

833IS User Guide

Copyrights

Copyright 1995 - 2002, Perle Systems Limited and its suppliers.

Cisco and Cisco IOS are registered trademarks of Cisco Systems, Incorporated.

IBM is the registered trademark of International Business Machines Corporation.

Microsoft, MS-DOS and Windows are registered trademarks of Microsoft Corporation.

Novell and NetWare are registered trademarks of Novell, Incorporated.

All other trademarks mentioned in this document are the property of their respective owners.

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, both feature card slots are to be covered. The thumbscrews on the feature cards should be tightened with screwdriver. This is to prevent the operators from access to the internals of the unit. 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 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.

INDUSTRY CANADA REQUIREMENTS.

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

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company’s inside wiring associated with a single line individual 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;

Facility Interface Codes (FIC):	02IS5
Service Order Code (SOC):	6.0Y
USOC Jack:	RJ49C
REN:	Not applicable

About this Book

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

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 833IS, 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 833IS, 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 833IS.

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.

What's in the Guide

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 833IS



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



Information: Provides important information that will make use of the 833IS 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 833IS.

Chapter 3: Setting Up and Installing the Perle 833IS: 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 833IS Manager: This chapters describes the requirements, function and features of the Manager Software.

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

Chapter 6: Configuring the Interfaces: Describes the unique characteristics and requirements of each Interface.

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 833IS: 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 833IS as well as its performance capabilities.

Appendix 4: RADIUS Server Attributes

Appendix 5: Cisco Mode

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.

What's in the Guide

Contents

Introduction	1	Interfaces.....	26
LAN-to-LAN.....	3	Serial Number Label.....	27
Section 1: Installation	5	Power Switch.....	27
Chapter 1: Quick Installation Overview	7	Assembling the Hardware.....	27
Preparing the Site.....	7	Connect the Power Cord.....	27
Setting up and Installing the 833IS Hardware.....	8	Attaching the Rack Mount.....	28
Setting up the LAN Connection.....	9	Factory Default Mode.....	29
Configuring the 833IS.....	9	Attaching the LAN Cable.....	29
Attaching to the Telephone Network.....	10	Ethernet.....	29
Verifying Correct Operation.....	10	Token Ring.....	30
Chapter 2: Site Preparation	11	Setting up the 833IS LAN Connection.....	31
Site Preparation Overview.....	11	IPX Connection to the Manager.....	32
Electrical Requirements.....	12	IP Connection to the Manager.....	32
Environmental Requirements.....	13	Set up the basic parameters.....	33
Placement.....	13	Verifying Connection.....	37
Cable Planning and Requirements.....	14	Manager Status.....	38
LAN Cabling.....	14	LAN Status.....	38
Ethernet.....	14	IP Status.....	39
Token Ring.....	17	IPX Status.....	40
Telephony Cabling.....	19	Configuring the 833IS.....	41
S/T Termination.....	19	Using the Manager.....	41
Chapter 3: Setting Up and Installing	21	Using Cisco Mode.....	41
What's in the box?.....	21	Attaching to the Telephone Network.....	42
Unpacking the 833IS.....	22	What's next?.....	42
Familiarize Yourself with the Unit.....	23	Chapter 4: Using the Perle 833IS Manager	43
833IS Views.....	23	Overview.....	43
833IS Chassis Description.....	24	System Requirements.....	44
Feature Cards.....	25	LAN Connection.....	44
System Card.....	25	WAN Connection.....	44
Expansion Card.....	26	Installing the Manager Software.....	45
		Setting up for Connection.....	45
		IPX Connection.....	45

IP Connection	45	Configure the Token Ring LAN Interface.....	78
Connecting to the Server	47	Configure the ISDN BRI Line Interface	80
Using IPX	47	Overview	80
Using IP	47	ISDN BRI U Interface Configuration.....	81
Troubleshooting.....	48	ISDN BRI S/T Interface Configuration	83
Dial-In Connection.....	48	Configuring the Perle DSP Modem Interface.....	86
Completing the Connection.....	49	V.90 Modems	88
Using the Manager Main Screen	51	Chapter 7: Configuring the Protocols.....	89
Menu Bar.....	52	Overview	89
Tool Bar	56	Configuring the Protocols	91
Off-Line Configuration.....	57	Configuring IP Protocol.....	92
Loading Firmware	58	WAN	94
Download via Manager.....	58	WAN Network Address	94
Download via TFTP	59	WAN IP Addresses	96
Section 2: Configuration.....	61	DHCP	98
Chapter 5: Configuring the Perle 833IS.....	63	IP Pool.....	99
How the 833IS Works.....	63	Server IP Address	101
Dial-In Access.....	63	DNS/WINS.....	103
Dial-Out Access.....	66	Routing.....	104
Configuration Overview	67	RIP Setup.....	104
Using Configuration Files.....	68	Static Routes.....	106
Creating.....	68	Add/Edit IP Static Routes	108
Opening.....	68	IP Filter.....	109
Uploading.....	68	Filter Definition	110
Saving.....	69	Add/Edit IP Filter Definition.....	112
Downloading.....	69	Filter Assignment.....	113
Configuration Main Window.....	70	Configuring IPX.....	114
Adding.....	72	IPX Protocol.....	115
Removing.....	73	Routing.....	117
Setting the Date and Time.....	74	Static Route.....	117
Chapter 6: Configuring the Interfaces.....	75	Add/Edit IPX Static Routes.....	120
Overview	75	IPX SAP Table List.....	121
Editing.....	76	Add/Edit IPX SAP Entries.....	122
Configure the Ethernet LAN Interface.....	77	Filter Definition	123
		Add / Edit IPX Filter Definition.....	124
		Filter Assignment.....	125

Configuring the Bridge Function (BCP)	126	Trigger Characters	168
Protocol Filter	127	Security.....	169
Configuring PPP.....	129	Overview	169
Apple PPP.....	131	Configuring User Authentication Security.....	171
Using AppleTalk.....	132	User Database	171
Using NetBEUI	133	Netware Bindery.....	172
Chapter 8: Configuring the User Database.....	135	RADIUS	173
Overview of the User Database.....	135	Axent.....	176
Internal User Database.....	136	SecurID	179
Configure the Internal User Database	137	NT Domain.....	181
User Main.....	137	Group Settings.....	182
Add/Edit User.....	139	Group Main.....	184
User Profile.....	141	Add/Edit Group.....	185
Protocols	143	Group Advanced.....	187
User Callback.....	145	User Standard Profile - Group	187
Lan To Lan.....	147	PPP - Group	187
Routing Information.....	148	Dial-Out - Group	187
LAN to LAN Connection Timers.....	148	Bridge Filter - Group.....	188
Authentication.....	149	SNMP	189
Dialing the router	150	SNMP Configuration.....	190
Lan To Lan Configuration.....	151	Community and Community Tables.....	191
Remote System Login.....	151	Logging Configuration.....	192
Phone Numbers.....	151	Section 3: Management.....	197
Connection.....	152	Chapter 10: Managing the Perle 833IS	199
Configure Virtual Connection.....	152	833IS Manager Statistics	199
RIP Setup.....	154	Viewing Statistics.....	199
Standard Profile.....	155	Accessing Interface Statistics	202
IP Filter Assignment.....	159	Ethernet Interface.....	202
IPX Filter Assignment	160	Token Ring Interface.....	203
Shared User Database.....	160	ISDN BRI Line Interface	204
Chapter 9: Configuring the Server	163	Perle DSP Modem Interface.....	207
Overview	163	IP Protocol.....	209
Configuring the Server.....	164	IPX Protocol	212
To configure the Server	164	User Statistics	216
Dial-Out	166	Event Log.....	218

833IS Front Panel	220
Front Panel Modes.....	220
Navigating the Front Panel.....	221
Editing Fields.....	221

Appendix 1: Menu Descriptions and Maps...223

Front Panel Main Screen.....	223
Front Panel Main Screen Map.....	223
Control.....	224
Control Menu Map	225
Status.....	226
Status Menu Map.....	227
Card Status	228
Card Status continued	229
Card Status continued	230
Card Status Menu Map	231
Network Status Display.....	232
Network Status Display Menu Map.....	234
Factory Default Mode	235
Factory Default Setup	235
Factory Default Mode and Setup Map.....	236
Factory Default Mode	237
Factory Default Mode Menu Map.....	239

Appendix 2: AT Command Set241

AT Commands.....	241
AT& Commands.....	251
AT% Commands	253
AT\ Commands.....	254
AT+ Commands.....	255
Error Detection and Data Compression Commands.	259
AT% Commands	259
AT\ Commands.....	259
S-Registers	261
S-Register Definitions	263
AT Command Set Summary	266

Basic AT Commands.....	266
ECC Commands.....	269
MNP 10 Commands.....	269
FAX Class 2.....	269

Appendix 3: Specifications271

Dimensions.....	271
Physical/Electrical Specifications.....	271
Chassis.....	272
Memory	272
LAN Interfaces.....	272
ISDN BRI Interface.....	273
PerleDSP Modem Interface.....	274
Approvals	275
Protocols Supported.....	276
LAN Environments.....	276
Dial In Clients Supported.....	277
Dial Out.....	277
Security.....	277
Management	277
RFCs Supported	278

Appendix 4: RADIUS Server Attributes.....279

Account Request Messages.....	279
Access-Accept Messages.....	280
Accounting Messages.....	282

Appendix 5: Cisco Configuration Mode.....285

Introduction to Cisco Configuration Mode.....	285
Overview of 833IS.....	286
Differences Between 833IS and Cisco Products.....	288
Command Overview.....	291
Installation and Configuration of 833IS with Cisco Configuration Mode.....	291
Monitoring the 833IS	296
Differences between 833IS Manager and Cisco Configuration Mode.....	296

Glossary.....299

Index.....305

Introduction

The Perle 833IS...Reliability and Flexibility

About the Features of the 833IS

Dial- In Access

The 833IS 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 833IS 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.

BRI Support

Calls are brought into the 833IS by an Integrated Services Digital Network (ISDN), Basic Rate Interface (BRI) line. Using digital technology provides for a higher reliability and the ability to transfer data at rates of up to 64kbps per channel. ISDN also greatly increases the speed at which calls can be established and torn down. The unit can support as many as 8 ISDN, BRI lines. Each BRI line can support up to 2 simultaneous phone calls allowing for a total of 16 simultaneous sessions. ISDN provides for remote access from conventional modems, ISDN BRI cards or Terminal Adapters.

There are two basic types of BRI interfaces available today. The "U" interface is a 2 wire interface which connects a Network Termination (NT) device to the central office (CO). This is common in North America where the customer supplies the NT

Multiprotocol Support

device. The “S/T” interface is a 4 wire interface which is used to connect a “NT” device to a Terminal Endpoint (TE) device. In this type of configuration, the user can connect up to 8 TE device on one S/T bus. This type of configuration is more common in Europe where the network normally provides the “NT” device.

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 833IS are the Perle Remote Dial-In Clients for DOS and Windows 3.1. Microsoft Dial Up Networking Clients are supported for Windows 95, 98, 2000 and Windows NT. For the Macintosh user, the 833IS is compatible with Apple Remote Access.

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

Advanced User Security

The 833IS 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 833IS to meet high security requirements.

The internal database of the 833IS supports up to 500 users, each with their own password.

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

Grouping

The 833IS'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 833IS LAN-to-LAN feature lets you establish IP/IPX connections to remote Routers. These connections can be initiated by either the 833IS 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 833IS to meet the needs of your business. The 833IS supports the addition of an expansion card. As your remote access needs grow, this card can be used to address the added demand. An expansion card can add an additional 4 ISDN BRI ports to your unit or an additional 4 ISDN BRI ports as well as an additional 8 modems. This capability allows the 833IS to grow to a total of 8 ISDN BRI ports and 16 modems.
Flexible Modem Support	The 833IS modems support all the standard modem modulations, including V.90 and 56Kflex. 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 833IS Manager is a Windows based application used to configure and manage the 833IS. You can connect to the 833IS by a LAN or Dial In connection, using either IP or IPX. The configuration process is entirely GUI based - no editing of complex configuration files is needed. The Manager also displays the operational status of the 833IS. Key statistics are provided for all interfaces to enable monitoring of normal operation and assist in network troubleshooting if necessary.
Cisco™ style Configuration Mode	The 833IS contains a Cisco™ style setup and configuration mode for users trained in the installation and configuration of Cisco™ products. The familiar Cisco Command Line Interface can be used along with applicable Cisco commands to set up and manage the 833IS.
High Performance Architecture	The 833IS was designed for high performance, even when handling the maximum number of incoming calls. At its heart is a high speed PowerPC Reduced Instruction Set Computer (RISC) CPU, which is optimized for communications. The expansion card contains its own PowerPC processor. This enables the 833IS to grow the number of sessions supported without degrading the level of performance.

**High Reliability
Design**

There are no moving storage devices such as floppy or hard drives in the 833IS. All program storage is on Flash Read Only Memory (ROM).

Section 1: Installation

Chapter 1: Quick Installation Overview

Chapter 2: Site Preparation

Chapter 3: Setting Up and Installing

Chapter 4: Using the Perle 833IS Manager



Chapter 1: Quick Installation Overview

About Installation

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

These are the major steps:

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

The 833IS can be set up either using the 833IS Windows Based Manager or by following a "Cisco mode" setup procedure. The Quick Installation Overview will cover installation via the 833IS Manager. For information on Cisco mode installation and operation, please refer to "Appendix 5: Cisco Configuration Mode". This mode is intended only for advanced users previously trained on the operation of Cisco equipment.

Preparing the Site

For detailed instructions, see "Chapter 2: Site Preparation".

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

- Arranging the installation of telephone services by the carrier.
- Locating the 833IS 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 PC that will be used for installation of the 32 bit Windows Manager. This PC must be attached to the LAN.
- Extending all telephony and LAN wiring to the location where the 833IS will be installed.

Setting up and Installing the 833IS Hardware

For detailed instructions, see “Chapter 3: Setting Up and Installing” on page 21.



To Install the 833IS Hardware:

1. Unpack the 833IS.
2. Set up the 833IS. See “Unpacking the 833IS” on page 22.
3. If the unit is to be rack mounted, install the Rack Mount Kit and place the unit in the rack.
4. Connect and plug in the power cord.



It is not recommended that you attach the LAN or the telephone network wiring at this time. If the 833IS is powered up with a configuration that does not match the carrier's 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.

5. Power on the 833IS.

Setting up the LAN Connection

For more details, see “Set up the basic parameters” on page 33.

To Set up the 833IS 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 833IS. 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 33.

2. Power off the 833IS.
3. Attach the LAN cable to the appropriate connector, based on your LAN type and media type. See “Configuration for the Manager is now complete.” on page 36.
4. Power on the 833IS.
5. Verify that the 833IS can see LAN network traffic. See “Verifying Connection” on page 37.

Configuring the 833IS

For detailed instructions, refer to Section 2: Configuration

You configure the 833IS with the 833IS Manager. The Manager Software must be installed on a 32 bit Windows PC that is LAN attached. The PC must also have IP or IPX network software installed and set up. This network software is built into Windows 95, 98, 2000 and NT.

Attaching to the Telephone Network

See “Attaching to the Telephone Network” on page 42.

Now that the 833IS is configured, the telephone cables can be attached to the unit.

To attach the telephone line:



1. Power down the 833IS.
2. Attach the cable(s) from the phone network to the appropriate interface(s) on the 833IS.
3. Power up the 833IS.
4. Verify that the 833IS can operate correctly with the telephone line.

Verifying Correct Operation

For details, see “Verifying Connection” on page 37.

At this point, installation is complete. Now you can verify that remote users can dial into the 833IS 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 833IS. 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 833IS 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 19.

Electrical Requirements

then,

- ✍ __ Order the ISDN BRI lines 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	.5 A (Maximum)	.25 A (Maximum)
Power	62.5 W (Maximum)	60 W (Maximum)

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

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.

Environmental Requirements

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

Condition	Temperature Range	Relative Humidity
Operating	0° - 40° C 32° - 104° F	0% - 95% non-condensing

Placement

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

Locate the 833IS in an area where:

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



Sufficient clearances must be maintained at both sides of the unit to allow proper air flow to the internal fans.

For rack mounting, the 833IS requires 1.5 rack mount spaces (i.e. the 833IS height is 1.5U). 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

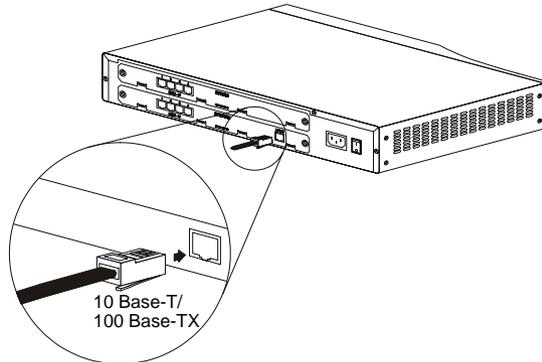
Depending on the type of system card inserted into the 833IS, the unit can support either an Ethernet or a Token Ring interface. The type of LAN cabling you will need will depend on the following factors:

- 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 following physical interfaces are available for Ethernet:

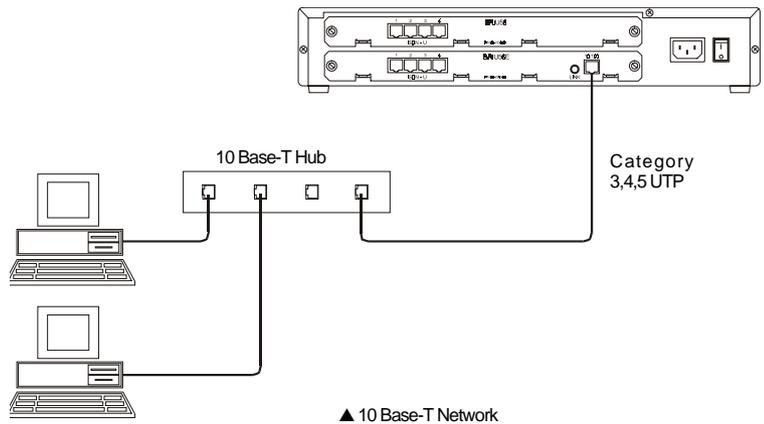
- 10Base-T/100Base-TX - uses an RJ-45 connector



▲ Ethernet/LAN Cable Connection

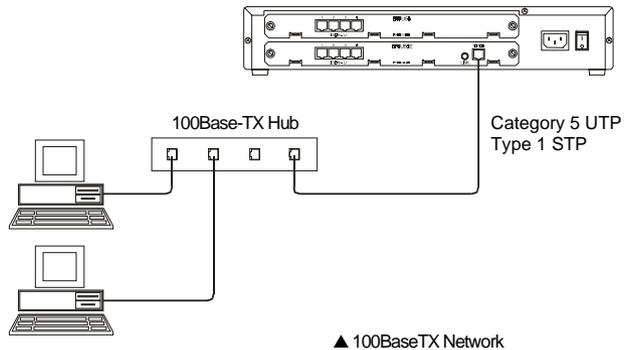
10Base-T:

- 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 833IS to hub is 100m (328 ft.).



