Failure Control	-	-	*	7
S37	Reserved				
S38	Reserved				
S39	Reserved				
S40	Reserved				
S41	Reserved				
S42-S45	Reserved				
S46	Data Compression Control	-	-	*	138
S48	V.42 Negotiation Control	-	-	*	7
S86	Call Failure Reason Code	0-255	-		-

* Register value may be stored in one of two user profiles with the &W command.

S-Register Definitions

S3 - Carriage Return Character

Sets the command line and result code terminator character. Pertains to asynchronous operation only.

Range: 0-127, ASCII decimal
Default: 13 (Carriage Return)

S4 - Line Feed Character

Sets the character recognized as a line feed. Pertains to asynchronous operation only. The Line Feed control character is output after the Carriage Return control character if verbose result codes are used.

Range: 0-127, ASCII decimal
Default: 10 (Line Feed)

S5 - Backspace Character

Sets the character recognized as a backspace. Pertains to asynchronous operation only. The modem will not recognize the Backspace character if it is set to a value that is greater than 32 ASCII. This character can be used to edit a command line. When the echo command is enabled, the modem echoes back to the local DTE the Backspace character, an ASCII space character and a second Backspace character; this means a total of three characters are transmitted each time the modem processes the Backspace character.

Range: 0-32, ASCII decimal
Default: 8 (Backspace)

S6 - Wait Time for Dial Tone Before Blind Dialing, or After “W” Dial Modifier (W-Class Models)

1. Sets the length of time, in seconds, that the modem will wait before starting to dial after going off-hook when blind dialing. This operation, however, may be affected by some ATX options according to country restrictions. The "Wait for Dial Tone” call progress feature (W dial modifier in the dial string) will override the value in register S6.
2. For W-class models, S6 sets the length of time, in seconds, that the modem will wait for dial tone when encountering a “W” dial modifier before returning NO DIAL TONE result code.

The modem always pauses for a minimum of 2 seconds, even if the value of S6 is less than 2 seconds.

Range: 2-255 seconds
Default: 2

S7 - Wait Time For Carrier After Dial, For Silence, or For Dial Tone After "W" Dial Modifier

1. Sets the length of time, in seconds, that the modem will wait for carrier before hanging up. The timer is started when the modem finishes dialing (originate), or 2 seconds after going off-hook (answer). In originate mode, the timer is reset upon detection of answer tone if allowed by country restrictions.
2. Sets the length of time, in seconds, that modem will wait for silence when encountering the @ dial modifier before continuing with the next dial string parameter.
3. For US models, S7 sets the length of time, in seconds, that the modem will wait for dial tone when encountering a "W" dial modifier before continuing with the next dial string parameter.

Range:	1-255 seconds
Default:	50

S8 - Pause Time For Dial Delay

Sets the time, in seconds, that the modem must pause when the "," dial modifier is encountered in the dial string.

Range:	0-255 seconds
Default:	2

S9 - Carrier Detect Response Time

Sets the time, in tenths of a second, that the carrier must be present before the modem considers it valid and turns on RLSD. As this time is increased, there is less chance to detect a false carrier due to noise from the telephone line.

Range:	1-255 tenths of a second
Default:	6 (0.6 second)

S10 - Lost Carrier To Hang Up Delay

Sets the length of time, in tenths of a second, that the modem waits before hanging up after a loss of carrier. This allows for a temporary carrier loss without causing the local modem to disconnect. When register S10 is set to 255, the modem functions as if a carrier is always present.

The actual interval the modem waits before disconnecting is the value in register S10 minus the value in register S9. Therefore, the S10 value must be greater than the S9 value or else the modem disconnects before it recognizes the carrier.

Range:	1-255 tenths of a second
Default:	14 (1.4 seconds)

S11 - DTMF Tone Duration

Sets the duration of tones in DTMF dialing.

Range:	50-255 milliseconds
Default:	95 (95 milliseconds)

S36 - LAPM Failure Control

Default: 7 (00000111b)

Bits 0-2 This value indicates what should happen upon a LAPM failure. These fallback options are initiated immediately upon connection if S48=128. If an invalid number is entered, the number is accepted into the register, but S36 will act as if the default value has been entered.

0 = Modem disconnects.

1 = Modem stays on-line and a Direct mode connection is established.

2 = Reserved.

3 = Modem stays on-line and a Normal mode connection is established.

4 = An MNP connection is attempted and if it fails, the modem disconnects.

5 = An MNP connection is attempted and if it fails, a Direct mode connection is established.

6 = Reserved.

7 = An MNP connection is attempted and if it fails, a Normal mode connection is established. (Default.)

Bits 3-7 Reserved

S46 - Data Compression Control

Controls selection of compression. The following actions are executed for the given values:

Range: 136 or 138

Default: 138

S46=136 Execute error correction protocol with no compression.

S46=138 Execute error correction protocol with compression. (Default.)

S48 - V.42 Negotiation Action

The V.42 negotiation process determines the capabilities of the remote modem. However, when the capabilities of the remote modem are known and negotiation is unnecessary, this process can be bypassed if so desired.

Range: 0, 7, or 128 If an invalid number is entered, it is accepted into the S-Register, but S48 will act as if 128 has been entered.