100Base-TX:

- 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 8331S to hub is 100m (328 ft.).



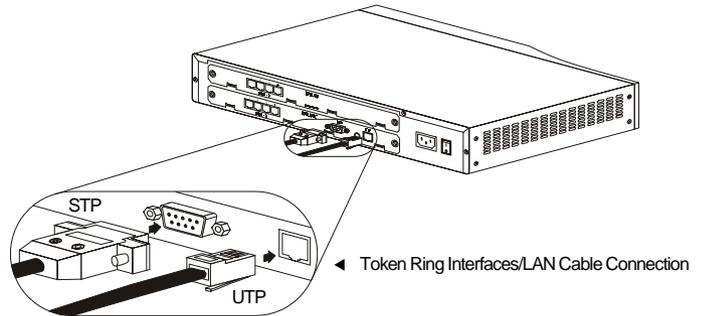
There are other cabling types that are available for Ethernet:

- 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.

Token Ring

The following physical interfaces are available for Token Ring:

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



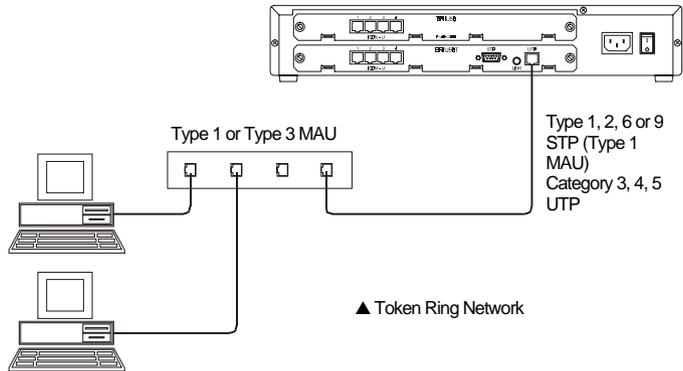
Cable Planning and Requirements

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.



Telephony Cabling

The connection to the ISDN network is made via an RJ-45 connector. The 833IS is shipped with the appropriate cables required to connect to the telephone network. These cables are standard UTP cables.



▲ UTP Cable

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

S/T Termination

A BRI S/T interface requires line termination. Some telcos require that this 100-ohm termination be provided within the customer equipment. Check with your telco to see if it is necessary for the 833IS to provide this termination.

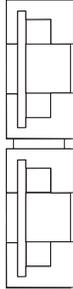
An improperly terminated BRI line may cause line errors on the BRI line. This would typically be seen as a dial in client abnormally losing connection.

The 833IS ships with termination enabled. Termination is enabled or disabled by using jumpers on the System Card and (if installed) Expansion Card. There is one pair of jumpers for each interface:

- JP250 - BRI 1
- JP350 - BRI 2
- JP450 - BRI 3
- JP550 - BRI 4

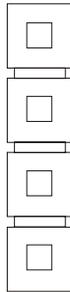
Telephony Cabling

To enable termination, use the supplied jumpers (attached to the jumper block) to jumper the two top jumpers together and the two lower jumpers together.



▲ Enable 100 termination - Jumper block

To disable termination, remove the jumpers.



▲ Disable 100 termination - Jumper block

Note that a BRI U interface has no user adjustable termination.

Chapter 3: Setting Up and Installing

About Setting Up and Installing

In this chapter you will read about:

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

What's in the box?

The 833IS shipping carton contains the following:

- 833IS
- Rack Mount Kit
- Power Cord
- ISDN Cables
- Documentation Package
- Software Package

Rack Mount Kit

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

Power Cord

The appropriate power cord for your location is provided.

ISDN Cables

Standard UTP cables with an RJ-45 connector used to connect the ISDN interfaces to the termination point provided by the service provider.

Documentation

The following documents are available:

- Perle 833IS User Guide
- Perle Remote User's Guide
- Perle Dial-Out User's Guide

Software

The Software contains the following:

Unpacking the 833IS

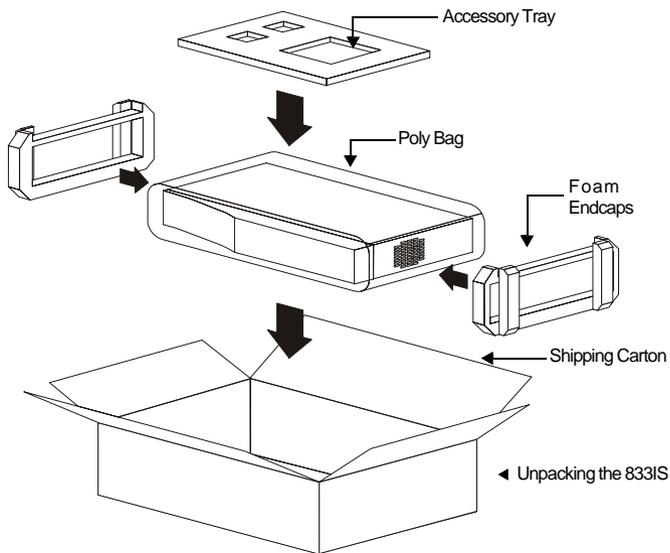
- Perle RAS Manager
- 833IS Firmware
- Perle Remote Client
- Perle Dial-Out Client

Unpacking the 833IS

To Unpack the 833IS:



1. Open the shipping carton.

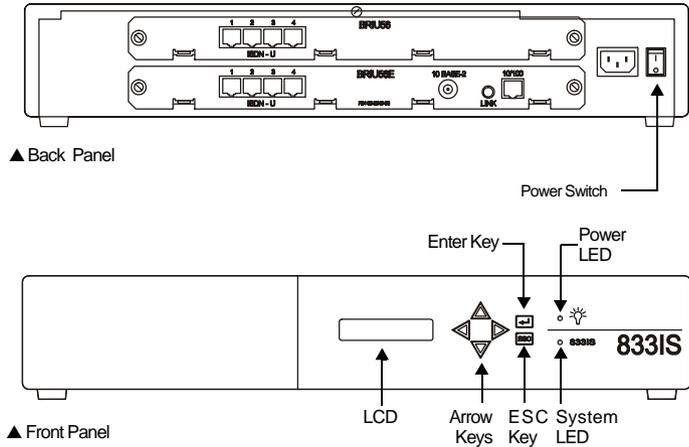


2. Remove Accessory Tray containing the Power Cords.
3. Remove the Documentation and Diskette packets from the side cavity between the unit and outer carton.
4. Lift the 833IS out of the shipping carton.
5. Remove the packing material.

Familiarize Yourself with the Unit

833IS Views

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



The card(s) in your unit may be slightly different, depending on the type of card(s) you purchased. Slot 2 may not be occupied on your unit.

**833IS Chassis
Description**

Operator Panel LCD

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

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

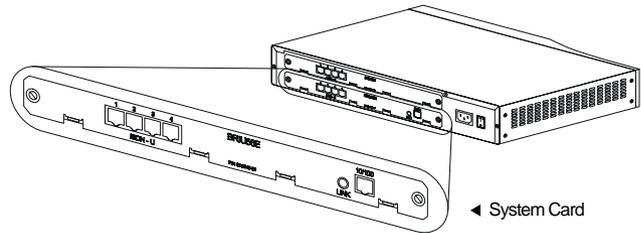
Menu	Description
Power	Indicates that the 833IS is powered up.
System Active	Blinks continuously when the 833IS is operational. Blinking will start after System initialization is complete.

Feature Cards

The 833IS can hold up to two Feature cards. The card in Slot 1 is called the System card, and the card in Slot 2 is called the Expansion card. The system card must be present in the 833IS, but the Expansion card is optional. Both cards come with different interfaces as described below.

System Card

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



The following system cards are currently supported:

Card name	Interfaces supported
BRIU56E	4 ISDN BRI U-interface, 8 56K modems, 10/100 Mbit Ethernet
BRIU56T	4 ISDN BRI U-interface, 8 56K modems, Token Ring
BRIS56E	4 ISDN BRI S/T-interface, 8 56K modems, 10/100 Mbit Ethernet
BRIS56T	4 ISDN BRI S/T-interface, 8 56K modems, Token Ring
BRIUE	4 ISDN BRI U-interface, 10/100 Mbit Ethernet
BRIUT	4 ISDN BRI U-interface, Token Ring
BRISE	4 ISDN BRI S/T-interface, 10/100 Mbit Ethernet
BRIST	4 ISDN BRI S/T-interface, Token Ring

Expansion Card

The 833IS is an expandable unit and therefore provides for the insertion of an optional expansion card in slot 2. The following expansion cards are currently supported:

Card name	Interfaces supported
BRIU56	4 ISDN BRI U-interface, 8 56K modems
BRIS56	4 ISDN BRI S/T-interface, 8 56K modems
BRIU	4 ISDN BRI U-interface
BRIS	4 ISDN BRI S/T-interface

These cards allow the user to double the number of ISDN ports as well as doubling the number of modems available in the system. If the unit was purchased with an expansion card, it will come already installed in the unit.

Interfaces

LAN Interface The LAN interface is available for an Ethernet or Token Ring attachment to the LAN.

Ethernet The Ethernet interface supports a 10 Mbps or 100 Mbps connection, through the RJ-45 (supports 10Base-T and 100Base-TX) interface type. There is also a Link LED associated with the interface which flashes when the interface is connected to the LAN and data is being received.

Token Ring The Token Ring interface supports a 4 Mhz or 16 Mhz connection. It contains two physical interfaces. A DB9 connector provides the STP interface used to connect to a Media Access Unit (MAU) which utilizes the IBM style universal connectors. An RJ-45 connector provides the UTP interface used to connect to a MAU using Unshielded Twisted Pair wiring. A LAN LED is provided to indicate successful connection to the Ring and to identify activity on the interface.

ISDN interface There are two types of ISDN interfaces supported. A "U" interface (most common in North America) and an "S/T" interface (most common outside of North America). The type of interface you purchased should match the type of connection provided by your Telephone network provider.

Modem Interface

The card may include 8 central site modems on board. These modems will support a rate of up to 56K using the V.90 or 56Kflex protocol. These modems can be used to accept incoming analog calls or to establish outgoing calls.

Please take a moment to identify the type of cards present in your 833IS.

Serial Number Label

This label contains such information as the name and model of the unit, the serial number for the unit, power requirement information as well as the various types of approvals registered for the unit. The serial number label can be found on the bottom of the unit.

Power Switch

This switch is used to turn off all power to the unit. When the power is cycled, the unit will restart its power up sequence. The 833IS can maintain its program and log information event when no power is applied to the unit.

Assembling the Hardware

Connect the Power Cord

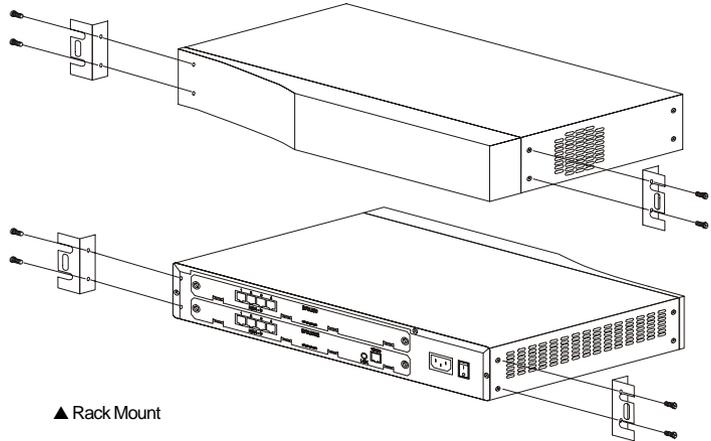
Connect one end of the supplied power cord into the 833IS power connection and the other end into a properly grounded electrical outlet.



For safety, this equipment is designed to be electrically grounded. The 833IS must be connected to a three wire grounded outlet only. The power cord 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 833IS in a standard 19" equipment rack. Use the screws included in the Rack Mount Kit to attach the Rack Mount brackets to the 833IS.



You require 4 Rack Mount screws (2 per side) to mount the 833IS in the Rack. Do not install the 833IS in the Rack with fewer screws. For rack mounting, the 833IS requires 1.5 rack mount space (i.e. the 833IS height is 1.5U). It is not necessary to leave empty spaces above or below the unit in the rack.



Sufficient clearances must be maintained at both sides of 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 833IS is downloaded to the Server from the Manager, or optionally via TFTP and Telnet. Before this occurs, the 833IS is in Factory Default mode, or simply Factory mode. In Factory mode, you use the Front Panel to configure any parameters needed for the initial download connection. Factory mode also provides statuses on the Front Panel to help diagnose communication problems with the initial download connection. Front Panel operation in this mode is detailed in "Factory Default Mode" on page 235.

Once the 833IS 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 53) or Front Panel ("Control" on page 224).

Attaching the LAN Cable

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

Ethernet

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

- 10Base-T: UTP, Category 3, 4 or 5
- 100Base-TX: Category 5 UTP or Type 1 STP

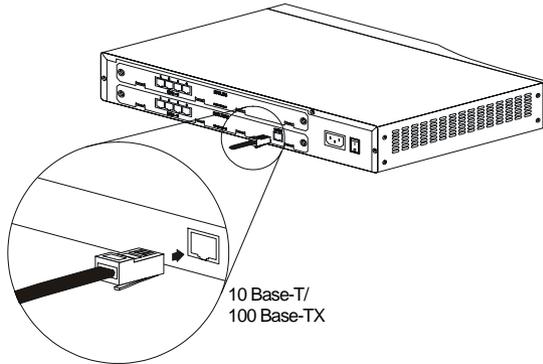
For a complete discussion on Ethernet cable requirements, see "Cable Planning and Requirements" on page 14.

To attach the cable:

Attaching the LAN Cable



1. Ensure that the 833IS 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 833IS.

Token Ring

If you are attaching the 833IS to a Token Ring network, you will need either:

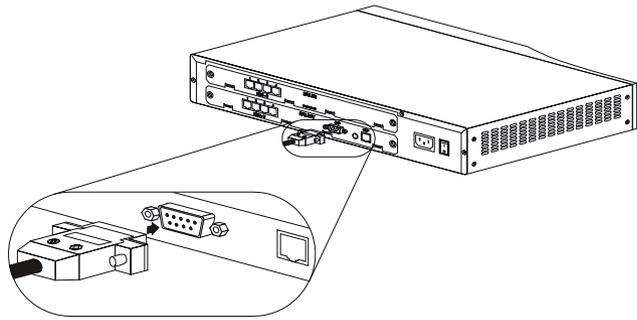
- A UTP cable (Type 3 wiring), or
- A STP (Shielded Twisted Pair) adapter cable (DB9 to either Type 1 or Type 6 Token Ring wiring).

To attach the cable:



1. Ensure that the 833IS is powered off.
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 833IS.

Setting up the 833IS LAN Connection

This step sets the parameters needed for the initial download configuration. During installation, a LAN connection is used to talk to the 833IS. Once fully configured, you can manage the 833IS across the LAN or from a Dial-in connection.

The Manager communicates with the 833IS 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 833IS to support both IPX and IP.

If you are using the Cisco mode setup procedure, follow the steps for an IP connection. IPX is not supported for the Cisco mode setup.

The 833IS can be connected to the LAN via an Ethernet or Token Ring connection depending on the specific system card purchased with the unit.

If your unit is equipped with a Token Ring interface, you must set the interface speed using the front panel. The valid options are 4 or 16Mbps. (see page 33)

IPX Connection to the Manager

No configuration is required for the Manager to communicate with a 833IS using IPX. By listening to the traffic on the LAN, the 833IS 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.

If there is a router between the 833IS and the management connection, the 833IS will need to know the address of this router.

The 833IS requires the following IP parameters be established:

IP Address

This address uniquely identifies the unit to the IP network. The 833IS provides the following 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 833IS attempts to acquire the IP address from a BOOTP or RARP server by default. You will need the MAC address of the 833IS to do this. This address can be obtained from the Front Panel.

If you do not configure an IP address and do not get the address from an Address server, the 833IS will be unable to communicate with the manager using the IP protocol.

This IP address will need to be explicitly defined in the Manager as detailed in "Using IP" on page 47.

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 Default Router Address

If the IP network path to the Management Connection passes through an IP router (gateway), enter the IP address of the router that is on the same LAN segment as the 833IS and is responsible for forwarding the IP packets to the network to which the Management PC is connected.

Set up the basic parameters

The LAN cable should not be connected to the 833IS at this time. Power up the 833IS by turning on the power switch at the rear. The power LED should be lit.

The Front Panel will display:

Perle 833IS

After 5 seconds, the display will change to:

No Manager

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

Using the Front Panel

When the 833IS 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 Management PC
- Monitor the 833IS'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.

Setting up the 833IS LAN Connection

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 ▶

Manager Setup

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
233.233.233.011

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 833IS 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 DefaultRouter 000.000.000.000

Enter the IP address of the default router if required.

Press ▼

LAN Speed Auto Detect
--

Set the value to match your LAN speed, set to 4 or 16 Mbps for Token Ring or set to Auto, 10 or 100 Mbps for Ethernet.

Press ▼

Port RJ45

If you have an Ethernet interface on the card installed in slot 1, this panel may be displayed.

Some versions of the 833IS contain a BNC Ethernet interface in addition to the RJ45 interface. For these units, you can use this panel to override the auto port detect feature of the 833IS. Once set, the 833IS will no longer try to auto detect this port, even after a restart of the unit. The only way to re-enable the auto detect feature is via this menu item.

Set the value to the desired port (RJ45, BNC, or Auto Detect).

Setting up the 833IS LAN Connection

Press ▼

Save Config

If you wish to save your configuration to NVRAM then press Enter.

**Save Config
Confirm**

Press Enter again to confirm the saving of this configuration.



This configuration takes affect immediately and does not require an IPL of the 833IS.

Note: if the 833IS is powered off before the 833IS Firmware is downloaded this manager setup configuration will have to be repeated.

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

Press the ▲ key until you see this front panel:

Manager Setup

Press ►

Status

Press ▼

**MAC Address
020000044444**

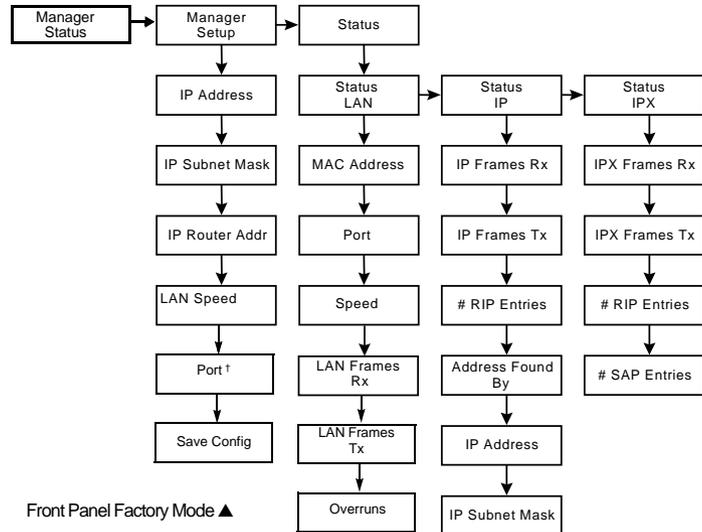
Provide this address to your IP Network Administrator.

Configuration for the Manager is now complete.

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 833IS LAN adapter and the Hub or MAU (Multistation Access Unit).

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



† Can be configured only when the unit includes Ethernet interface.

Status Fields are listed in the following section. A complete description of Front Panel Factory Mode is found in “Factory Default Mode” on page 235, and “Factory Default Mode” on page 237.

Manager Status

Displays one of the following messages:

No Manager

Displayed if there is no Manager connected to the 833IS.

Manager IP/IPX

Displayed if the Manager is connected to the 833IS and which protocol is used for communication

Ping #

IP address

If the 833IS receives an IP ping command in Factory Default mode, this message will display the address of the device that sent the ping command. The count (#) will increment for each ping received. If you experience difficulty in communicating with the 833IS from the Manager or Telnet/FTP, you can send a ping command from a device and verify that the 833IS is receiving it.

LAN Status

MAC Address

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

Port

Only displayed for an Ethernet interface. Displays the physical port being used to communicate to the hub. Valid options are: RJ45, BNC.

The BNC option is valid only for versions of the 833IS that contain a BNC port.

Speed

Display the operating speed of the interface. For Token Ring the valid options are 4Mbps or 16Mbps. For Ethernet, the valid options are 10Mbps or 100Mbps.

LAN Frames RX

Displays the number of frames received by the 833IS 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 833IS 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 833IS LAN adapter because of a receive overrun state. This condition indicates that the 833IS 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 833IS. 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 broadcasts (for example, RIPv) on your network.

IP Frames TX

Displays the number of IP frames transmitted by the 833IS. 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 833IS has received RIP broadcasts from other subnetworks.

Address Found by

Displays what mechanism was used to acquire the 833IS IP address. The value will be BOOTP, RARP, Configured, or None. If None is displayed, it indicates that the 833IS 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 833IS.

IP Subnet Mask

Displays the configured IP subnet mask.

IPX Status

IPX Frames RX

Displays the number of IPX frames received by the 833IS. 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 833IS receives IPX broadcast messages.

IPX Frames TX

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

RIP Entries

Displays the number of entries within the 833IS'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 833IS.

SAP (Service Advertising Protocol) Entries

Displays the number of entries within the 833IS'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 833IS.

Configuring the 833IS

Using the Manager

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

During this configuration process, you will:

- Connect the Manager with the 833IS. See "Chapter 4: Using the Perle 833IS Manager" .
- Download the 833IS System software.
- Set up the parameters for the interfaces on the cards installed in your system. See "Chapter 6: Configuring the interfaces" .
- 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 169.
- If you select "User Database" as your method of security, add users to the 833IS's user database and set their access rights and capabilities. See "Chapter 8: Configuring the User Database" on page 135.
- Download the configuration to the 833IS. See "Downloading" on page 69. 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 833IS 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 182). However, to simplify installation, it is recommended that Groups be set up after basic installation is complete and operation verified.

Using Cisco Mode

For information on Cisco mode installation and operation, please refer to "Appendix 5: Cisco Configuration Mode". This mode is intended only for advanced users previously trained on the operation of Cisco equipment.

Even if you are planning to use the Cisco mode for day to day operations, you may wish to use the Manager for initial configuration. The GUI Manager makes it very

easy to create a successful initial configuration. This configuration can then be modified using the Cisco style commands via Telnet.

Attaching to the Telephone Network



You will need the appropriate cable to attach the 833IS to the telephone network. The ISDN BRI interface uses an RJ-45 connector. The required telephone network cables are shipped with your 833IS unit.

1. Ensure that the 833IS is powered down.
2. Attach the cable between the ISDN BRI interface port and the line termination point. For a U interface, this will be the LT (Line Termination) point. For an S/T interface, this will be a NT (Network Termination) point.

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 833IS. You can now verify that remote users can dial into the 833IS 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 833IS Manager

About Using the Manager

This chapter describes how to install and use the 833IS 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 833IS Manager is a 32 bit Microsoft Windows application that configures, monitors and manages 833IS Servers. The Manager performs the following functions:

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

These functions can be performed for all 833IS 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 833IS LAN connection, or dialed in from the WAN.

The Manager is not supported under Windows NT Server. It is fully supported under Windows NT Workstation.

System Requirements

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

- Hard drive with at least 4 MB free storage space.
- Windows 95 or 98, or
- Windows NT 4.0 workstation, or
- Windows 2000
- 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.
- For an IPX connection, a working IPX connection to the LAN is required. The 833IS Manager works with Microsoft Windows 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 Manager:

- Microsoft Windows 95/Windows 98 Dial-Up Networking Client.
- Microsoft Windows NT Version 4.0 Dial-Up Client.
- Microsoft Windows 2000 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 833IS Manager software, follow these steps:

1. Start Microsoft Windows.
2. Click the **Start** button.
3. Click **Run**.
4. Type **D:\RAS Manager\Setup** where D: 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 833IS using IPX. By listening to the traffic on the LAN, the 833IS 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 33.

If the 833IS 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 833IS requires the following IP parameters to be established:

IP Address

This is the address that uniquely identifies the unit to the IP network. The 833IS 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. You will need the MAC address of the

Installing the Manager Software

833IS to do this. The MAC 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 Default 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 833IS.

Connecting to the Server

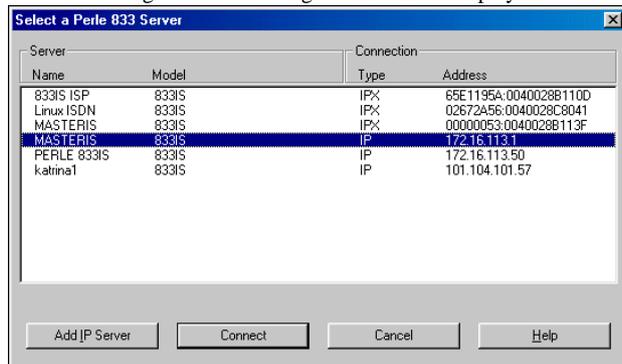
Using IPX

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

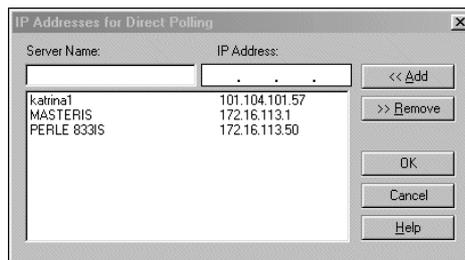
Using IP

The IP address of the 833IS needs to be defined to the Manager. To do this, perform the following steps:

1. Start the Manager. The following screen will be displayed:



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



3. The **Add IP Server** screen will display. Enter the name of the Server in the **Server Name** field.

Connecting to the Server

4. Enter the IP address of the Server in the **IP Address** field.
5. Click on **Add**.

The 833IS is now defined to the Manager. When the Manager connects via IP, it will check for the defined Servers.

If you are using Domain Name Servers (DNS) on the Manager PC, you can enter the name of the 833IS. The Manager will resolve this name to an IP Address.

Troubleshooting

The 833IS will appear in the Server list if the 833IS is correctly connected. See “Completing the Connection” on page 49 for details.

If the 833IS 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 833IS 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 and must pass through one or more routers to communicate with the server, verify that a Gateway address has been configured on the PC's LAN adapter. This Gateway address should be the address of the router that is on the same LAN segment as the Management PC.

Dial-In Connection



To establish a Dial-In Connection:

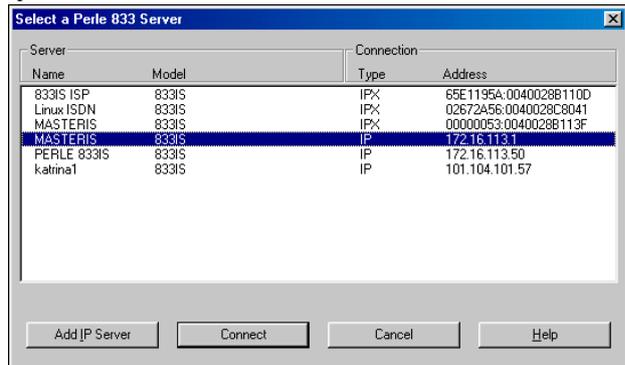
1. Install the Manager on your PC.
2. Using your **Dial-up Client**, set up a dial-up Network connection:
 - Enable either **IP** or **IPX**.
 - If you are using an **IP** connection, your client requires an **IP** address. Most clients provide the option to configure the IP address in the Client, or use an IP address supplied by the Server. If you have disabled "**Allow client specified IP addresses**" in the 833IS configuration, set the **IP** address supplied by the Server. See “Allow Client Specified IP Addresses” on page 96.
 - 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.

- Once the Dial-up session is connected, start the 833IS Manager.

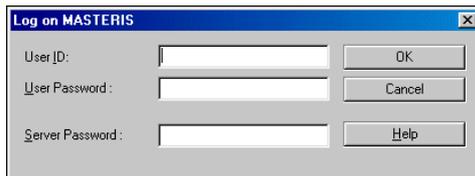
Completing the Connection

When the 833IS Manager connects to the network, it automatically locates all 833IS IPX Servers and all defined 833IS IP servers on the network and displays them in the Server List window.

To complete the connection to a server:



- 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 "Using IP" on page 47.
- Enter the **User ID**, **Password** and **Server Password** if configured for the selected Server and click **OK**.



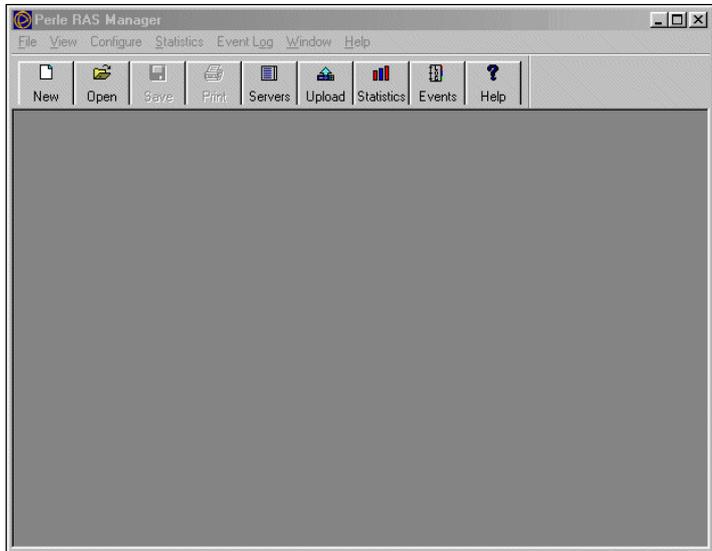
The default User ID for an unconfigured 833IS is “*superusr*”, with no password. The User ID is case sensitive.

This User ID and password is valid for an unconfigured 833IS only. You will be required to set up a User ID with Administration privileges or configure a server

Connecting to the Server

password when you configure the Server. This will not be required if you select “RADIUS” as your security method.

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



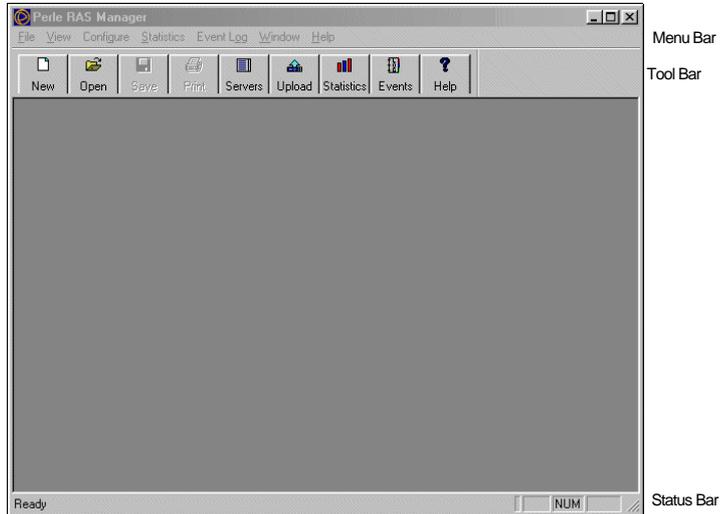
4. If this is the first time that this 833IS is connecting to the Manager you will have to download Firmware to the 833IS. If the 833IS has Firmware, the Manager checks the Firmware level. If the Firmware is at an older revision level, you will be prompted to update the Firmware. See “Loading Firmware” on page 58.

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

The Manager is not supported under Windows NT Server. It is fully supported under Windows NT Workstation.

Using the Manager Main Screen

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



Menu Bar

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

Tool Bar

A quick way to use the main functions of Perle 833IS. Each function is represented by a button.

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 833IS servers found.

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

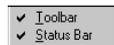
The most recent files that were opened are listed here. Select a file from the list to open that file.

Exit

Quit Perle 833IS 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 833IS 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 833IS.

Using the Manager Main Screen

Reset the Perle 833IS

Reset the Perle 833IS. Any sessions handled by the Server will be terminated.

Set Date and Time

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

Set 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 833IS.

Set to Factory Mode

Delete the current configuration and sets 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 833IS 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 833IS 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 let the user select any of the event types recorded by the 833IS. Only those events will be recorded.

Clear Event Log

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

PPP Debug

This popup menu displays the following PPP Debug options. Enabling any of the following options, displays PPP level information in the Event Log for each dial-in connection.



Authentication

Displays all PPP authentication packets in the Event Log

Negotiation

Displays PPP packets that are transmitted and received during PPP startup(i.e. LCP and NCP options) in the Event Log.

MP

Displays Multilink PPP protocol messages in the Event Log.

CBCP

Displays Callback (CBCP) protocol message in the Event Log.

Packet

Displays in the Event Log all PPP packets being transmitted and received

Error

Displays protocol errors and error statistics associated with PPP connection negotiation and operation in the Event Log.

Window Menu

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



Using the Manager Main Screen

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.

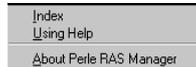
Arrange Icons

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 833IS Manager Help index.

Using Help

Displays general information about using Windows Help.

About Perle RAS Manager

Display the version number of the Perle RAS 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.



Print

Print the current configuration information.



Server List

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



Get Configuration

Get the current configuration from the connected Perle 833IS.



Get Statistics

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



Get Event Log

Get the event log from the Perle 833IS.



Help

Display the Perle 833IS 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** and select either **New** or **Open** from the Tool Bar.

Loading Firmware

Firmware is the basic operating code of a 833IS. A new 833IS must have Firmware downloaded before it is fully functional. This Firmware is shipped with the Installation disks.

Download via Manager

If you wish to install a new version of Firmware in your 833IS, 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.

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.

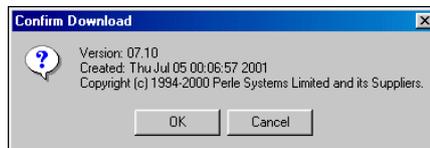


The new Firmware will not take effect until the 833IS is restarted.



To download Firmware:

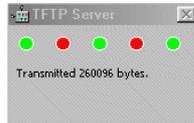
1. Using the 833IS Manager, connect to the 833IS that you wish to download.
2. If the Manager detects that the Firmware download should be done, a dialog box will appear:



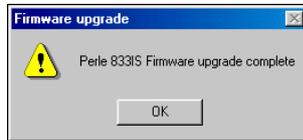
Click **OK** to continue, **Cancel** to cancel the download.

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

3. A window 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 TFTP Server window is displayed indicating the progress of the download.



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



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

Note: After the firmware download is completed, you can download the configuration before restarting the 833IS.



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

If the 833IS is reset before the download completes, the target 833IS 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.

Download via TFTP

Firmware can be downloaded to the 833IS via TFTP. For details, please refer to “Appendix 5: Cisco Configuration Mode”.

Loading Firmware

Section 2: Configuration

Chapter 5: Configuring the Perle 833IS

Chapter 6: Configuring the Interfaces

Chapter 7: Configuring the Protocols

Chapter 8: Configuring the User Database

Chapter 9: Configuring the Server

Chapter 5: Configuring the Perle 833IS

About Configuring the Perle 833IS

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

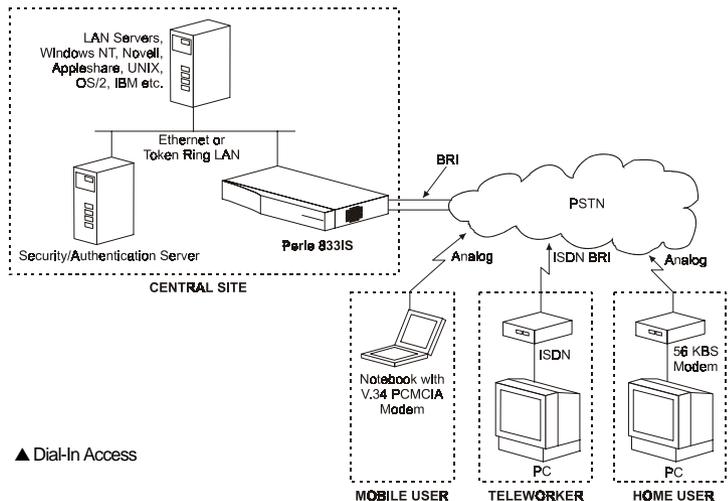
- How the 833IS Works.
- Configuration Overview.
- Using Configuration Files.
- Setting the Date and Time.

How the 833IS Works

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

Dial-In Access

The 833IS 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*.



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 one of the BRI lines, the system identifies the type of call as being either a digital or analog call. At this point, a check is made to see if the resources required to handle the call are available. For example, a modem is required if it is an analog call.

The System assigns the needed resources to the call. Resources are allocated on a round robin basis to ensure that all resources are used equally. The resource does not have to reside on the same physical card as the one on which the call came in. Once the required resources have been identified, the call is accepted and is forwarded to the appropriate resource. The calls are moved about in the system via a special bus used for this purpose.

As an example, a call originating from a modem can come in on channel B2 of the ISDN BRI line connected to the first port of the card in slot 1. This type of call will require a modem. The system may locate an available modem on the card in slot 2. The call would then be switched to this modem. All physical data would be sent and received over the BRI line connected to port 1 of the first card but internally, the data would be handled by the modem on the second card. This flexibility allows the 833IS to allocate its available resources in an effective and efficient manner.