Default: 7

S48=0 Disable negotiation; bypass the detection and negotiation phases; and proceed with LAPM.

S48=7 Enable negotiation. (Default.)

S48=128 Disable negotiation; bypass the detection and negotiation phases; and proceed at once with the fallback action specified in S36. Can be used to force MNP.

S86 - Call Failure Reason Code

When the modem issues a NO CARRIER result code, a value is written to this S-Register to help determine the reason for the failed connection. S86 records the first event that contributes to a NO CARRIER message. The cause codes are:

Range: 0, 4, 5, 9, 12, 13, or 14

Default:

S86=0 Normal disconnect, no error occurred.

S86=4 Loss of carrier.

S86=5 V.42 negotiation failed to detect an error-correction modem at the other end.

S86=9 The modems could not find a common protocol.

S86=12 Normal disconnect initiated by the remote modem.

S86=13 Remote modem does not respond after 10 re-transmissions of the same message.

S86=14 Protocol violation.

AT Command Set Summary

Basic AT Commands

Command	Function
A/	Re-execute command.
A	Go off-hook and attempt to answer a call.
B0	Select V.22 connection at 1200 bps.
B1	Select Bell 212A connection at 1200 bps.
C1	Return OK message.
Dn	Dial modifier.
E0	Turn off command echo.
E1	Turn on command echo.
F0	Select auto-detect mode (equivalent to N1). (RC144)
F1	Select V.21 or Bell 103. (RC144)
F2	Reserved. (RC144)
F3	Select V.23 line modulation. (RC144)
F4	Select V.22 or Bell 212A 1200 bps line speed. (RC144)
F5	Select V.22 bis line modulation. (RC144)
F6	Select V.32 bis or V.32 4800 line modulation. (RC144)
F7	Select V.32 bis 7200 line modulation. (RC144)
F8	Select V.32 bis or V.32 9600 line modulation. (RC144)

F9 Select V.32 bis 12000 line modulation. (RC144)

F10 Select V.32 bis 14400 line modulation. (RC144)

SPEAKER ON DURING ANSWERING.

N0 Turn off automode detection.

N1 Turn on automode detection.

O0 Go on-line.

O1 Go on-line and initiate a retrain sequence.

Q0 Allow result codes to DTE.

Q1 Inhibit result codes to DTE.

Sn Select S-Register as default.

Sn? Return the value of S-Register n.

=v Set default S-Register to value v.

? Return the value of default S-Register.

T Force DTMF dialing.

V0 Report short form (terse) result codes.

V1 Report long form (verbose) result codes.

W0 Report DTE speed in EC mode.

W1 Report line speed, EC protocol and DTE speed.

W2 Report DCE speed in EC mode.

X0 Report basic call progress result codes, i.e., OK, CONNECT, RING, NO CARRIER (also, for busy, if enabled, and dial tone not detected), NO ANSWER and ERROR.

X1 Report basic call progress result codes and connections speeds (OK, CONNECT, RING, NO CARRIER (also, for busy, if enabled, and dial tone not detected), NO ANSWER, CONNECT XXXX, and ERROR.

X2 Report basic call progress result codes and connections speeds, i.e., OK, CONNECT, RING, NO CARRIER (also, for busy, if enabled, and dial tone not detected), NO ANSWER, CONNECT XXXX, and ERROR.

X3 Report basic call progress result codes and connection rate, i.e., OK, CONNECT, RING, NO CARRIER, NO ANSWER, CONNECT XXXX, BUSY, and ERROR.

X4 Report all call progress result codes and connection rate, i.e., OK, CONNECT, RING, NO CARRIER, NO ANSWER, CONNECT XXXX, BUSY, NO DIAL TONE and ERROR.

&C0 Force RLSD active regardless of the carrier state.

&C1 Allow RLSD to follow the carrier state.

&F Restore factory configuration.

&R0 CTS tracks RTS (async) or acts per V.25 (sync).

&R1 CTS is always active.

&S0 DSR is always active.

&V Display current configurations.

&V1 Display connection statistics

%E0 Disable line quality monitor and auto retrain.

%E1 Enable line quality monitor and auto retrain.

%E2 Enable line quality monitor and fallback/fall forward.

\Kn Controls break handling during three states:

- When modem receives a break from the DTE:

  \K0,2,4 Enter on-line command mode, no break sent to the remote modem.

  \K1 Clear buffers and send break to remote modem.

  \K3 Send break to remote modem immediately.

  \K5 Send break to remote modem in sequence with transmitted data.

- When modem receives \B in on-line command state:

  \K0,1 Clear buffers and send break to remote modem.

  \K2,3 Send break to remote modem immediately.

  \K4,5 Send break to remote modem in sequence with transmitted data.

- When modem receives break from the remote modem:

  \K0,1 Clear data buffers and send break to DTE.

  \K2,3 Send a break immediately to DTE.

  \K4,5 Send a break with received data to the DTE.

  \N0 Select normal speed buffered mode.

  \N1 Select direct mode.

  \N2 Select reliable link mode.

  \N3 Select auto reliable mode.

  \N4 Force LAPM mode.

  \N5 Force MNP mode.

  +MS Select modulation.

ECC Commands

%C0	Disable data compression.
%C1	Enable MNP 5 data compression.
%C2	Enable V.42 bis data compression.
%C3	Enable both V.42 bis and MNP 5 compression.
\A0	Set maximum block size in MNP to 64.
\A1	Set maximum block size in MNP to 128.
\A2	Set maximum block size in MNP to 192.
\A3	Set maximum block size in MNP to 256.
\Bn	Send break of n x 100 ms.

MNP 10 Commands

-K0	Disable MNP 10 extended services.
-K1	Enable MNP 10 extended services.
-K2	Enable MNP 10 extended services detection only.
-SEC=0	Disable MNP10-EC.
-SEC=1,[<tx level>]	Enable MNP10-EC and set transmit level <tx level> 0 to 30 (0 dBm to -30 dBm).

FAX Class 2

+FCLASS=n	Service class.
+FAA=n	Adaptive answer.
+FAXERR	Fax error value.
+FBOR	Phase C data bit order.
+FBUF?	Buffer size (read only).
+FCFR	Indicate confirmation to receive.
+FCLASS=	Service class.
+FCON	Facsimile connection response.
+FCIG	Set the polled station identification.
+FCIG:	Report the polled station identification.
+FCR	Capability to receive.
+FCR=	Capability to receive.
+FCSI:	Report the called station ID.
+FDCC=	DCE capabilities parameters.
+FDCS:	Report current session.
+FDCS=	Current session results.
+FDIS:	Report remote capabilities.
+FDIS=	Current sessions parameters.
+FDR	Begin or continue phase C receive data.

+FDT=	Data transmission.
+FDTC:	Report the polled station capabilities.
+FET:	Post page message response.
+FET=N	Transmit page punctuation.
+FHNG	Call termination with status.
+FK	Session termination.
+FLID=	Local ID string.
+FLPL	Document for polling.
+FMDL?	Identify model.
+FMFR?	Identify manufacturer.
+FPHCTO	Phase C time out.
+FPOLL	Indicates polling request.
+FPTS:	Page transfer status.
+FPTS=	Page transfer status.
+FREV?	Identify revision.
+FSPL	Enable polling
+FTSI:	Report the transmit station ID.

Appendix 3: Specifications

Dimensions

Height x Width x Depth	222 x 435 x 425 mm 8.75 x 17.25 x 16.75 inches
Weight	15 kg/ 33 lbs maximum

Physical/Electrical Specifications

Ambient Temperature	10^{o} - 30^{o} C 50^{o} - 80^{o} F
Relative Humidity	20% - 80%, non condensing
Power	100 - 125 VAC, 50 - 60 Hz, 2 A 200 - 240 VAC, 50 - 60 Hz, 1 A
BTU Output	400 BTU/hour maximum
MTTR	30 minutes
MTBF	100,000 hours

Chassis

- 8 slots, front loading
- 1 System/Ethernet card
- Add up to 4 T1 or 4 E1 Line cards.
- Add up to 5 PerleDSP Modem cards.
- Add up to 1 Token-Ring card.

Power Supply

- Dual redundant supply

LCD Panel

- 2 rows by 16 characters backlit display

Keypad

- 6 keys used for system setup and status inquiry.

Status LEDs

- Power
- System Active
- Additional Status LEDs on Feature Cards.

System/Ethernet Card

- Provides system control and Ethernet functions.
- 10/100 Mbps Ethernet Network interface with hardware MAC address range filtering.

Ethernet Protocols Supported

- 10Base-2
- 10Base-T
- 100Base-TX

Physical Interfaces

- BNC
- RJ45
- DB9 Service port

Ethernet LAN Wiring Supported

- 10Base-T: Category 3, 4, 5 Unshielded Twisted Pair
- 10Base-2: 50 ohm Thin Ethernet coaxial cable
- 100Base-TX: Category 5 Unshielded Twisted Pair or Type 1 shielded twisted pair

Memory

- 8 meg RAM
- 2 SIMM sockets for RAM expansion.
- 4 meg Flash for Firmware storage.
- 128K non volatile log

Other

- Link Connect LED

T1/PRI Feature Card

- Network interface 4 Wire PRI
- Network connector RJ48C Female

Pin 1 = Receive (Tip)

Pin 2 = Receive (Ring)

Pin 3 = Grounded

Pin 4 = Transmit (Tip)

Pjn 5 = Transmit (Ring)

Pin 6 = Grounded

Pin 7 = OPEN

Pin 8 = OPEN

LEDs

- Red alarm
- Yellow alarm
- Blue alarm

Network Interface Mode

- CSU (DS1) - Drive capability 6000 feet on 22AWG.
- DSX-1 - Drive capability 500 feet

Line build out

- CSU
  - 0 dB
  - -7.5 dB
  - -15 dB
  - -22.5 dB
- DSX-1

  - 0-133 ft.
  - 133-266 ft.
  - 266-399 ft.
  - 399-533 ft.
  - 533-655 ft.