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 clients are examples of this type. They connect using their 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 a WAN 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 WAN connection. The PC client strips off the PPP and delivers the frames to the NDIS or ODI (Multilink 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 WAN connection. The Server strips off the PPP and transmits the frame over the LAN connection.

Apple Remote Access Client

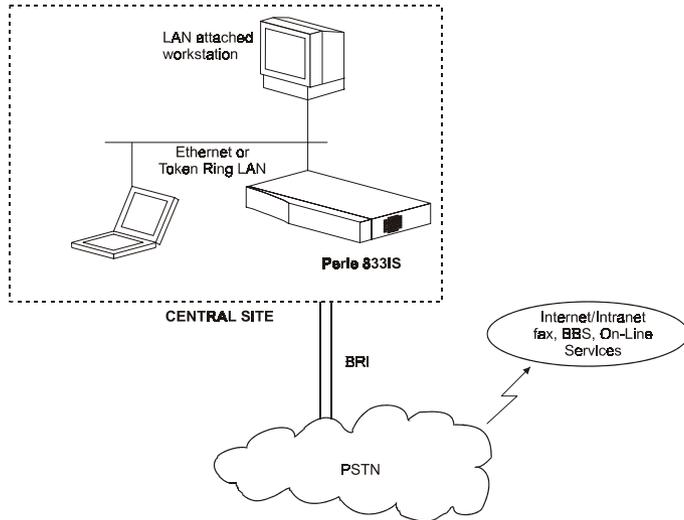
The network protocol, AppleTalk, and the WAN protocol, Apple Remote Access (ARA) are specific to the Apple network environment.

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 833IS as Dial-Out modems. To the PC application, the PerleDSP Modem and line attached to the 833IS 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.



The Dial-Out client communicates with the 833IS using either IP or IPX protocol. When the Dial-Out client starts, he locates all 833IS servers on the network which are available for Dial-Out. For each Server, a list of lines that can be used for Dial-Out are displayed.

The 833IS 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 2000

- Windows Communication Interface (COM port redirection)

Dial-Out will use the internal PerleDSP Modems of the 833IS and a channel of the ISDN BRI line. Although there are significant differences between making a call on an ISDN line and a standard phone line, the 833IS 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 241.

Configuration Overview

The 833IS 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:

- The Cards installed in your 833IS.
- Server name.
- Server password.
- Server MAC address.
- Date and time.
- ISDN 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 833IS. 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.

Creating



To create a new configuration file:

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

*If you are NOT currently connected to a server, the **New Configuration** window will appear and prompt you to choose which server type you wish to configure.*

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 833IS from the list.
3. The **Log On** dialog box appears. Enter a **User ID**, **Password** and **Server Password** if configured, and click **OK**. If a **Server Password** is not configured then the User must have administrative privileges to proceed.



*The default administrative name for an unconfigured 833IS is: User ID: **superusr**, no password and no server 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. A TFTP dialog window will be displayed indicating the upload process of the configuration file.
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 833IS for the parameters to take effect.

For system changes to take effect, the 833IS must be reset. If a system reset is done, all sessions will be terminated.

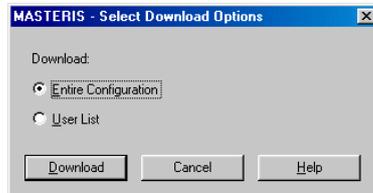
The only changes which do not require a system reset to take effect are changes to the user data base. These can be downloaded at any time and will take immediately. However, changes made to a user who is currently connected to the server will only take effect the next time the user attempts to connect. For example, 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 833IS.
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:



- **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 TFTP server dialog window will be displayed as the configuration is downloaded:
 6. When the download is complete, the **Reset** dialog box will appear if the entire configuration was downloaded.
 7. At this point you will be prompted to **Cancel** or **Reset**.

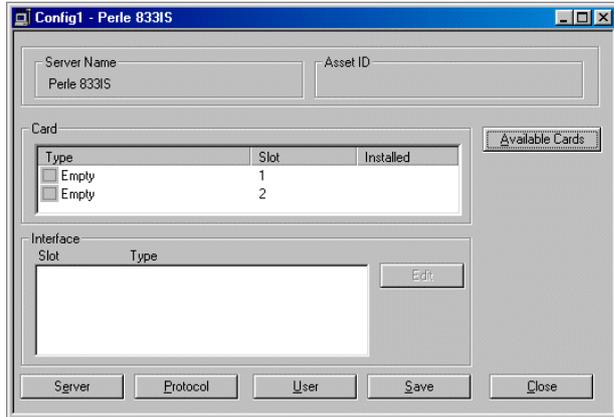
Configuration Main Window

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

The 833IS reports to the Manager which cards are installed, allowing you to determine which cards require configuration. If you are not connected to the 833IS 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 a Feature card in the future, you can pre-configure it. 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.

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



Server Name

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

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 type of cards in this 833IS. It also is used to add and remove cards.

Type

The type of Feature Card installed in this slot.

Slot

The slot of the Feature Card.

Using Configuration Files

Installed

Indicates whether the Feature Card is installed in this slot.

If the Manager is currently attached to the 833IS being configured, the Card list will display all cards detected by the 833IS 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.

Available Cards

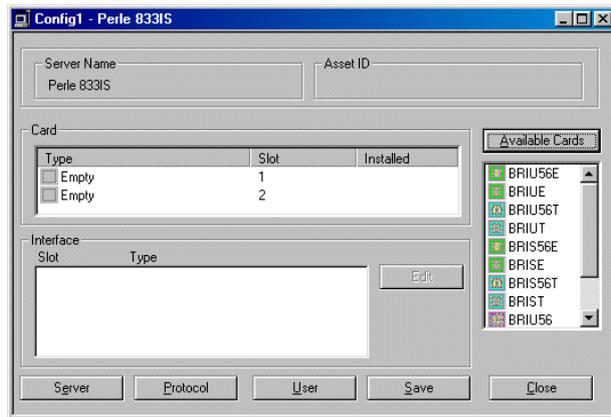
Used to add and remove Feature cards to the configuration.

Adding



To add a new Feature Card to the Manager:

1. Click and release the **Available Cards** button to display a list of available cards that can be added to the configuration.



2. Click and drag the Feature card you wish to configure over an "Empty" slot in the Card area.

The card is now added. All interfaces associated with the new card will appear in the interface window below.

Removing

To remove a Feature Card from the Manager:

1. Click and drag the card you wish to remove over to the **Available Cards** area. The card is now removed from the configuration.

Interface

This area displays information about the Interfaces in this 833IS. It also is used to select an Interface to configure.

Slot

The slot of the Interface.

Type

The type of Interface installed in this slot.

Edit

Edits the configuration of the currently selected Interface.

Please refer to Chapter 6 on page 75 for details on "Configuring the Interfaces".

Server

Provides settings for the entire server. See "Chapter 9: Configuring the Server" on page 163.

Protocol

Access the protocol settings. See "Chapter 7: Configuring the Protocols" on page 89.

User

Access the configuration for the User Database. See "Chapter 8: Configuring the User Database" on page 135.

Save

Saves the configuration.

Close

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

Help

Displays Help for this configuration window.

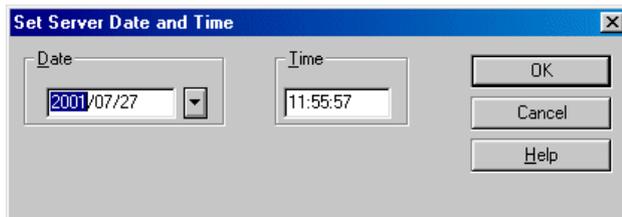
Setting the Date and Time

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

To set the 833IS Server date and time:



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



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

Chapter 6: Configuring the Interfaces

About Configuring the Interfaces

In this chapter, you will read about:

- Overview of Interface Configuration
- Interface selection screen
- Configuring the Ethernet LAN interface
- Configuring the Token Ring LAN interface
- Configuring the ISDN BRI U interface
- Configuring the ISDN BRI S/T interface
- Configuring the PerleDSP Modem interface

Overview

The 833IS has been designed to provide a highly integrated platform for remote access. Depending on your specific needs, the 833IS can support a variety of specific interfaces. The following is a list of the interface currently supported by the 833IS product family. Please note that not all of the interfaces listed below will necessarily be present on your 833IS unit.

LAN Interface

- 10 Mbps Ethernet via RJ-45 connector
- 100 Mbps Ethernet via RJ-45 connector
- 4 or 16 Mbps Token Ring via DB-15 (AUI) connector
- 4 or 16Mbps Token Ring via RJ-45 connector

Line Interface

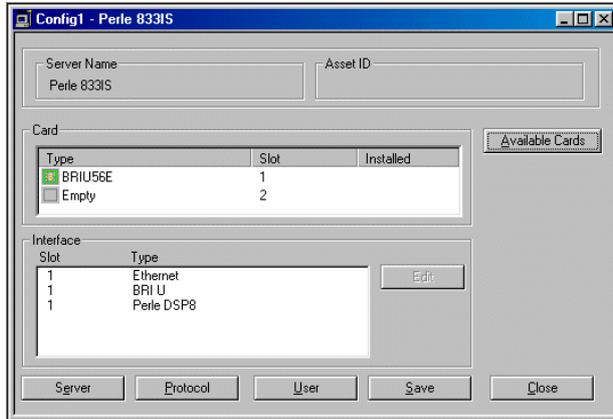
- ISDN BRI, U-interface via RJ-45 connector
- ISDN BRI, S/T-interface via RJ-45 connector

Modems

- V.90 or K56flex modems with no external connector required

For each of the above interfaces there is a default configuration available which attempts to satisfy the common environment. Please check the configuration over to ensure that it has been configured correctly for your specific environment.

Interface Selection Screen



The interface selection screen will display all interfaces present on each slot.

Editing

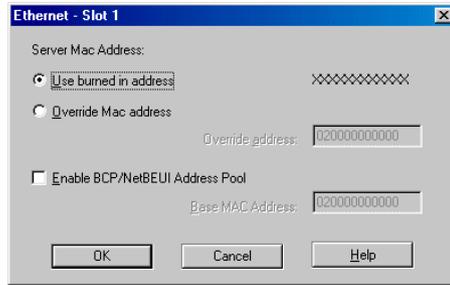


To Edit an interface on the Manager:

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

Configure the Ethernet LAN Interface

The Ethernet LAN interface configuration screen is as follows:



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 833IS. 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 characters hex. This address will be restricted by the Manager to a Locally 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 833IS 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 16 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 133. 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 126 for more details.

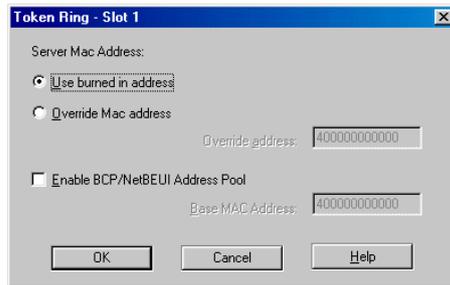
Configure the Token Ring LAN Interface

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 02FFFFFFF00 for Ethernet. You can use the default provided from a special manufacturer's range. However, all Perle 833IS 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 LAN Interface

The Token Ring LAN interface configuration screen is as follows:



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 833IS. 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 characters hex. This address will be restricted by the Manager to a Locally 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. For example, addresses starting with 40, 50, 60, 70, 41, 51... are legal.

Enable BCP/NetBEUI MAC Address Pool

Certain protocols require that the 833IS 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 16 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 133. 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 126 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 40FFFFFFF00 for Token Ring. You can use the default provided from a special manufacturer's range. However, all Perle 833IS 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 ISDN BRI Line Interface

Overview

An ISDN, BRI line is a digital transmission link with a capacity of 160Kbps. This bandwidth is split up into 2*64Kbps “B” channels which carry user data and a 16Kbps “D” channel used to transfer control information for such tasks as setting up and tearing down calls. From the user perspective, each “B” channel looks like an individual phone line with its own phone number. Each “B” channel can carry either pure digital data or digitized analog data. If the call originates from an ISDN type of a device (eg. a Terminal Adapter), the B channel will contain pure digital data. If the call originates from an analog device (eg. a modem), the B channel will contain a digital representation of the analog data. The latter type of traffic will require a digital modem to handle the data.

The ISDN interface is available in two types: A U interface and an S/T interface. To find out which type of interface you have follow this procedure.

- Look at the card name. This can be found on the back of the card or see “Feature Cards” on page 25.
- The first 3 letters should be BRI
- The fourth letter is either a U or an S.

If the fourth letter of the card name is a U, this is a U interface ISDN card. If it is an S, this is an S/T interface ISDN card.

The type of information which will be required for the line interface depends on the Network provider you have selected and the type of ISDN interface they provide. Different Telephone companies use different switches to handle the ISDN BRI lines which in turn require different parameters to be set up. In general, your ISDN provider should provide you with the information you will need to correctly configure the line interface. Some of the fields on the screen may not be required for your specific environment.

If you are unsure about any of the fields, ask your ISDN provider for the correct value for the field in question. If your ISDN provided has no information on a specific item, leave the field blank.

The 833IS needs to synchronize with the ISDN line. All BRI lines connected to an 833IS must be driven from the same clock. In most applications, the 833IS is connected to the telco network, and all clocks from the telco are guaranteed to be derived from the same clock. If you are connecting the 833IS to a PBX, ensure that the PBX is providing the line clock.

An S/T line can be ordered (or configured, if on a PBX) such that clocking is not supplied unless a call is active on the S/T line. It is strongly recommended that at least one S/T BRI line always provide line clock.

The 833IS will synchronize to the lowest number BRI line that provides clocking. When clocking is lost, it will switch to an internal clock while it looks for another BRI line providing clocking. Although this process is quick, calls on other BRI lines that are active while this clock is resynchronizing could experience data errors.

A BRI line will be assigned a phone number per B channel. However, it is not safe to assume that the phone number is tied to the channel. When a call comes in, it signals on the D channel what B channel the call is on, and what phone number is used. Thus it is possible to get a call on the first B channel from the second phone number.

ISDN BRI U Interface Configuration

The ISDN BRI U interface configuration screen is as follows:

BRI	SPID 1	SPID 2	Directory number 1	Directory number 2
1				
2				
3				
4				

Channel	Disabled	Used By Group	Dial In	Dial Out	Call Back	Name
1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$11F11
2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$11F12
3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$11F21
4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$11F22
5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$11F31
6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$11F32
7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$11F41
8	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$11F42

Network Protocol

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

Configure the ISDN BRI Line Interface

- US NI-1
- AT&T 5ESS
- Northern Telecom DMS 100

SPID (Service Profile Identifiers)

The Service Profile Identifier is a string assigned to an interface or channel by the service provider. The SPID configured on the 833IS is sent to the service provider at start-up. This is used by the service provider to assign class of service to a channel.

Depending on the Service Provider you may be assigned 1 or 2 SPIDS. If your Service Provider has only provided you with 1 SPID, leave the SPID2 field blank.

Directory Number1, Directory Number 2

To have the router verify a called-party number in the incoming setup message for ISDN BRI calls, the directory numbers need to be configured. For the US-NI-1 and DMS-100 switch types, both directory numbers must be set. For the 5ESS switch type, you may need to set none, one, or both directory numbers depending on your ISDN subscription. For the NET3 and NTT switch-types, all incoming calls will be accepted if the directory numbers are not specified.

BRI/Channel

Indicates the interface number and channel number.

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.

Used By 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 182.

Dial-In

When checked, channel will accept dial in calls.

Dial-Out

When checked, channel is available for dial out calls.

Callback

When checked, channel is available for callbacks.

Name

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

- 833IS Manager Statistics
- 833IS Front Panel

Maximum length is 16 characters. The default name is automatically generated as SxIFyz, where x = slot number, y = interface number and z = channel number.

ISDN BRI S/T Interface Configuration

The ISDN BRI S/T interface configuration screen is as follows:

Channel	Disabled	Used By Group	Dial In	Dial Out	Call Back	Name
1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$1IF11
2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$1IF12
3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$1IF21
4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$1IF22
5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$1IF31
6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$1IF32
7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$1IF41
8	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	\$1IF42

Network Protocol

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

- US NI-1
- AT&T 5ESS

Configure the ISDN BRI Line Interface

- Northern Telecom DMS 100
- ETSI Net3 (Europe)
- NTT INSnet64 (Japan)

TEI Topology

The Terminal Endpoint Identifier (TEI) can be configured to either:

- Automatic - The Terminal Endpoint Identifier (TEI) is negotiated automatically between the 833IS and the carrier.
- Fixed - The Terminal Endpoint Identifier is constant whose value is between 0 and 63. This information is supplied by the carrier.

Directory Number1, Directory Number 2

To have the router verify a called-party number in the incoming setup message for ISDN BRI calls, the directory numbers need to be configured. For the US-NI-1 and DMS-100 switch types, both directory numbers must be set. For the 5ESS switch type, you may need to set none, one, or both directory numbers depending on your ISDN subscription. For the NET3 and NTT switch-types, all incoming calls will be accepted if the directory numbers are not specified.

BRI/Channel

Indicates interface number and channel number.

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.

Used By 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 182.

Dial - In

When checked, channel will accept dial in calls.

Dial - Out

When checked, channel is available for dial out calls.

Callback

When checked, channel is available for callbacks.

Name

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

- 833IS Manager Statistics
- 833IS Front Panel

Maximum length is 16 characters. The default name is automatically generated as SxIFyz, where x = slot number, y = interface number and z = channel number.

Minitel Enabled

When checked, support for Minitel servers is enabled. This is a special feature used by Minitel Servers to allow the first 3 minutes of a connection to be free (i.e billing starts when the call is connected, but the CONNECTED message is delayed for 3 minutes using a caveat in the Q.931 specification).

Configuring the Perle DSP Modem Interface

No configuration is necessary for the modems to operate in the 833IS. 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.

The following parameters can be set:

Modem	Enable	Name	Used by group	Modify	Modem Initialization String
1	<input checked="" type="checkbox"/>	\$2M1	<input type="checkbox"/>	<input type="checkbox"/>	
2	<input checked="" type="checkbox"/>	\$2M2	<input type="checkbox"/>	<input type="checkbox"/>	
3	<input checked="" type="checkbox"/>	\$2M3	<input type="checkbox"/>	<input type="checkbox"/>	
4	<input checked="" type="checkbox"/>	\$2M4	<input type="checkbox"/>	<input type="checkbox"/>	
5	<input checked="" type="checkbox"/>	\$2M5	<input type="checkbox"/>	<input type="checkbox"/>	
6	<input checked="" type="checkbox"/>	\$2M6	<input type="checkbox"/>	<input type="checkbox"/>	
7	<input checked="" type="checkbox"/>	\$2M7	<input type="checkbox"/>	<input type="checkbox"/>	
8	<input checked="" type="checkbox"/>	\$2M8	<input type="checkbox"/>	<input type="checkbox"/>	

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 182.

Name

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

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

Maximum length is 16 characters. The default name is automatically generated as `SxMy`, where `x` = 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 833IS. 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 182.

The modem behaves differently from a stand-alone modem because it does not directly interface to the telephone line. Phone call handling is done by the ISDN BRI interface. Once the call is established it is switched to the modem. Therefore, modem commands that do line control (such as ATA, ATH) may behave slightly different then they would in the case of a modem which is connected to a telephone line.

V.90 Modems

A V.90 modem obtains its high data rates by treating the analog data line as an imperfect digital line. This "digital line" appears to the modem as having a number of impairments, and the modem during negotiation attempts to determine what impairments exist, then compensate for them. Certain connections (for example, some GSM modem connections) can trick this negotiation. If this occurs, either the modems will not negotiate, or they will connect, but the data error rate will be so high as to make the connection impractical.

If these problems are encountered, it is necessary to prevent the modems from attempting to negotiate V.90. Modems have parameters that can be set to disable the V.90 modem. This can be done either in the client modem or by setting the Modem Initialization String in the 833IS modem.

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 Perle 833IS supports a variety of different communication protocols. The protocols are used on the communication line to transport data between different devices. Protocols in the 833IS 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 (ARA)
- BCP

The 833IS supports IP, IPX, NetBEUI, ARA and BCP as routed protocols. Other protocols are handled by bridging. See “Client Handling” on page 64 for details.

WAN Transport

Protocols are used to transport data across the dial in connection between the client PC and the 833IS or between the 833IS and a router on another LAN. These

protocols are designed to optimize transmission across a WAN connection. The networking protocol is encapsulated within the WAN transport protocol. Protocols supported for WAN transport by the 833IS are:

- PPP
- ARA

833IS Management

Protocols are used between the 833IS Manager and 833IS. Protocols supported for managing the 833IS 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 833IS, you have to define the 833IS itself as a node on the IPX or IP network. This requires setting up IP or IPX address parameters for the 833IS itself.

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

The 833IS 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 833IS supports BCP.

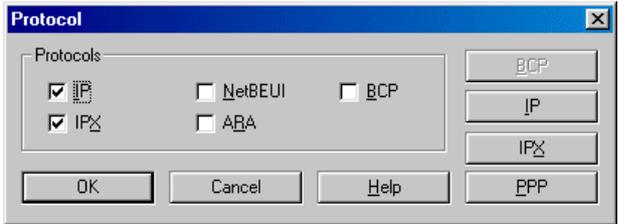
No configuration is required for ARA.

Configuring the Protocols

To configure the Protocols:

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

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



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 accessible.
- 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 Protocol

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 833IS itself and establish IP parameters for the WAN client's dialing in to the 833IS.

For IP, the 833IS looks like a router between two networks. The first network is comprised of the devices on the LAN. The second network, referred to as the "Internal WAN network", is comprised of all IP clients and routers that are dialed into the WAN ports. Setting up a basic 833IS IP configuration requires the following:

- Defining the network on the LAN side, and defining the address of the LAN router port.
- Defining the network on the WAN side, and defining the address of the WAN router port.

All clients dialed into the WAN, see the same address for this WAN router port.

- Each client dialing in requires a unique IP address. The 833IS supports multiple methods for defining and supplying IP addresses to clients.

For the 833IS router to be able to route IP packets, it has to know how to reach the destination. The 833IS supports the following methods:

- RIPV1 and RIPV2.
- Default gateway.
- Static routes.
- Proxy ARPs.

It may be desirable to restrict certain IP traffic. The 833IS has the following features that can be used to do this:

- Static routers.
- IP Packet filters.

The 833IS has the ability to forward the address of a DNS or WINS server to a dial in client.

In general, it is recommended to define the Internal WAN network distinct from the LAN network. It is possible to define the Internal WAN network as a subnet of the LAN network, but there are limitations:

- Routers on the LAN using RIP V1 cannot discover the Internal WAN network, and will not be able to route to the dial in clients on the Internal WAN network.
- DHCP is not supported for dial in clients in this mode.

Defining the Internal WAN network as a subnet can still be useful if:

- Routers on the LAN use RIP V2. RIP V2 sends subnet information and any routers on the LAN network using RIP2 will be learned.
- All WAN traffic uses the configured default gateway.
- Static routes are defined.
- The "Enable Proxy ARP" setting is used.

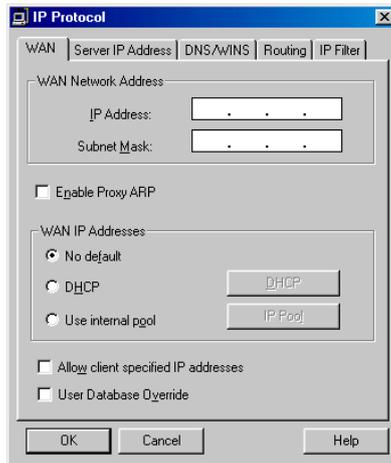
Directed IP traffic from a dial in client will reach another dial in client in the same 833IS. However, IP broadcasts from a dial in client will not reach another dial in client. Most applications will work, but IP applications that rely on broadcast or multicast messages (such as NetBEUI over IP) are not supported.

If a router dials in to the WAN, the 833IS can route traffic from the dial in router to the LAN. This feature is referred to as "LAN-to-LAN". Note that it is not possible to route from this dial in router to a client or router on the Internal WAN network.

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

WAN

The **IP Protocol - WAN** screen is as follows:



WAN Network Address

Clients dialing in to the 833IS must be assigned IP addresses on an Internal WAN Network. This section defines the Internal WAN Network used by the 833IS 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.

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.

All dial in IP devices that are dialed into the WAN appear as if they are on their own IP network. This network is referred to as the "Internal WAN Network". The 833IS also requires one address on this network for the router port.

In general, it is recommended to define the Internal WAN network distinct from the LAN network. It is possible to define the Internal WAN network as a subnet of the LAN network, but there are limitations:

- Routers on the LAN using RIP V1 cannot discover the Internal WAN network, and will not be able to route to the dial in clients on the Internal WAN network.
- DHCP is not supported for dial in clients in this mode.

Defining the Internal WAN network as a subnet can still be useful if:

- Routers on the LAN use RIP V2. RIP V2 sends subnet information and any routers on the LAN network using RIP2 will learn about the Internal WAN network.
- Static routes are defined.
- The "Enable Proxy ARP" setting is used.

To set the WAN Network Address, the following fields must be defined:

IP Address

Enter the IP address that will be used by the 833IS on the Internal WAN Network for its router port. Be careful to ensure that this address does not conflict with any dial-in client IP addresses.

Subnet Mask

Enter the subnet mask for the internal WAN network

Enable Proxy ARP

Devices that are connected on the same IP network discover each other by sending a message on the local network known as an ARP (Address Resolution Protocol). On the 833IS, the Internal WAN network is usually defined as a different network from the LAN network, and ARPs are not used. If the Internal WAN network is defined as a subnet of the same LAN network (as described in "WAN Network Address" on page 103z), Proxy ARPs can be enabled so that a device on the LAN can discover a dial in client. There are some limitations associated with Proxy ARP:

- IP broadcasts will not be forwarded in this mode. Most applications will work, but IP applications that rely on broadcasts or multicasts (such as NetBEUI over IP) are not supported.
- There is a small performance penalty if Proxy ARPs are enabled.

Check the "Enable Proxy ARP" field to enable Proxy ARP.

WAN IP Addresses

Clients dialing in to the 833IS 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 833IS LAN port segment. The 833IS will route packets between the LAN port segment and the Internal WAN Network. The Perle 833IS can manage the client IP addresses using a number of different schemes:

- You can define an internal pool of IP addresses in the 833IS. 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 833IS 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 833IS 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 "Enter the IP address of the Secondary WINS server. Blank indicates no Secondary WINS server." on page 104 for more details.

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

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 addresses 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 833IS 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 99.

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

In DHCP, a “scope” is defined as “An administrative grouping of computers running the DHCP client.” These computers are grouped according to a range of IP addresses. Simply put, all dial-in clients on 833IS share the same scope, namely the range of addresses defined for the Internal WAN network.

On the DHCP server, you must define a scope that matches the IP address range for the dial-in clients on an Internal WAN network. Ensure that the IP address of the Internal WAN network itself is excluded from the scope, so the DHCP server does not attempt to assign this address to a dial-in client.

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

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



DHCP Server Discover

Select **Discover** to allow the 833IS 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 833IS to use the leased IP address on behalf of the client. The range is 1 to 65535 minutes. Longer lease times will increase the chances that the client can reconnect to the 833IS and get the same IP address.

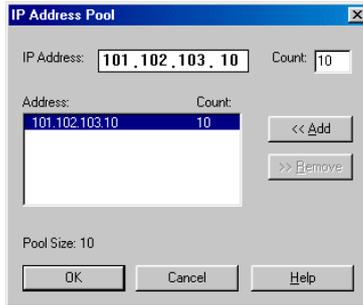
Reconnect Enable

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:



The screenshot shows a dialog box titled "IP Address Pool". It contains the following fields and controls:

- IP Address:** A text field containing "101.102.103.10".
- Count:** A text field containing "10".
- Address:** A list box containing "101.102.103.10", which is currently selected.
- Count:** A text field containing "10" next to the list box.
- Buttons:** "<< Add" and ">> Remove" buttons are located to the right of the list box.
- Pool Size:** A label "Pool Size: 10" is located below the list box.
- Bottom Buttons:** "OK", "Cancel", and "Help" buttons are located at the bottom of the dialog.

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 16 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.

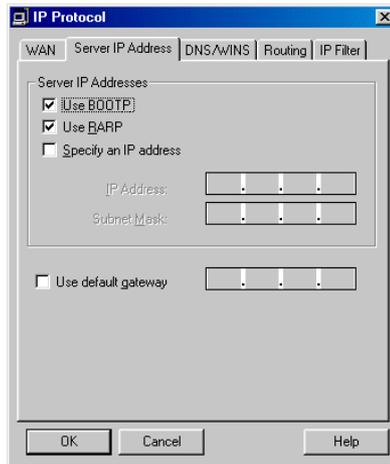
To remove IP addresses from the pool, highlight the entry in the **IP Pool** display and click **Remove**.

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.

Server IP Address

The **IP Protocol - Server IP Address** screen has the following settings:



The Server requires an IP address that uniquely identifies the unit to the IP network. The Perle 833IS 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 Perle 833IS 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 833IS to do this. This address can be obtained from the Front Panel.

Use BOOTP

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

Configuring IP Protocol

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 833IS will attempt to acquire the **Server IP** address from a RARP server.

Specify an IP Address

When checked, the 833IS 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.

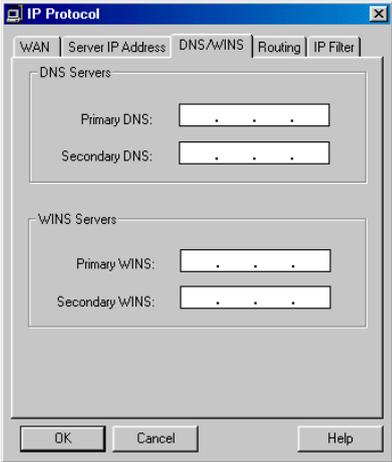
Use Default IP Gateway

When checked, lets the 833IS 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.

DNS/WINS

The 833IS 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 833IS will forward the configured values. The **IP Protocol - 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.

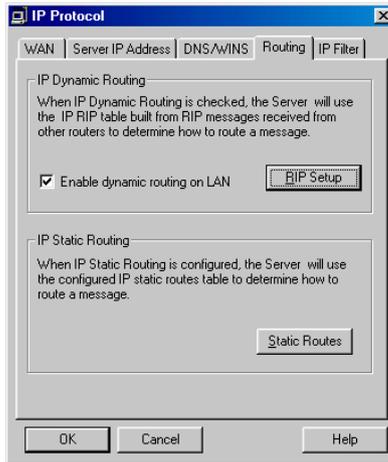
Configuring IP Protocol

Secondary WINS

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

Routing

The **IP Protocol - Routing** screen has the following settings:



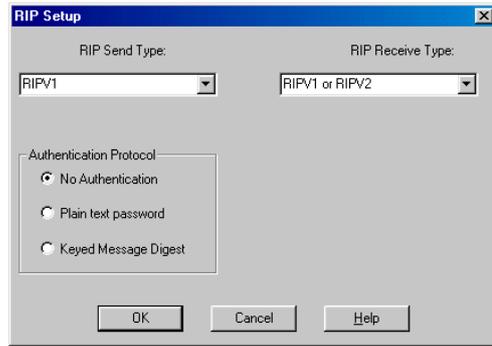
Enable Dynamic Routing on LAN

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

RIP Setup

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

The RIP Configuration screen has the following settings:



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 RIPs
- 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 IPv2, you have the option of choosing the form of authentication protocol to be used when processing IPv2 messages. If IPv2 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")

Static Routes

When dynamic routing is enabled, the Perle 833IS 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 creating an IP RIP Table for the networks it knows about.

There is room in this table to keep entries for 600 routers. If there are more routers than this in the networks to which your 833IS is connected (both local and LAN to LAN), some of the RIP table entries will be overwritten and unavailable.

For most networks, there is no benefit to disabling IP dynamic routing. You may wish to disable 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 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.

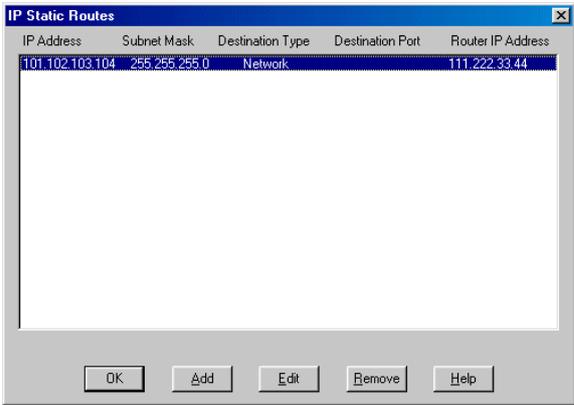
By defining IP static routes and disabling dynamic routing, the network administrator can configure the Perle 833IS with the addresses of only the routers needed to reach the desired routes and the Routing Table will not change.

The static routing feature can also be used to restrict which hosts (servers) can be accessed from the 833IS. 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 833IS 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.

Configuring IP Protocol

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

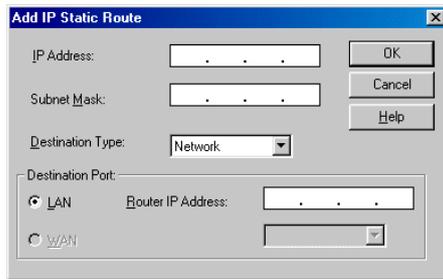
To edit an existing entry, select an entry from the table, and click the **Edit** button.

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:



The screenshot shows a dialog box titled "Add IP Static Route" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- IP Address:** A text input field with a dotted placeholder (". . .").
- Subnet Mask:** A text input field with a dotted placeholder (". . .").
- Destination Type:** A dropdown menu currently set to "Network".
- Destination Port:** A section with two radio buttons: "LAN" (selected) and "WAN".
- Router IP Address:** A text input field with a dotted placeholder (". . .") located next to the LAN radio button.
- Buttons:** "OK", "Cancel", and "Help" buttons are located on the right side of the dialog.

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 833IS'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.

IP Filter

The **IP Protocol - IP Filter** screen has the following settings:



The Packet Filtering feature allows the Perle 833IS 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 833IS or to each user or to both.

Filters will be used by the Perle 833IS 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 833IS. These records will be sent to the Local Perle 833IS when a user dials in and makes a connection.

RADIUS

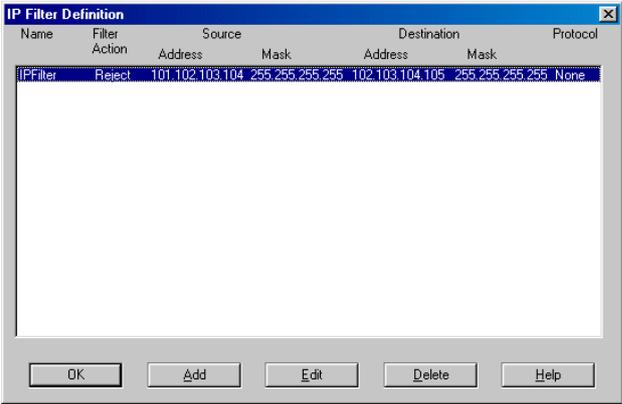
To use packet filtering with the RADIUS security server:

1. Define the filters on the Perle 833IS 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 833IS, the name of the filters will be sent from the RADIUS server to the Perle 833IS.

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 **IP Protocol - IP Filter** screen, the **IP Filter Definition** window appears. The fields are as follows:



Add

To add a filter definition, click **Add**. The **Add IP Filter Definition** window will appear. See “Add/Edit IP Filter Definition” on page 112 for details on how to create a filter definition.

Edit

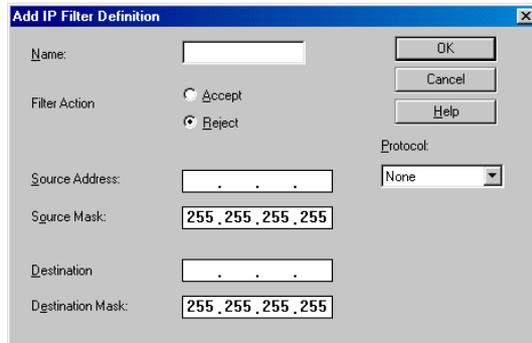
To edit a filter definition, select a filter from the list and click **Edit**. The **Edit IP Filter Definition** window will appear. See “Add/Edit IP Filter Definition” on page 112 for details on how to modify the filter definition.

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:



The screenshot shows a dialog box titled "Add IP Filter Definition". It contains the following fields and controls:

- Name:** A text input field.
- Filter Action:** Two radio buttons, "Accept" and "Reject". The "Reject" radio button is selected.
- Source Address:** A text input field with three dots (". . .").
- Source Mask:** A text input field containing "255.255.255.255".
- Destination:** A text input field with three dots (". . .").
- Destination Mask:** A text input field containing "255.255.255.255".
- Protocol:** A dropdown menu currently set to "None".
- Buttons:** "OK", "Cancel", and "Help" buttons are located on the right side of the dialog.

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 None, 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. To change the order of the assigned filter, select the IP filter to move and while holding down the left mouse button, drag the entry to the new location. See “IP Filter” on page 109 for more details on how the filters are used.

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



Configuring IPX

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 833IS 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.