- Remote Loopback supported

Framing Formats

- D4 (SF)
- ESF

Line Formats

- AMI
- B8ZS
- JBZS

Signaling Supported

- Robbed Bit
  - E & M Wink Start
  - E & M Delay Start
  - E & M Immediate Start
  - FXS Loop Start
  - FXS Ground Start
  - SAS Loop Start
  - SAS Ground Start
- Q.931/Q.921 message based

Dialing Modes Supported

- Q.931/Q.921 message based
- Pulse dial
- Tone dial (DTMF) supported
  - *PerleDSP Modem card required for Tone dial*

ISDN Network Protocols Supported

- US NI-2
- AT&T TR 41449 (4ESS, 5ESS)
- NT DMS100, DMS250
- Japan INSnet 1500
- V.120

Facilities Data Link Supported

- AT&T
- ANSI

E1/PRI Feature Card

- Network interface RJ48C Female

Pin 1 = Receive (Tip)

Pin 2 = Receive (Ring)

Pin 3 = Grounded

Pin 4 = Transmit (Tip)

Pjn 5 = Transmit (Ring)

Pin 6 = Grounded

Pin 7 = OPEN

Pin 8 = OPEN

- Network Interface ISDN PRI 120 ohm

LEDs

- Red alarm
- Yellow alarm
- Blue alarm

Framing Formats

- CRC4
- No-CRC4

Line Formats

- HDB3

Signaling Supported

- Q.931/Q.921 message based

Dialing Modes Supported

- Q.931/Q.921 message based

ISDN Network Protocols Supported

- EuroISDN ETSI NET5
- ITR6
- V.120

PerleDSP Modem Feature Card

Data Modulations Supported

- 56K (K56flex, Central Site mode)
  - 56K modulation will be supported for dial in applications only. Maximum baud rate for dial out applications is 33.6K
- V.34 (28.8K)
- V.34 Annex 12 (33.6K)
- V.32
- V.32 bis
- V.22 bis
- V.22A/B
- V.23
- V.21
- Bell 212A
- Bell 103

Fax Modulations Supported

- V.17
- V.21 channel 2
- V.27 ter
- V.29
- V.33

Other modem protocols

- V.42 LAPM error correction
- MNP Class 2-4 error correction
- MNP 10 error correction
- V.42 bis data compression
- MNP Class 5 data compression
- T.30 Fax protocol
- Facsimile Class 2

Other

- mu-Law and A-Law Supported
- DTMF Signaling Supported

Token Ring Feature Card

- 4/16 Mbps Token Ring Network interface with hardware MAC address range filtering.
- Link connect LED.

Physical Interface

- RJ45
- DB15

Token Ring LAN Wiring Supported

- Shielded twisted pair types 1, 2, 6, 9
- Unshielded twisted pair type 3, 4, 5

Approvals

CE Mark

Safety

- CSA Standard C22.2, No. 0M-1982 - General Requirements Canadian Electrical Code, Part II
- CSA Standard C22.2, No. 0.4-M1982 - Bonding and Grounding of Electrical Equipment (Protective Grounding)
- CSA Standard C22.2, No. 220M-1986 - Information Processing and Business Equipment
- UL Standard UL 1950 (Fourth Edition) - Electronic Data Processing Equipment
- TUV Rheinland (GS Mark) -DIN Standard DIN VDE 0805/05.90\EN60950/1988
- IEC 950 (1991) Second Edition with Amendments 1, 2, 3 and 4

Emissions

- Department of Communications (DOC) - DOC Radio Interference Regulations C.R.C., c.1374
- Federal Communications Commission (FCC) - FCC Rules and Regulations Part 15, Subpart J, Class A
- VCCI
- EN55022, CISPR 22
- EN 50082-1: 1992 (EMC Directive 89/336/EEC)
- AS/NZS 3548: 1995 Class A

Telephony

- CE Telecommunications

- FCC Part 68
- DOC CS03
- JATE
- European Harmonized Standard I-CTR4 (94/796/EC)
- European Technical Standard NET 5 (CTR4)
- German National Standard BAPT 223 ZV 25
- Australian Communications Authority Technical Standard: TS-038 (1997)
- Telecom New Zealand Limited: PTC 232/98/006

Protocols Supported

Network

- IPX
- SPX
- IP
- TCP
- UDP
- Netbeui
- LLC2

Note: Other protocols (example - Lantastic) can be supported by bridging via LLC2

WAN

- PPP
  - Link Control Protocol
  - Network Control Protocols: IPCP, IPXCP
  - Header Compression Protocols: IP-VJ, CIPX
- MP
- ARA

Security

- Password Authentication Protocols (PAP/CHAP)

LAN Environments

- Novell Netware 3.x and 4.x
- Windows NT Advanced Server
- Windows for Workgroups
- IBM OS/2 LAN Server
- Microsoft LAN Manager
- UNIX
- IBM Hosts (AS/400, Mainframe)
- Lantastic
- Appleshare Server

Dial In Clients Supported

- Perle Remote
- Microsoft Dial Up Networking
- Apple Remote Access
- Any PPP client compliant with PPP standards in "Supported RFCs"

Dial-Out

- Perle Dial-Out Client Supported

Emulated Interfaces

- DOS
  - INT14
  - Novell NASI/NACI
- Windows 3.x/95/98/NT 4.0
  - Windows Communication Interface (COM port redirection)

Security

PPP

- PAP, CHAP
- Call back authentication
- Password aging function

Authorization Servers

- Novell Netware Bindery, NDS
- RADIUS
- Windows NT Domain

Token Authorization

- Security Dynamics SecureID
- Axent

Management

- 833AS Manager connected via IPX or IP enables configuration and management through LAN and dial up
- Manager supported on Windows 3.x/95/98/NT Workstation
- SNMP support
- DHCP support
- IP address pooling
- MAC address pooling
- DNS/WINS remote user assignment
- Static and dynamic IP and IPX routing tables supported.