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**.

Configuring IPX

The 833IS 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 833IS 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

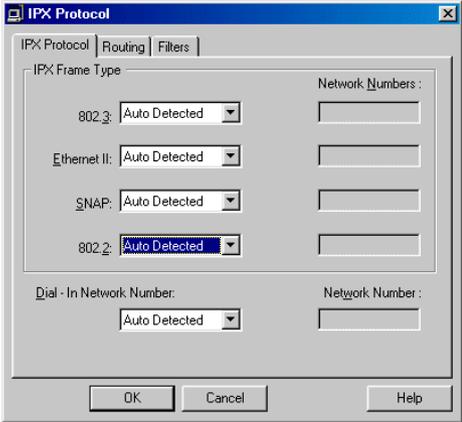
For Token Ring, IPX can be transported over these frame types:

- 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.

IPX Protocol

The **IPX Protocol - IPX Protocol** screen has the following settings:



IPX Frame Type

For each available frame type, you can select:

Auto Detected

The 833IS 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 833IS 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 833IS 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 833IS 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 Number** is formatted as 1 to 8 hex digits. The numbers FFFFFFFF and 0 are reserved.

Routing

The **IPX Protocol - Routing** screen has the following settings:



Enable Dynamic Routing on LAN

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

IPX Static Routing

When checked, the 833IS 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.

Static Route

The Perle 833IS 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

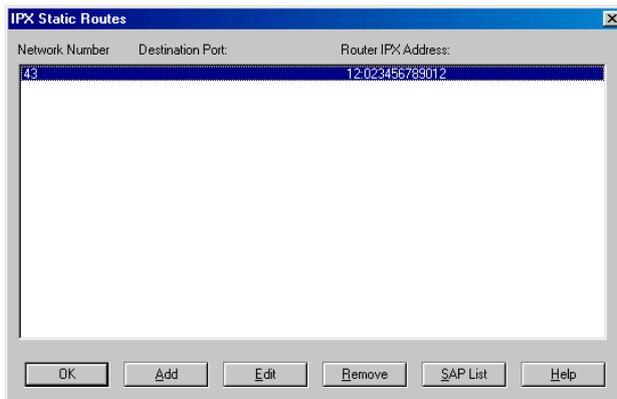
the Perle 833IS IPX routing tables to store 250 RIP entries and 500 SAP entries. If your network has more routers and services than this, some of the table entries will be overwritten and those routes and services will be unavailable.

Static routing lets the network administrator configure the Perle 833IS 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 833IS'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.

The dialog box is titled "Add IPX Static Route". It features a "Destination Network Number" input field at the top left. To the right of this field are three buttons: "OK", "Cancel", and "Help". Below the "Destination Network Number" field is a "Destination Port" section. This section contains two radio buttons: "LAN" (which is selected) and "WAN". The "LAN" radio button is associated with a "Router IPX Address" section, which includes a "Network Number" dropdown menu and a "Node Address" input field. The "WAN" radio button is associated with a dropdown menu.

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

Network Number

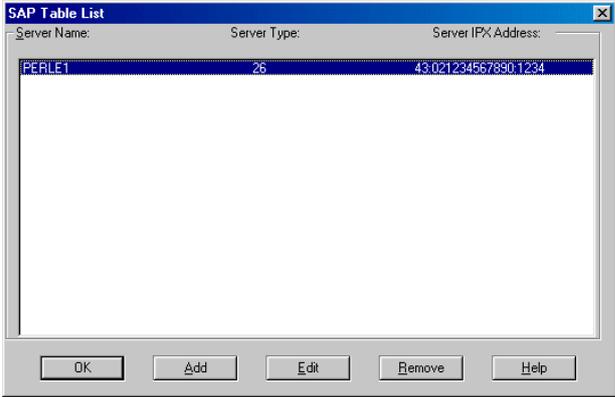
Specifies the **Network Number** for the local router. This must be one of the network numbers that was configured in the IPX Frame Type section on the previous screen.

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 hexadecimal digits.

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

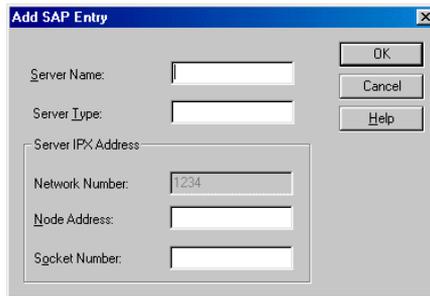
Add
To configure a new SAP entry, click on the **Add** button.

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:



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 hexadecimal 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.

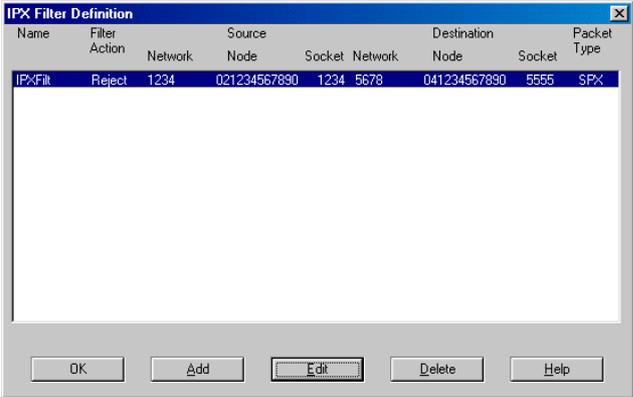


If Static Routing is enabled and the Manager is not on the local subnetwork, then the route to the Manager's network must be defined. A SAP entry is not created for the Manager.

If you are using any security servers configured for IPX (i.e. Novell Bindery, Axent, NT Domain) to provide 833IS 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 124 for details on how to create a filter definition.

Edit

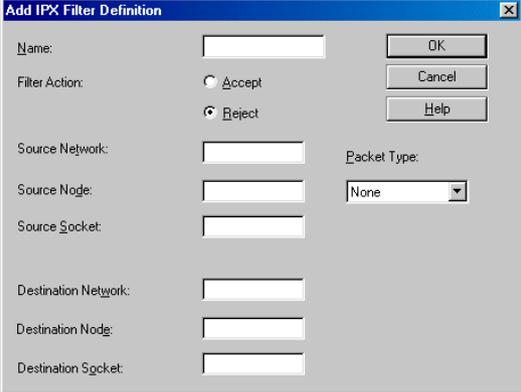
To edit a filter definition, select a filter from the list and click **Edit**. The **Edit IPX Filter Definition** window will appear. See “Add / Edit IPX Filter Definition” on page 124 for details on how to modify a filter definition.

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:



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 hexadecimal 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 None, 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 allows 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 “IP Filter” on page 109 for more details on how the filters are used.

Configuring the Bridge Function (BCP)

To assign IPX filters for the 833IS, follow these steps, click **Filter Assignment**. The **Server Filter Assignment** window appears.



See “Filter Definition” on page 110 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 833IS 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:

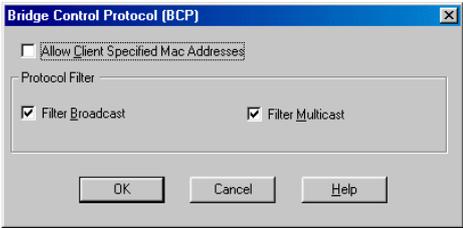
- If the protocol on the Client PC does not need the MAC address at the time the PC is started.
- If it is not important that the user always has the same MAC address.
- You can enter the MAC address in the user database for some users and use the internal pool for the others.

The 833IS 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 833IS. All other addresses will be discarded in hardware.

When a user connects with Bridge Control Protocol (BCP) to the 833IS, 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 LAN Interface” on page 77 and “Configure the Token Ring LAN Interface” on page 78.

The **BCP** screen is as follows:



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

Configuring the Bridge Function (BCP)

filtering should be set. The filter settings have no effect on Routing clients such as Perle Remote or Windows Dial Up Networking clients.



Filter Broadcast

When checked, the 833IS will not pass any broadcast messages received from the LAN to the WAN client.

Filter Multicast

When checked, the 833IS will not pass any multicast messages received from the LAN to the WAN client.

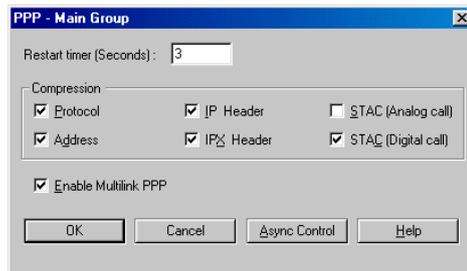
Configuring PPP

PPP is used for communication between the Dial-In PC and the 833IS. 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 833IS.

When a client dials in to the 833IS, 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 833IS. 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:



Time-outs Restart timer

When the 833IS connects with the client, they negotiate operational values between them. It is possible that the client will not respond to an 833IS negotiation message. This timer sets the maximum time the 833IS will wait for a response to negotiation messages.

Compression Protocol

When checked, the 833IS will attempt to negotiate protocol compression during connection. This reduces the size of the PPP header. For protocol compression to be used, both the 833IS and the client must negotiate this option.

Configuring PPP

Address

When checked, the 833IS will attempt to negotiate address compression during connection. This reduces the size of the PPP header. For address compression to be used, both the 833IS and the client must negotiate this option.

IP Header

When checked, the 833IS will attempt to negotiate IP header compression.

IPX Header

When checked, the 833IS will attempt to negotiate IPX header compression.

STAC (Analog Call)

When checked, the 833IS will attempt to negotiate STAC compression (software compression) for all analog calls.

STAC (Digital Call)

When checked, the 833IS will attempt to negotiate STAC compression (software compression) for all digital calls.

Enable Multilink PPP

By default, Multilink PPP is enabled for all dial in clients. To disable you may wish to disable Multilink PPP if:

- You want to restrict dial in clients to a single PPP session
- The dial in client you are using does not support the negotiation of Multilink PPP. On connect, the 833IS will check with the client to see if it wishes to use Multilink PPP. Some clients (for example, MacPPP) do not support this negotiation and will fail to connect.

Async Control

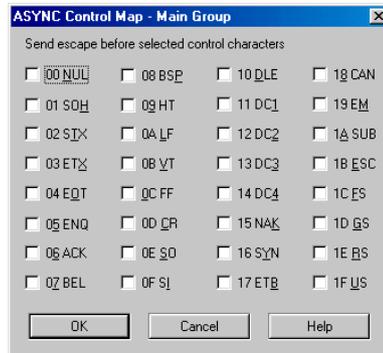
Click this button to access the **Async Control** screen.

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 an ISDN BRI connection to the phone network, all control characters may be transmitted by the 833IS. 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 833IS, and no control characters should need to be set in the 833IS **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.



Apple PPP

PPP was originally available on the Mac using freeware PPP stacks. The two most popular were FreePPP and MacPPP. In Mac OS 7.6, Apple introduced a PPP client which has evolved to the current Remote Access Client.

Recent versions of this client also supports PPP transport of AppleTalk, known as MacIP. MacIP is not supported by the 833IS.

On connect, the 833IS will check with a dial in client to see if it wants to use Multilink PPP.

MacPPP does not support this negotiation and will fail. To resolve this, disable Multilink PPP on the PPP configuration screen.

Using AppleTalk

The native protocol for the Apple Macintosh is AppleTalk. AppleTalk is a transport layer protocol, providing similar functionality to IP. This protocol is used for connecting to native Apple file servers (known as AppleShare), other Macintoshes, and to printers. A remote Macintosh user connects using Apple Remote Access Protocol (ARAP), which provides similar functionality to PPP. Unlike PPP, ARAP can transport only one protocol, namely AppleTalk.

Until recently, a Macintosh user that wished to use ARA would have to purchase Apple Remote Access client. This is now bundled with PPP in a single client called "Remote Access Client", included with the Mac OS. This client supports version 2.1 of ARA.

ARAP cannot be transported "as is" across a digital (ISDN) dial up connection but is supported using V.120 rate adaptation.

The Perle 833IS 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 833IS and access the AppleTalk network. AppleTalk is supported on both Ethernet and Token Ring connected Perle 833ISs. 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 833IS. 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 833IS. This name and password will be used solely to access the 833IS, and do not correspond to names and passwords used to access any other Macintosh.

Fixed callback is supported by the ARA client.

Using NetBEUI

The Perle 833IS 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 833IS emulate a LAN adapter. The 833IS 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 LAN Interface” on page 77 and “Configure the Token Ring LAN Interface” on page 78 for details on defining the pool.

Because the Perle 833IS 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 833IS, the user must be defined to the system. You can do this in a number of different ways:

833IS Internal Database

You can define the user in the internal database of the 833IS. 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.
- Callback.
- Protocols
- Compression
- Packet Filtering
- Lan To Lan

Shared User Database

Access to an 833IS can be controlled by using the Internal Database that is configured in a Remote 833IS server.

External Security Systems

The 833IS can use network security servers to control access to the 833IS. The servers supported are: **Novell Bindery, RADIUS, Axent, SecurID and 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 833IS 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 833IS can store user records for 500 users. These user records are used:

- For password authentication if the 833IS has been configured for User Database security. See “Configuring User Authentication Security” on page 171.
- To assign either a fixed MAC address for Bridging clients, or a User IP address for IP clients.
- To provide information on Callback 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 administrative privileges. The **Use Standard Profile** checkbox on this screen tells the 833IS to use the settings for callback, inactivity time-outs and connect time limits that were defined in the **Standard Profile**.

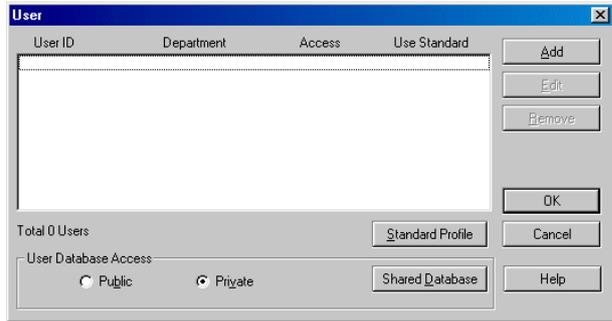
If you wish to use different settings from the Standard Profile for this user, deactivate **Use Standard User Profile**. You can then get three additional tabs, User Profile, Protocols and User Callback presented, in order to change additional parameters for this user.

Configure the Internal User Database

From the Configuration File window, click on **User**.

User Main

The User main screen appears. Fields are as follows:



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 the Standard profile.

Add

Adds a user to the database.

Configure the Internal User 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.

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 833IS 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 833IS. However, the local Perle 833IS can access the user databases on other Perle 833IS servers on the LAN if the local server is configured for **Search Remote**.

Shared Database

Click this button to configure the 833IS 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 833IS Manager for configuration and monitoring.

The **Add/Edit User - User** screen is as follows:

User Disabled

A user record is enabled by default. If you want to prevent a user from accessing the 833IS, 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.

Configure the Internal User Database

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 833IS Manager to configure and monitor this 833IS.



It is recommended that at least one user record be created with administration privileges for each 833IS 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.

Use Standard User Profile

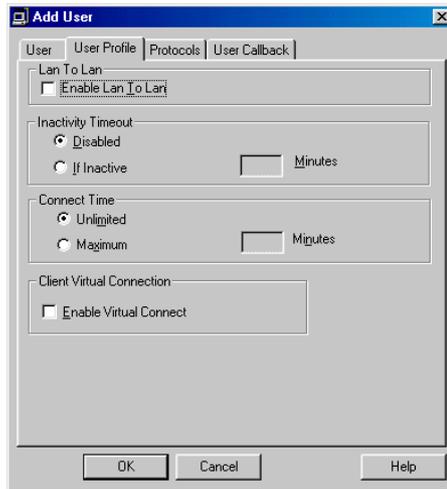
When checked, the values in the **Standard Profile** will be used for this User. If you wish to use **Fixed Callback** (i.e. callback from the 833IS to a number stored in the user database), the **Standard Profile** cannot be used.

When cleared, additional Tabs will be shown, allowing these values to be customized for the user.

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, and Client Virtual Connection for this user. These values will override the values set in the Standard Profile.

The **User Profile** screen is as follows:



Enable Lan To Lan

When checked, this option allows a remote Router to access the 833IS. Enabling this will bring up a Lan To Lan tab that allows parameters for the remote router to be set. Refer to the Lan To Lan section on page 147 for more detail on these parameters.

Inactivity Timeout

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.

Configure the Internal User Database

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.

This feature is can be used by remote IP or IPX dial in clients to save on connection charges. With client virtual connect enabled, the client can drop the physical connection, but the 833IS will keep the session active. The client can then reconnect and the 833IS will reassign the same session, and client IP address.

The Inactivity Timeout and Connection timers affect the virtual connection in the following manner:

- **Inactivity Timeout**

If there is no data transfer on the link for the duration set in this timer, the client session drops and the physical connection drops. Time in the virtual connection state is included. If "disabled" is set for inactivity timeout, the session will be released after 10 minutes in the virtual state. This is to prevent an unused session from being tied up permanently.

- **Connect Time**

The client will be disconnected and the session will be dropped after the time limit set in this timer, regardless of activity. Time in the virtual connection state is included.

If you are using Radius as your authentication server, you can configure the Radius server to set the Inactivity Timeout and Connect Time.

To be effective, the dial in client should support virtual connect. It should have a mode that:

- Drops the physical connection if inactive, but not notify the application of disconnect
- Automatically reconnects if data is to be sent

Reconnect to the 833IS is driven solely by the client in this mode. The 833IS cannot redial the client. In practice this is not a real limitation, as servers will typically only send data in response to a request from the client. However, if you are using a client application that supports unsolicited data from a server, you can configure the LAN to LAN feature for use with a dial in client.

Enable Virtual Connection

Click on this box to enable a client virtual connection.

This feature is used by remote Dial-in clients to save packet charges. The client drops the physical link to the 833IS 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.

Protocols

The **Protocols** screen is as follows:



Configure the Internal User Database

Protocols

Disable any **Protocols** that the user should not have access to by removing the check in the check box. IP and IPX protocols are enabled by default. However, if the server has any protocols disabled, then that protocol cannot be enabled for the User.

Compression

Enable Protocol compression for IP and IPX for a specific user. If enabled, compression will be done on the protocol headers.

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.

Addresses

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.

Fixed MAC Address:

The Fixed MAC Address field is used to assign a specific MAC address to a dial-up user. When the user connects using a BCP or native NetBeui client, the MAC address defined will be assigned to the user. If the MAC Address is not specified, one will be taken from the pool defined on the server or it may be specified by the dial-up client. If the user is on an Ethernet lan, the valid address range is 020000000000 - 02FFFFFFF00. If the user is on a Token Ring lan, the valid address range is 400000000000 - 40FFFFFFF00.

User Callback

With User Callback enabled, when a user dials into the 833IS, the 833IS will disconnect the call and then callback the user.