RFCs Supported

- RFC 1144 - Compressing TCP/IP Headers for Low-Speed Serial Links.
- RFC 1157 - A Simple Network Management Protocol. (SNMP)
- RFC 1213 - Management Information Base for Network Management of TCP/IP Internets: MIB II.
- RFC 1332 - The PPP Internet Protocol Control Protocol. (IPCP)
- RFC 1334 - PPP Authentication Protocols.
- RFC 1406 - Definitions of Managed Objects for the DS1 and E1 Interface Types.
- RFC 1471 - The Definitions of Managed Objects for the Link Control Protocol

of Point-to-Point Protocol.

- RFC 1541 - Dynamic Host Configuration Protocol.
- RFC 1552 - The PPP Internetwork Packet Exchange Control Protocol. (IPXCP)
- RFC 1553 - Compressing IPX Headers Over WAN Media. (CIPX)
- RFC 1570 - PPP LCP Extensions.
- RFC 1573 - Evolution of the Interface Groups of MIB-II.
- RFC 1638 - PPP Bridging Control Protocol. (BCP)
- RFC 1643 - Definitions of Managed Objects for Ethernet-like Interface Types.
- RFC 1659 - Definitions of Managed Objects for RS-232-like Hardware Devices using SMIv2.
- RFC 1661 - The Point-to-Point Protocol. (PPP)
- RFC 1696 - Modem Management Information Base (MIB) using SMIv2.
- RFC 1742 - AppleTalk Management Information Base II.
- RFC 1743 - IEEE 802.5 MIB using SMIv2.
- RFC 1990 - The PPP Multilink Protocol. (MP)
- RFC 2127 - ISDN Management Information Base using SMIv2.

Appendix 4: RADIUS Server Attributes

Account Request Messages

This section describes the attributes which will be included by the 833AS when requesting authentication from a RADIUS server.

Number	Name	Description
1	User-Name	The name of the user to be authenticated.
2	User-Password	The password of the user to be authenticated when using PAP.
3	CHAP-Password	The encrypted password when using CHAP.
5	NAS-Port	Port number of connection being authenticated.
30	Called-Station-Id	The phone number that the caller used.
31	Calling-Station-Id	The phone number from which the call originated.
32	NAS-Identifier	The name of 833AS making the request.
60	CHAP-Challenge	CHAP challenge sent to client by the 833AS.
61	NAS-Port-Type	Identifies the type of connection the user has. Support types include: 0 = Async (Analog connection) 2 = ISDN Sync (Digital, PPP connection) 3 = ISDN Async V. 120 (Digital connection)

Access-Accept Messages

This section describes the attributes which will be accepted by the 833AS from a RADIUS authentication server in response to an authentication request. The values returned will override any values currently in use. This includes values derived from a record in the local user database or from the default user record.

Number	Name	Description
6	Sevice-Type	The type of service to be provided. Supported values include: 2 = Framed 4 = Callback Framed 6 = Administrative 11 = Callback Administrative
7	Framed-Protocol	The link layer protocol to be used by this user. Supported values include: 1 = PPP
8	Framed-IP-Address	The IP address to be assigned to this user.
9	Framed-IP-Netmask	The subnet to be assigned to this user.
10	Framed-Routing	Indicates how RIPS will be handled if user is defined as a LAN-to-LAN node. Supported values include: 0 = None 1 = Send routing packets 2 = Listen for routing packets 3 = Send and listen
11	Filter-ID	The name of a filter to be applied to this user.
13	Framed-Compression	Compression protocol to be used on the link. Supported values include: 0 = None 1 = VJ TCP/IP header compression 2 = IPX header compression
19	Callback-Number	The number at which the user should be called back.

Number	Name	Description
22	Framed-Route	Routing information to be configured for the user. This would identify any networks that can be reached by this node. The format of this field is: nn.nn.nn.nn [/yy] vv.vv.vv.vv m nn = destination network yy = number of bits to use for subnet (optional) vv = router IP address (0 = use address assigned to router by 833AS) m = hop count
25	Class	This value is sent to the accounting server unmodified by the 833AS.
27	Session-Timeout	Maximum number of seconds the user will be allowed to stay logged on.
28	Idle-Timeout	Maximum number of consecutive seconds with no link activity before the connection is terminated.

Accounting Messages

This section describes the attributes which will beincluded by the 833AS when sending an accounting message to the RADIUS server.

Number	Name	Description
40	Acct-Status-Type	Indicates if this is the beginning or end of a session. Supported values include: 1 = Start 2 = Stop
41	Acct-Delay-Time	Number of seconds the 833AS has been attempting to send this accounting event.
42	Acct-Input-Octets	Number of bytes which were received from the client during this session.[1]
43	Acct-Output-Octets	Number of packets which were transmitted to the client during this session.[1]
44	Acct-Session-ID	A string which identifies the session. The same string must be used in the start and stop messages.
45	Acct-Authentic	Method used to authenticate the user. Supported values include: 1 = RADIUS
46	Acct-Session-Time	Number of seconds for which the user has been connected in this session.[1]
47	Acct-Input-Packets	Number of packets which were received from the client during this session.[1]
48	Acct-Output-Packets	Number of packets which were transmitted to the client during this session.[1]

49	Acct-Terminate-Cause	Indicates how the session was terminated. Supported values include:[1] 1 = User Request 2 = Lost Carrier 3 = Lost Service 4 = Idle Timeout 5 = Session Timeout 14 = Port Suspended 16 = Callback

[1] This attribute is only valid in an accounting message where the *Acct-Status-Type* is set to **Stop**.

Glossary

3270

A class of IBM terminals and printers used in SNA Networks.

5250

A class of IBM terminals used in mid-range environments. e.g. AS/400

AIS (Alarm Indication Signal)

This is a signal transmitted downstream indicating that an error has been detected upstream.

AMI (Alternate Mark Inversion)

A line coding format used in T-1 transmission systems that alternately inverts successive marks. (reverse polarity of the previous mark)

Analog

Refers to telecommunication and/or switching that is not digital. e.g. voice communication over the phone. Computers require digital, therefore computers require modems to communicate over voice grade telephone lines.

ANSI

American National Standards Institute

ARA (Apple Remote Access)

Apple’s dial-in client software for Mac users allowing them remote access with other servers.

Asset ID

A way to identify a server.

Async Control

Allows you to select control characters that are prohibited from transmission. A technique where control characters are converted into non-control characters for transmission and then converted back at the destination.

AT command

Also known as the Hayes Standard AT Command Set. A language that allows PC communication software to get an asynchronous and Hayes-compatible modem to do what you want it to.

ATP (AppleTalk Transaction Protocol)

A transport level protocol that provides reliable, connection oriented, and sequenced data transfer.

AUI (Autonomous Unit Interface)

Refers to the 15 pin D type connector and cables that connects single and multiple channel equipment to an Ethernet transceiver.

Axent

A software based security server that provides user authentication using their SecureNet Key cards.

B8ZS (Binary 8 Zero Substitution)

A method of meeting the ones density requirement for digital T-carrier facilities that allows 64kbps clear data for each channel. Instead of inserting a 1 for every 7 zero’s, two violations of the bipolar encoding technique are inserted.

Base MAC Address

This is the base address for the address range filter. The address is a 12 hex digit value that ends in 00. The legal values are 020000000000 to 02FFFFFFFF00 for Ethernet, and 400000000000 to 40FFFFFFFF00 for Token Ring.

Beacon

A Token Ring frame that has been sent by an adapter after it has detected a serious problem on the ring. i.e. a broken cable. *see Beaconing*

Beaconing

When a Token Ring adapter has sent a beacon frame indicating a serious network problem, it is said to be beaconing. *See beacon*

Bindery

A Novell NetWare database that contains information about users, servers, groups and other elements.

BNC (Bayonet-Neill-Concelman connector)

A small coaxial connector with a half twist locking shell that is used on the Ethernet.

BOOTP (BOOTstrap Protocol)

A single BOOTP message specifies many of the items used at start-up, including IP address, the address of the gateway, and the address of the server.

BRI (Basic Rate Interface)

One of two interfaces in ISDN. Also called the 2B+D interface. Consists of 2 bearer B channels and a data D channel. *See ISDN and PRI*

Bridge

A Network Device that connects two networks so that devices on one network can communicate with devices on the other network. Sometimes called a *Filtering Bridge. See Router.*

Burned In Address

An address installed at the time of manufacture that cannot be altered.

Call Back

A Security feature where the Perle 833AS calls back the User at a predetermined number defined in the User's account. *See Fixed and Roaming Call Back*

CBCP (Call Back Control Protocol)

A call back protocol defined by a RFC.

Central Site

A generic term that refers to the Perle 833AS that you are using.

Channel

Usually what you rent from the Telephone Company. Acts like an individual telephone line and has a defined frequency response, gain, and bandwidth. Also known as circuit, facility, line or link.

Channelized

The division of a channel into smaller channels so that it can carry more information.

CHAP (Challenge Handshake Authentication Protocol)

Standard authentication protocol for PPP connections. It provides a higher level of security than PAP and should be used whenever possible. *see PAP*

Community

A community is a group of users having a defined Name and a defined Access level.

Compression

A method of reducing the representation of information without reducing the information itself. Saves transmission time.

Configure

The method of arranging hardware and software to determine what the system will do.

CRC4

A frame format used with E1 lines.

CSU (Channel Service Unit)

A device that connects a digital telephone line to a multiplexer, bridge or router.

D4

A channel bank that serves as an interface between the T-1 carrier and an analog device such as an analog PBX. *see analog, PBX*

Database

A collection of information or data organized in an efficient way to allow quick and easy access to that information.

Default

Refers to the factory set software settings and configurations.

Demark Point

The point of demarcation and connection between the telephone company's communication hardware and the hardware of the subscriber. Also know as *demarcation point*.

DHCP (Dynamic Host Configuration Protocol)

A TCP/IP protocol that provides static and dynamic address allocation and management.

Dial In

The process of attaching to a local network from a remote client that is using dial-in software.