This can be used:

- *For additional security.* The user record can contain a phone number to be used for callback. Only if the user is at that phone number will access be permitted.
- *For centralized billing.* With callback enabled, the dial in session is charged to the server. The user pays only for the short initial connection to the 833IS.

Callback can be either Fixed or Roaming.

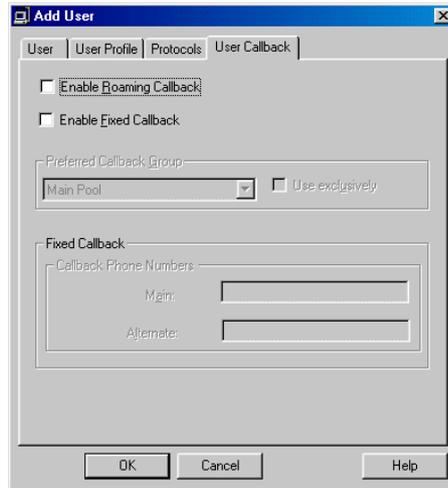
- With Fixed callback, the callback numbers are stored in the user database. In the 833IS database, two phone numbers can be stored – a main and an alternate callback number. During the initial connection, the client asks for a callback, and can optionally specify whether to callback the main or the 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 callback number can be set. RADIUS Callback ID is not supported.
- With Roaming callback, the client supplies the callback number at connect time. The client must support the Callback 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 callback is also supported by the Apple Remote Access client, using Apple's dial in protocol.

You can enable both roaming and fixed callback for a single user. If both are enabled, the 833IS will callback the roaming number if it is supplied at connect. If it is not supplied, fixed callback will be done. The dial-in client must support both fixed and roaming callback for this to work.

Callback is available both analog and digital ISDN BRI connections. 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 callback 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 243.

Configure the Internal User Database

The **User Callback** screen is as follows:



Enable Roaming Callback

When checked, this option will enable **Roaming Callback**. If a client asks for roaming callback during connect, the 833IS will callback with the number supplied by the client. If a client does not request roaming callback, the session will be established as if roaming callback was not checked.

If this option is not checked, any roaming callback requests will be rejected at connect time. Client behavior will be dependent on the client – the client may either continue the session without callback, or end the session.

Enable Fixed Callback

When checked, fixed callback will always be performed for this user when dialing in. If you are using the internal database, the callback will be done to the main phone number, or optionally to the alternate phone number if requested by the client. With RADIUS, the callback will be made to the phone number provided by the RADIUS server.

Preferred Callback Group

By default, a callback will be performed on the next available line that has been enabled for callback. If you wish to allocate a specific group of channels for callback by this user, select the group in the drop box. The callback group must have been previously defined.

Use Exclusively

If you check **Use Exclusively**, the callback will occur only if there is a free channel available in the selected group. If Use Exclusively is not checked, the callback will use another channel enabled for callback if a channel from the preferred group is not available.

Callback Phone Numbers

These are the phone numbers that are used by fixed callback. Each number can be up to 32 characters long. If you have enabled fixed callback, you must enter a Main phone number. The Alternate phone number is optional.

Lan To Lan

The LAN to LAN features allows a router to dial in to the 833IS. The network on the router's LAN can then communicate with the network on the 833IS LAN using IP or IPX.

Note that the communication is strictly between the router's LAN and the 833IS LAN for this connection. If a second router dials into the same 833IS, it cannot communicate with the first router.

The 833IS provides flexibility in the connection:

- The dial in router can originate the connection
- The 833IS can originate the connection on power up or if it loses contact with the dial in router
- A "virtual connection" can be established between the dial in router and 833IS. To save toll charges, it may be desirable to keep the link established between the dial in router and the 833IS only if there is data traffic. You can configure a "virtual connection" in the 833IS, which will keep the dial in session alive but drop the physical link if there is no data traffic. When there is data to be sent to the dial in router, it is dialed automatically and the data is then sent. This automatic reconnect is sometimes referred to as "dial on demand". Similarly, the dial in router can drop the connection, and reconnect to the same session when

it has data to send.

Routing Information

The dial in router and the 833IS need to learn about each other's network. This can be done by:

- Using dynamic routing. The routers exchange routing information (using RIPv2 for IP, or RIPv2 and SAPs for IPX) when they connect, and periodically refresh their routing information when they are connected.
- Using static routing. Static routes can be defined in the 833IS. Note that routing information can still be sent to the dial up router if static routes are defined.

If a virtual connection has been established, but the physical link has been dropped, the link is reestablished if the 833IS receives data that it knows that it has to send to the dial in router. It makes this decision based on the routing information that it has for the dial in router. With dynamic routing, the learned routes are stored for 12 hours. If there is a possibility that the dial in router and the 833IS will be physically disconnected for greater than 12 hours, you should:

- Use static routes, or
- Enable auto reconnect. This feature will force the 833IS to reconnect to the dial in router based on the time set in the "Reconnect Every" field.

For IP, by default the 833IS will send RIPv2 with no multicasts so as to be RIPv1 compatible, and receive RIPv1 or RIPv2. This can be changed in the LAN to LAN RIP Setup submenu. For IPX, routing information is always sent for a LAN to LAN connection if IPX is enabled. IPX (as well as other protocols) can be disabled for the LAN to LAN connection in the User Profile.

Note that no routing information is sent for a dial in client that is not defined as LAN to LAN.

It is strongly recommended that the dial in router use a fixed IP address. If a dynamic IP address is supplied (for example, from the Internal IP pool) inconsistent behaviour could result after a physical disconnect/reconnect.

LAN to LAN Connection Timers

There are timers that affect the LAN to LAN connection behavior, if virtual connection is not enabled:

- Inactivity Timeout

If there is no data transfer on the link for the duration set in this timer, the LAN to LAN session drops and the physical connection drops.

Note that any routing information exchanged between the 833IS and the dial up router will not be considered activity.

- **Connect Time**

The dial up router will be disconnected after the time limit set in this timer, regardless of activity.

If virtual connection is enabled, the Inactivity Timeout and Connect Time apply to the virtual session. Timers that affect the LAN to LAN connection when virtual connection is enabled are:

- **Inactivity Timeout (User profile)**

If there is no data transfer on the link for the duration set in this timer, the LAN to LAN session drops and the physical connection drops. Time in the virtual connection state is included.

- **Connect Time (User profile)**

The dial up router will be disconnected and the session will be dropped after the time limit set in this timer, regardless of activity. Time in the virtual connection state is included.

- **Disconnect If Inactive (LAN to LAN, Virtual Connection)**

If there is no data transfer on the link for the duration set in this timer, the physical connection is dropped, but the LAN to LAN session is maintained. This timer is in effect only after the "Connect a Minimum of" timer expires.

- **Connect a Minimum of (LAN to LAN, Virtual Connection)**

When the physical connection is established, this timer sets the minimum duration that the physical link stays active. A minimum duration may be required if dynamic routing is used (to allow the exchange of routing information).

- **Reconnect Every (LAN to LAN, Virtual Connection)**

This timer can be used to ensure that the physical link is periodically reestablished so that routing information is exchanged.

If you are using Radius as your authentication server, you can configure the Radius server to set the Inactivity Timeout and Connect Time.

Authentication

A dial in router is authenticated in the same manner as any other dial in user. The user ID and password must be set up in the authentication database that has been defined in the Security settings of the 833IS. Authentication that relies on token security (SecureID, Axent) cannot be used with the LAN to LAN feature, as the dial in router has no mechanism for responding to the security challenge. The 833IS will

send out PAP and/or CHAP requests as defined in the security settings, and the dial in router PAP/CHAP settings must match.

If the 833IS is calling the dial up router, the dial up router may need to authenticate the 833IS. The login (user) ID and password for the dial in router are entered in the Remote System Login section of the LAN to LAN screen. On connection the dial in router may request from the 833IS:

- A login ID
- A login ID and password
- Neither a login ID and password

Fill in the fields as required by the dial in router. The 833IS supports both PAP and CHAP authentication requests from the dial up router in this mode. Some routers (for example, some Cisco routers) can be configured to request a login ID even if the router is calling the 833IS. If the router calls the 833IS and requests a User ID and Password, the 833IS will send a User ID of "P833" and a Password of "PERL". This will not compromise security, as the 833IS must still authenticate the remote router against the User ID and Password in the User Record before a connection can be established.

Dialing the router

If the 833IS is configured to call the dial up router, the phone number of the router is configured in the "Primary Phone Number" field. When the 833IS needs to dial out, it will use an available channel that is enabled for dial out. You may wish to ensure that the 833IS always has a channel to dial the router. This can be done by enabling "Reserve Channel" and selecting the reserved channel from the drop down menu.

If the call type is defined as analog, a modem enabled for callback will also be required. If no modem is available, the dial out will not occur.

If "Enable Multilink PPP" is enabled, the 833IS will use two channels to connect to the dial out router. Enter the phone number for the second channel in the "Secondary Phone Number" field.

Callback should not be used to have the 833IS call the dial in router. If callback is used, the router will be treated as a standard dialup client. Routing information will not be exchanged, and the LAN to LAN connection timers will not be used. Always use the dial out parameters reserved for the LAN to LAN function.

Lan To Lan Configuration

The following list of parameters are used for Lan To Lan connections.

The screenshot shows the 'Add User' dialog box with the 'Lan To Lan' tab selected. The 'Remote System Login' section includes fields for 'Login ID', 'Password', and 'Confirm', along with a 'RIP Setup' button. The 'Phone Numbers' section has a checkbox for 'Enable Multilink PPP', radio buttons for 'Call Type' (Digital and Analog), and fields for 'Primary Phone Number' and 'Secondary Phone Number', each with a 'Reserve Channel' dropdown menu. The 'Connection' section has a checkbox for 'Enable Auto Connect' and a 'Virtual Connection' button. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

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 833IS 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.

Phone Numbers

Enable Multilink PPP

The 833IS 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 833IS 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.

Reserve Channel

When the Reserve Channel is enable, a user can be assigned a specific channel. Available channels will be listed in the drop down list and one may be selected for the particular user.

Connection

Enable Auto Connect

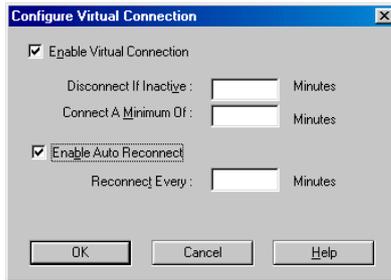
When this option is selected, the 833IS maintains a permanent connection to the remote server. The 833IS initiates this connection at bootup and will automatically retry if the link goes down. The Inactivity Time Out and the Maximum Connect Time parameters are disabled when Auto Connect is active.

Configure 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 **Configure Virtual Connection** screen is as follows:



Enable Virtual Connection

When enabled, the 833IS 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 833IS will simulate the RIPs, SAPs, and watchdog messages when the virtual connection is enabled.

Disconnect If Inactive

This specifies the longest continuous time interval of inactivity (except for RIP, SAP and IPX Type 20 packet exchange) allowed before the virtual link is brought down.

Connect a minimum of

This specifies the shortest continuous time interval in seconds 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.

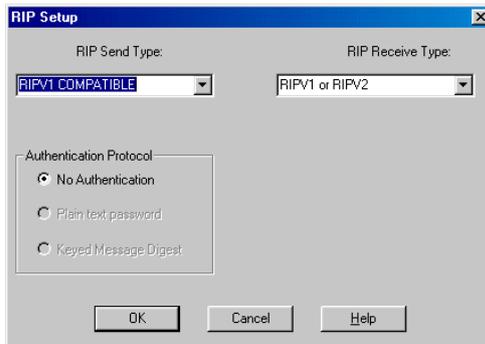
Enable Auto Reconnect

When checked, this allows the 833IS to re-establish the virtual connection after a specified period of time defined by the Reconnect Every field.

Reconnect Every

This field specifies the maximum downtime allowed on a link before the link is re-established. This option is used to periodically 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 WAN 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 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

Standard Profile

From the **User Main** screen, click on **Standard Profile**.

The Standard Profile screen appears. Fields are as follows:

Inactivity Timeout

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 timeout, 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 Callbacks

For a complete discussion on callback, See “User Callback” on page 145.

Enable Roaming Callback

When checked, this option will enable **Roaming Callback**. If a client asks for roaming callback during connect, the 833IS will callback with the number supplied by the client. If a client does not request roaming callback, the session will be established as if roaming callback was not checked.

If this option is not checked, any roaming callback requests will be rejected at connect time. Client behavior will be dependent on the client – the client may either continue the session without callback, or end the session.

Preferred Callback Group

By default, a callback will be made on the next available line that has been enabled for callback. If you wish to allocate a specific group of channels for callback, select the group in the drop box. The callback group must have been previously defined. See “User Callback” on page 145.

If you check **Use Exclusively**, the callback will occur only if there is a free channel available in the selected group. If **Use Exclusively** is not checked, the callback will use another channel enabled for callback if a channel from the preferred group is not available.

Client Virtual Connection

Click on this box to enable a client virtual connection.

This feature is used by remote Dial-in clients to save packet charges. The client drops the physical link to the 833IS 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.

This feature is can be used by remote IP or IPX dial in clients to save on connection charges. With client virtual connect enabled, the client can drop the physical connection, but the 833IS will keep the session active. The client can then reconnect and the 833IS will reassign the same session, and client IP address.

The Inactivity Timeout and Connection timers affect the virtual connection in the following manner:

- **Inactivity Timeout**

If there is no data transfer on the link for the duration set in this timer, the client session drops and the physical connection drops. Time in the virtual connection state is included. If "disabled" is set for inactivity timeout, the session will be released after 10 minutes in the virtual state. This is to prevent an unused session from being tied up permanently.

- **Connect Time**

The client will be disconnected and the session will be dropped after the time limit set in this timer, regardless of activity. Time in the virtual connection state is included.

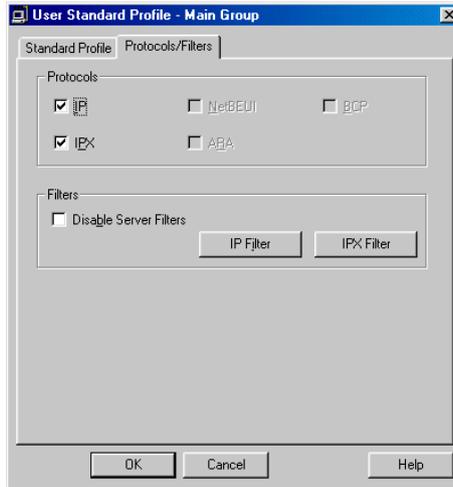
If you are using Radius as your authentication server, you can configure the Radius server to set the Inactivity Timeout and Connect Time.

To be effective, the dial in client should support virtual connect. It should have a mode that:

- Drops the physical connection if inactive, but not notify the application of disconnect
- Automatically reconnects if data is to be sent

Reconnect to the 833IS is driven solely by the client in this mode. The 833IS cannot redial the client. In practice this is not a real limitation, as servers will typically only send data in response to a request from the client. However, if you are using a client application that supports unsolicited data from a server, you can configure the LAN to LAN feature for use with a dial in client.

Protocols The **User Standard Profile - Protocols/Filters** screen is as follows:



Disable any **Protocols** that the user should not have access to by removing the check in the check box. If the server has any protocols disabled, then that protocol will show as disabled for the User.

Filters For a discussion on protocol filters and how to define them, see “IP Filter” on page 109.

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.

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 113.

IPX Filter Assignment

To assign an IPX filter, click on **IPX Filter**. The **IPX User Filter Assignment** window appears.



For instructions on how to assign IPX filters, see “Filter Assignment” on page 125.

Shared User Database

The Shared User Database feature allows the Perle 833IS to access the User Database of specified remote Perle 833IS servers on the LAN. Two Remote Servers can be defined for the local server. When a user connects to the Perle 833IS, 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 833IS 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

Set the check box of the **Search Remote** field to enable the Perle 833IS 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.

Standard Profile

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
- Logging

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
- Logging

For most installations, parameters in this section do not have to be configured for the 833IS 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 833IS supports a number of different types of user authentication security. If you are using the password security provided in the Internal 833IS 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.

Configuring the Server

If you will be using an SNMP Manager such as HP OpenView to monitor the 833IS, you will need to set the SNMP parameters.

If you will be using a Sys Log Server to receive the 833IS event log information then you will need to up the syslog parameters.

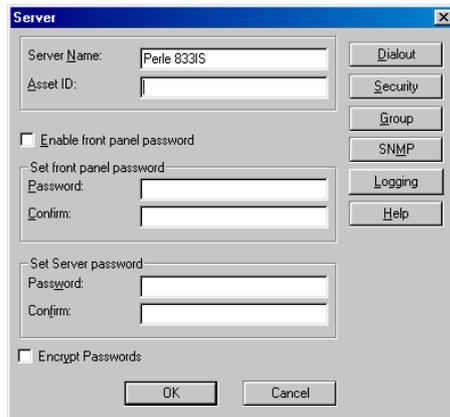
Configuring the Server

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 **Server**.

The **Server** main screen appears. Fields are as follows:



The screenshot shows a dialog box titled "Server" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Server Name:** A text field containing "Perle 833IS".
- Asset ID:** An empty text field.
- Enable front panel password:** A checkbox that is currently unchecked.
- Set front panel password:** A section with "Password:" and "Confirm:" text fields, both empty.
- Set Server password:** A section with "Password:" and "Confirm:" text fields, both empty.
- Encrypt Passwords:** A checkbox that is currently unchecked.

On the right side of the dialog, there is a vertical stack of buttons: "Dialout", "Security", "Group", "SNMP", "Logging", and "Help". At the bottom of the dialog are "OK" and "Cancel" buttons.

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 833IS.

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 833IS.

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.

Set Server Password

The Server Password provides an additional layer of security for users accessing the server via the manager or telnet. Maximum length is 32 characters. Enter the password in both the password and confirm fields.



If the server password is defined on the server then the Server Password field as well as the User ID and User Password field will have to be entered on the Manager Login screen in order to gain access to that server.

If the server password is defined on the server then a user accessing the server with this password does not have to have administration privileges to gain full access to the server.



Both Front Panel Password and Server Password are encrypted when stored in the configuration file.

Encrypt Passwords

When checked, all defined user passwords will be encrypted when stored in the configuration file. The default is not to encrypt user passwords.

Dial-Out

To access the Dial-Out settings, click this button. See page 166.

Security

To access the Security settings, click this button. See page 169.

Dial-Out

Group

To access the Group settings, click this button. See page 182.

SNMP

To access the SNMP settings, click this button. See page 189.