Dial Mode

Either Tone or Pulse.

Dial Out

The process of attaching to a remote server from a local device that is using dial-out software.

Digital

On and Off signalling. A form of Binary Code where On is represented by 1 and Off by 0. All computer communication is in digital form. Other forms of communication not in digital must be converted to digital before they are accepted by the computer. Digital is the opposite of Analog. *See Modem*

Disabled

No longer functioning.

DSX-1 (Digital Signal Cross Connect Level 1)

Refers to a set of parameters for cross connecting DS-1 lines.

DTMF Tones (Dual Tone Multi-Frequency)

Touch-tone dialing.

Dynamic

Refers to Hardware or Software that can respond instantly to changes as they occur.

E & M

A trunking arrangement used for two way switch to switch or switch to network connections.

Emulation

When a piece of hardware or software acts like another in order to allow a program written for one computer to work on another computer.

Encapsulate

The carrying of frames of one protocol as data in another. TCP/IP is an encapsulating protocol.

Errored Seconds

Number of seconds within the current interval (a 15 minute period) that errors have occurred.

ESF (Extended Superframe)

This is a T-1 format that uses the 193 bit as a framing bit. Its frames use 24 bits instead of the previous standard of 12. This results in error information to be stored and retrieved easily.

Ethernet

A high-speed (10Mbps,100Mbps) cable technology that connects devices to a LAN, using one or more sets of communication protocols.

FDL (Facilities Data Link)

Allows the phone company to diagnose the operation of the line by requesting information and tests from the terminating equipment. The mode used should be supplied by the phone company.

Feature Card

An optional circuit board addition that increases the capabilities of the 833AS. The card can be installed by the reseller. Available cards are Token Ring, T1,E1, PerleDSP12 and PerleDSP18 Modem.

Fixed Call Back

A method where the number used for call back is contained within the 833AS database.

Frame

A group of data bits organized in a specific format. These groups are sent serially and contain flags at each end to indicate the beginning and end of the frame.

Framing

An error control procedure. Used on digital multiplexed channels.

FXS (Foreign Exchange Station)

A service that provides local telephone service from a central office that is outside of the user’s exchange area.

Gateway

Can be described as an entrance and exit to a Network. A Gateway has its own processor and memory and is used to connect two or more networks at the upper protocol layers of the OSI reference model. The networks can use different protocols and different physical media.

Ground Start

A method of signalling where one side of a two wire trunk is momentarily grounded to obtain a dialtone.

HDB3 (High Density Bipolar 3)

A Bipolar coding method that allows no more than three consecutive zeros.

IEEE (Institute of Electrical and Electronic Engineers)

A standard setting body that sets specifications for and relating to LAN’s.

Internal Pool

A database contained within the memory of the Perle 833AS.

IP (Internet Protocol)

A protocol that manages the routing of data packets between stations on the same or different networks.

IPX (Internet Packet eXchange)

A network transfer protocol from Novell, Inc.

ISDN (Integrated Services Digital Network)

A public telecommunications network that supplies end to end digital telecommunications services that can be used for both voice and non-voice data. See *BRI and PRI*

IP Subnet Mask

see *subnet mask*

JB7 (Jam Bit 7)

A zero suppression format.

JBZS (Jammed Bit Zero Substitution)

Coding format for T1.

LAN (Local Area Network)

A Network system that does not use Long Distance carriers. A LAN is usually limited by cable length restrictions.

Line Errors

The errors are calculated as defined in the SNMP RFC 1406 (Definition of Managed Objects for the DS1 and E1 Interface Types).

Logical Link Control (LLC)

The IEEE 802.2 Standard that corresponds to the ISO model's Data Link layer. LLC covers station-to-station connections, generation of message frames, and error control.

Local Security

Uses the user ID and password stored within the 833AS User database. When the remote Client connects, it will communicate with the 833AS using either the CHAP or PAP security protocols.

Loop Start

A way of starting a phone line. Commonly found in residential installations. When the phone is taken off the hook a DC loop is formed. This is detected by the phone company.

MAC (Media Access Code)

The lower half the data link layer specified in 802.3. It contains the specification for the LAN frame format and the rules for accessing the hardware of the network.

MAU (Multistation Access Unit)

A wiring concentrator used in LAN's. It allows PCs', printers, and other devices to be connected in a star-based configuration to a Token Ring or Ethernet.

Modem (MODulate/DEMmodulate)

A device that translates digital signals to a modulated form so that it can be transmitted over a telephone line. The modem can also reverse this process and receive signals.

Modem Initialization String

A series of commands sent to the modem by a communications program at start up and before a number has been dialed. These commands tell a modem how to set itself up in order to communicate easily with another modem.

Multicast

The broadcasting of messages to a specified group of workstations on a LAN, WAN, or internet.

Multiplexing

The transmission of two or more signals over a single channel.

NAK (Negative Acknowledgment)

A communication control character sent by the receiving destination indicating that the last message was not received correctly.

NDIS (Network Driver Interface Support)

A device driver specification that supports both MS-DOS and OS/2. By offering protocol multiplexing it allows multiple protocol stacks to coexist on the same host. *see protocol stack*

NetBEUI (NetBIOS Extended User Interface)

A transport layer driver often used by Microsoft's LAN Manager, Windows for Workgroups and Windows NT.

NetBIOS (Network Basic/Input Output System)

A Software system originally developed by IBM and Sytek that links network software to network adaptors. For a non-IBM network operating system to run an application that works with NetBIOS, it must have a NetBIOS emulator. *see emulation*

Network Broadcast Address

Network broadcast messages are used to inform systems on the network about the structure of the network. The Network Broadcast Address is the address used to send and receive these messages.

Network Number

The part of an Internet Address that indicates the network that the host belongs to.

OSI (Open Systems Interconnection model)

A model developed by the ISO used to define network architecture.

Packet

A unit of data transmitted on a network. Sometimes referred to as a *frame.*

PAP (Password Authentication Protocol)

Standard authentication protocol for PPP connections. *see CHAP*

PBX (Private Branch eXchange)

A smaller version of the telephone company's switching network for voice and data that is located on the customers site and owned by the customer.

PPP (Point to Point Protocol)

A form of transmission using telephone lines. It provides router to router and host to network connections. These connections can be over either synchronous or asynchronous circuits.

PRI (Primary Rate Interface)

One of two interface's in ISDN. Consists of 23B, or bearer channels and one D, or data channel. *see BRI and ISDN*

Protocol

A set of rules for exchanging data across a network.

Protocol Filter

Allows a network bridge to be programmed to send or reject transmissions according to specified protocols.

Protocol Stack

A set of protocol layers that provides reliable communication between one computer and another or a network. *see protocol*

Rack Mount

Supplied with the unit. Allows the 833AS to be mounted on a rack.

RADIUS (Remote Authentication Dial In Users Services)

An open standard network security server that communicates in both CHAP and PAP protocols.

RARP (Reverse Address Resolution Protocol)

A low level TCP/IP protocol used by a workstation to obtain the logical IP address of a node.

Remote Node Support

The ability of the 833AS to treat a remote user as if they were in "the office". By dialing in they become part of the LAN.

RFC (Request for Comment)

Standards, procedures and specifications for various TCP/IP protocols.

RIP (Routing Information Protocol)

A protocol that allows gateways and hosts to exchange information about various routes to different networks.

RISC (Reduced Instruction Set Computer)

A microprocessor architecture that simplifies the operating commands of a device to enable it to operate at high speeds.

RJ11

The most common telephone jack in the world. Used for voice transmissions.

RJ-45

A jack used for data transmissions over a standard telephone wire.

RJ-48C

An 8 position keyed plug used for connecting T-1 circuits.

Roaming Call Back

A method where the client supplies the number for call back when they dial in.

Robbed Bit Signalling

A technique where small signal bits are buried in a voice channel. These amounts are so small that they do not effect the quality of voice transmission.

Router

A device that connects Lans' at the network level and directs calls to applications. Like a bridge except that it can examine network addresses and determine the most efficient path for a frame to reach its destination. *See Bridge*

SAP (Service Advertising Protocol)

A protocol used by Novell NetWare devices to broadcast their names, addresses, and current state on the network.

Security Dynamics SecurID

A third party Token system security device.

SNAP (Subnetwork Access Protocol)

This is an Internet protocol that lets you use non-standard protocols. It is a mechanism that will distinguish one protocol from another.

SNMP (Simple Network Management Protocol)

A protocol for managing network devices.

Sockets

An interface for communicating between a user application program and TCP/IP.

Standard Profile

Used to define the user and their access to the network.

Static Routing

A route that you have manually entered in your routing table. This route then takes precedence over any dynamic routing protocol.

STP (Shielded Twisted Pair)

Twisted pair wiring that is enclosed in a metal foil sheath to limit interference.

Subnet Mask

The IP network mask. Identifies the device's IP address, which portion constitutes the network address and which portion constitutes the host address.

Support

A term that indicates that a particular piece of hardware or software is either included with your computer or will work with it.

TCP (Transmission Control Protocol)

A protocol that organizes packets, manages their transmission and ensures their accurate delivery to the receiving station. Usually combined with IP to produce TCP/IP.

TCP/IP

A protocol suite developed by the U.S. Department of Defense. Used to connect different types of computers while providing data correction, security, and reliability.

Thinnet

A term used to describe thin Ethernet coaxial cable.

Time Division Multiplexing

A method of transmitting a number of different data types (voice, video or data) together over one communications medium. The various data types are reconstructed at the destination end of transmission as separate and distinct signals. This method saves money by using fewer phone lines.

Token Ring

A LAN that conforms to the IEEE 802.5 Token Ring Access Method standard.

Trigger Character

A character that force the transmission of a network packet. Data characters accumulate in packets when they are received from the phone line or sent from a modem. A packet is sent out when a trigger character is encountered, when a character time-out or packet time-out occurs, or when a packet is filled.

UTP (Unshielded Twisted Pair)

A cable that has one or more pairs of twisted insulated copper conductors bound inside a single plastic sheath.

WAN (Wide Area Network)

A communication network that connects geographically separated areas.

Wink Start

A short duration off- hook signal that indicates that data is ready to be received.

ZBTSI (Zero Byte Time Slot Interchange)

Used by the ESF format. The ESF frame contains information about the location of all-zero bytes in the data stream.

Index

All italic page numbers refer to glossary entries