Logging

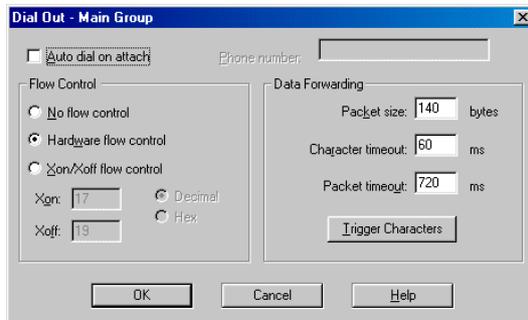
To access the syslog and internal logging settings click this button. See page 192.

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:



Auto Dial On Attach

When checked, the 833IS 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 internal flow of data between the 833IS software and the modem. The 833IS 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 833IS will ignore any flow control indication from the modem.

Hardware Flow control

When set, the 833IS will use hardware flow control with the modem.

Xon/Xoff Flow Control

Also known as software flow control. When set, the 833IS 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 833IS 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 833IS 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 Timeout

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 Timeout**.

This number can be decreased to improve the response at the client. It can be increased to reduce the frequency of network transmissions.

Packet Timeout

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 **Timeout** in milliseconds. The default value is 720 milliseconds, with a maximum value of 65535 milliseconds.

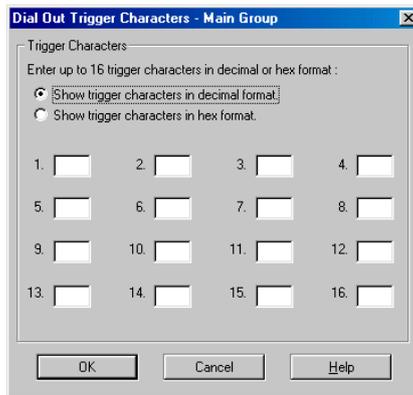
Reducing this value may improve the response of the client if the typical data transmission is smaller than a packet.

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.



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 setting the display to 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 833IS.
- Control who can access your network resources such as file servers.
- Control who can configure and manage the 833IS.

The 833IS has facilities for controlling all the above.

Overview

User Authentication

When a user dials in, the 833IS 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 833IS Internal User database, or an external database such as Novell Bindery or RADIUS.
- *Using a token authentication scheme* such as Security Dynamics SecurID or Acent. 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 833IS 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.

Callback

You can enable the Fixed Callback feature of the 833IS to enhance security. With Fixed Callback, the user record contains a phone number to be used for callback. Once the user is authenticated, the call is dropped. The 833IS then calls back using

the number stored in the User database. Only if the user is at that phone number will access be permitted.

Callback is detailed in “User Callback” on page 145.

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 833IS does not control LAN security, in some cases you can restrict which networks and servers are available to the 833IS.

Administration Privileges

To manage the 833IS, a user must have Administration privileges set in their user record in the 833IS Internal database. If you are using RADIUS, you must set the “Administrative” (value=6) or the “Administrative and Callback” (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 139.

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 165). 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 833IS 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 833IS, you can explicitly specify which IPX servers and networks can be accessed. See “Static Route” on page 117.

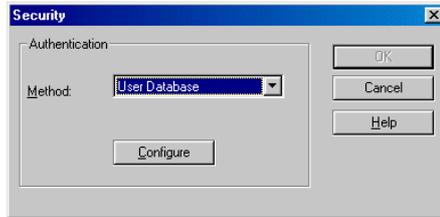
You can use the IP Static Routing Table feature to restrict which IP networks and hosts that remote users can access. See “Static Routes” on page 106. Note that if you specify an IP Default Gateway in the configuration, the 833IS will attempt to use it to route to any addresses not specified in the Static Routing Table.

Configuring User Authentication Security

To access the Security Screen:



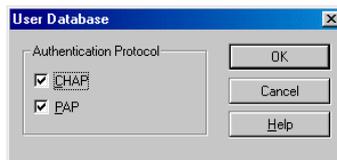
1. From the Configuration File screen, click on **Server**.
2. From the Server Screen, click on **Security**. The Security main screen will appear.



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 833IS User database. This database could be configured on the Local 833IS or on a remote 833IS. When the remote Client connects, it communicates with the 833IS 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:



Authentication Protocol

Click on the check box to enable CHAP or PAP authentication protocols. If both are checked, the 833IS will first attempt to authenticate using CHAP. If CHAP is not supported by the client, the 833IS will then use PAP.

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.



833IS Bindery support can also be used with Novell Directory Service (NDS) to control password access to the 833IS. 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 833IS does not support native NDS messages.

The 833IS can use the Bindery to control password access to the 833IS. On the Bindery server, a group is created containing all users that can access the 833IS. When the remote Client connects, it will communicate with the 833IS 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 833IS will grant access.

Users will be given the privileges granted in the Standard User Profile. See “Standard Profile” on page 155. However, you can add a user record to the Internal 833IS 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:

A screenshot of a Windows-style dialog box titled "Netware Bindery". It contains two text input fields: "Server Name:" and "Novell Group Name:". To the right of the input fields are three buttons: "OK", "Cancel", and "Help". The dialog box has a standard title bar with a close button (X) in the top right corner.

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 833IS using the CHAP or PAP protocol. Regardless of the protocol used to exchange the password information with the client, the 833IS 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 833IS. If any additional parameters were specified for the user on the RADIUS server, they will be forwarded to the 833IS at this time.

If RADIUS authentication has been configured on the 833IS, all users who attempt to gain access to the 833IS 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 833IS user database to define attributes not supported within RADIUS. The user ID field must match the user ID 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 833IS.
2. The 833IS will forward the user name and password to the RADIUS authentication server. If necessary, the password is first encrypted by the 833IS.
3. The RADIUS authentication server indicates to the 833IS if the user is authenticated. If authentication is rejected, the 833IS will notify the user.
4. If the user is authenticated, the 833IS 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 833IS. This server will be used if the main authentication server is not available.

A RADIUS accounting server can be optionally configured on the 833IS. 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 833IS. 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.

In order to provide Radius with full authentication authority over the 833IS unit, the local database will no longer be used to authenticate "administration" users (users who are authorized to manage the 833IS) when the 833IS is communicating with either a primary or backup Radius server. Customers using Radius as the authentication method will need to ensure that they have configured a user with "administrator" capabilities on their Radius server (Service-Type = Administrative).

In previous releases, a user record in the local data base was used for this purpose. Now, a record in the local database will only be used if the 833IS cannot communicate with a Radius Server. Do not put a record in the local database if you want to ensure that Radius authentication is used under all conditions for administration.

It is recommended that a local database record is used during initial setup to prevent being locked out because of a misconfigured Radius setup.

The RADIUS configuration screen contains the following:

The screenshot shows a window titled "Radius Servers" with a tabbed interface. The "Primary Authentication" tab is active. The fields are as follows:

- IP Address: [. . .]
- UDP Port: [1645]
- Secret: []
- Timeout value: [5] seconds
- Number of retries: [3]
- Authentication Protocol:
 - CHAP
 - PAP
- Host retry: [0] minutes

Buttons at the bottom: [OK] [Cancel] [Help]

Authentication server

Click on the **Primary Authentication** tab to configure the main RADIUS authentication server. Click on the **Backup Authentication** tab to configure the backup RADIUS authentication server.

Accounting server

Click on the **Primary Accounting** tab to configure the main RADIUS accounting server. Click on the **Backup Accounting** tab to configure the backup RADIUS accounting server.

Host Retry

The length of time in minutes after which the 833IS should retry a RADIUS host which had previously become unreachable. At the expiration of this retry time, the 833IS 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 833IS 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 833IS and the RADIUS server. Click on the check box to enable CHAP or PAP authentication protocols. If both are checked, the 833IS 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.

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 833IS and the RADIUS server to encrypt the data. This key must match the key configured on the RADIUS server.

Timeout Value

The length of time in seconds for the 833IS to wait for a reply from the RADIUS server. The default is 3 seconds.

Number of Retries

The number of times the 833IS 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 833IS, 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 833IS will ask the Axent server to start the authentication process. The 833IS 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 “Standard Profile” on page 155. However, you can add a user record to the Internal 833IS 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

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 833IS. 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 833IS as a valid Axent agent.

Confirm Agent Key

Re-enter the **Agent Key** in this field for confirmation.

Configuring User Authentication Security

Agent ID

Enter the **Agent ID** for the 833IS. 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 833IS 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 833IS 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 833IS will ask the ACE/Server to start the authentication process. The 833IS 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 “Standard Profile” on page 155. However, you can add a user record to the Internal 833IS 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

The IP address of the Master SecurID server.

Configuring User Authentication Security

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 833IS 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 833IS server by the SecurID server the first time the 833IS sends an authorization request. The Node Secret is used to encrypt the data that is sent between the 833IS and the SecurID Server.

Do not check this box unless there is a mismatch between the node secret in the 833IS and the SecurID server and you must reset the Node Secret to blank. This would occur if a 833IS is moved to another network with a new SecurID server.

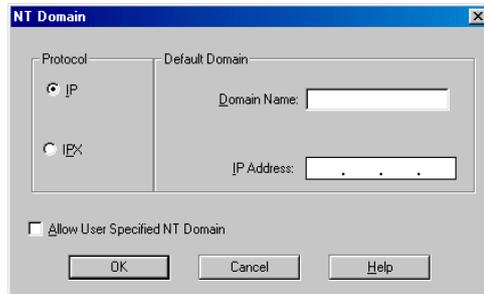
If the Node Secret is reset, or the 833IS is reset to factory defaults, then the SecurID server must be configured to resend the Node Secret to the 833IS.

NT Domain

NT Domain enables the Perle 833IS to use a Windows NT's domain user database for dial-in user authentication. The Perle 833IS 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 "Standard Profile" on page 155. However, you can add a user record to the Internal 833IS 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 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 833IS.

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 833IS 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 833IS 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 833IS 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 callback. (Note that by default Dial-In, Dial-Out and callback are enabled, but any of these functions can be disabled in the ISDN BRI Interface configuration screen).

When a Dial-In call comes in, the 833IS 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 186.

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 833IS 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 833IS 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.

Callback

The Callback group is determined by an entry in the user record. A channel and modem assigned to the group will be used when callback is required. There are no optional group settings for Callback.

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 Callback.

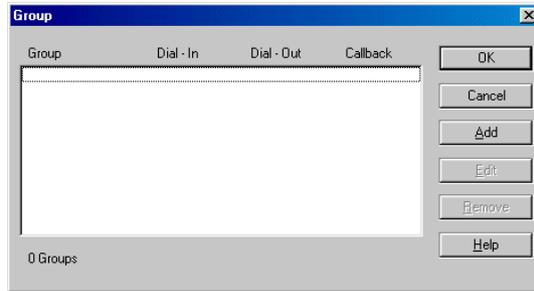
If a group is enabled for multiple modes, it will behave...

- 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 Callback group if callback is required.

...if Dial-In, Dial-Out, and callback 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 callback. 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.

Callback

Displays whether this group is enabled for callback.

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:

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.
- Callback.

The enable group settings override the settings for any channels and modems explicitly included in the group.

Lines 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 callback, the channel attributes that were defined in the ISDN BRI Line configuration will be used. For example, if a

channel is required for Dial-Out for this group, the 833IS 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 ISDN BRI Interface 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 callback, 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 833IS 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.

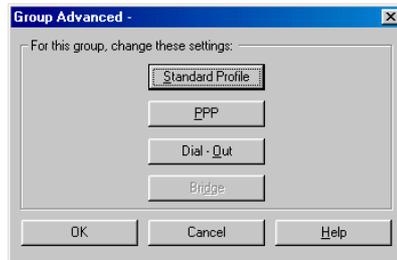
Advanced

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.



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

The 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.

The parameters for the User Standard Profile - Group setting are the same as the main Standard Profile setting. For details on these settings see “Configuring the Standard Profile” on page 155.

PPP - Group

The 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 129.

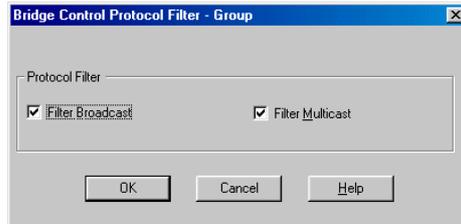
Dial-Out - Group

The 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 166.

Bridge Filter - Group

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 89.

Fields are as follows:



Filter Broadcast

When checked, the 833IS will not pass any broadcast messages received from the LAN to the WAN client.

Filter Multicast

When checked, the 833IS 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 833IS 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 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 833IS Agent supports read access of the SNMP information only. Configuration and control is performed via the 833IS Manager.

The 833IS can be controlled by an SNMP Manager that has dialed in to the 833IS.



SNMP Configuration

The **SNMP Configuration** screen is used to set parameters related to SNMP. Fields are as follows:

The screenshot shows the 'SNMP Configuration' dialog box. It includes the following elements:

- Name:** A text input field.
- Contact:** A text input field.
- Location:** A text input field.
- Trap Host:** A section containing:
 - Enabled
 - IP Address: A field with four vertical dividers.
 - Community: A dropdown menu currently showing 'public'.
- Community:** A table with two columns: 'Name' and 'Access'.

Name	Access
public	Read

 To the right of the table are three buttons: 'Add...', 'Edit...', and 'Remove'.
- Buttons:** 'OK', 'Cancel', and 'Help' are located at the bottom of the dialog.

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 833IS. Maximum length is 255 characters.

Location

Enter a description of the physical location of the 833IS.

Trap Host

When the SNMP Agent in the 833IS 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 833IS 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 833IS 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 833IS 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 833IS 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.

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.

Logging Configuration

The 833IS can be configured to direct Event Log messages to either an internal Event Log or a Syslog server.

Syslog

The 833IS can send Event Log messages in real time to a Syslog server. Messages sent to Syslog are assigned an error level that indicates the severity of the condition.

Some of the benefits of using the Syslog feature are the following:

- One Syslog Server can be used for the retrieval and storage of Syslog messages from multiple 833IS Servers and other devices that support Syslog in your network.
- Syslog Servers can store a large number of Syslog messages.
- You can display the received Syslog messages based on time, hostname or order received.

The **Logging-Syslog** screen is as follows:



Enable Syslog

Click on the box to enable the sending of Event Log messages to the configured Syslog Servers.

Syslog Servers

IP Address 1 - 4

Enter the IP address of the Syslog Servers that will receive the logging messages.

Error Level

Event Log Messages are assigned an error level (0 - 7), that indicates the severity of the event.

The levels are as follows:

- 0: Emergencies - System unusable
- 1: Alerts - Immediate action needed
- 2: Critical
- 3: Errors
- 4: Warnings
- 5: Notifications - Normal but significant condition
- 6: Informational - Informational messages only

7: Debugging - For Perle use only



Selecting a certain error level will cause all events of that Error Level and all events with an error level lower than the one selected to be sent to the Syslog Server.

Event Log

The **Logging - Event Log** screen is as follows:



Enable Event Log

Click on the box to enable the storing of Event Log messages to an internal Event Log in NVRAM.

This Event Log is circular in nature, so newer messages overwrite older messages after the Event Log is filled.

Error Level

The error levels are as follows:

- 0: Emergencies - System unusable
- 1: Alerts - Immediate action needed
- 2: Critical
- 3: Errors
- 4: Warnings
- 5: Notifications - Normal but significant condition

6: Informational - Informational messages only

7: Debugging - For Perle use only

Section 3: Management

Chapter 10: Managing the Perle 833IS

Appendix 1: Menu Descriptions and Maps

Appendix 2: AT Command Set

Appendix 3: Specifications

Appendix 4: RADIUS Server Attributes

Appendix 5: Cisco Mode Reference Guide

Chapter 10: Managing the Perle 833IS

About Managing the Perle 833IS

This chapter provides information related to managing the 833IS. You will read about:

- 833IS Manager Statistics
- 833IS Syslog
- 833IS Front Panel
- 833IS Event Log

All 833IS Statistics are also available via a Telnet connection. For details, please refer to the “Appendix 5: Cisco Configuration Mode.

833IS Manager Statistics

Built into your 833IS Manager is a facility that provides information about the:

- Operational status of the interfaces in the unit.
- Number of LAN transmission and receive errors encountered.
- Networks and Servers that can be reached by the 833IS on an IPX connection.
- Status of current calls, and what modems and lines are used by those calls.

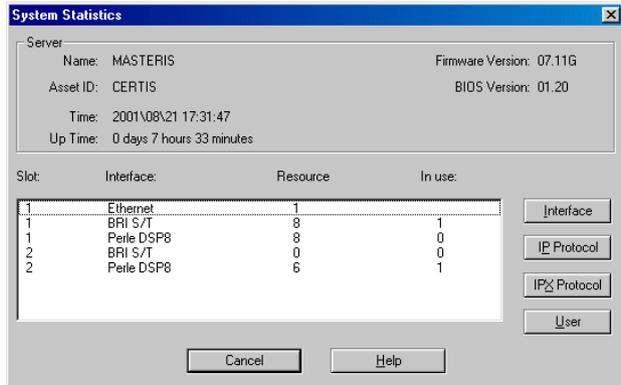
Viewing Statistics

To view the statistics of an 833IS, connect to the server and choose **Get Statistics** from the Statistics menu. Please See “Connecting to the Server” on page 47 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 an interface or protocol.

Server Information

The following general information about the Server is displayed:



Name

Name of this 833IS as defined in the Server configuration.

Asset ID

Asset ID of this 833IS as defined in the Server configuration.

Time

The current time as set within this 833IS.

Up time

Time elapsed since the 833IS was last started or reset.

Firmware Version

Version number of the 833IS operating Firmware.

BIOS version

Version number of the 833IS BIOS.

Interface Display

The interface display provides basic information about each interface installed in the 833IS. The following information is displayed for each interface:

Slot

Slot number of the interface.

Interface

Type of interface installed in the slot. Valid interface types are:

- Ethernet
- Token Ring
- ISDN BRI U
- ISDN BRI S/T
- Perle DSP8

Resources

The total number of resources available for this interface. A resource is a general term for the number of enabled modems or channels available on an interface. 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 interface that are currently in use.

Interface

Click on this button to access the **Statistics** for this interface.

IP Protocol

Click on this button to access the **IP Protocol Statistics**.

IPX Protocol

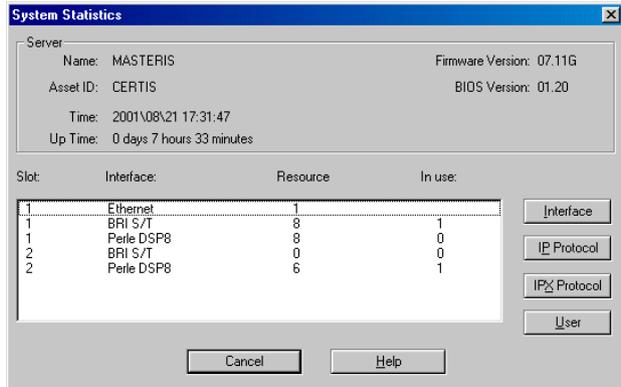
Click on this button to access the **IPX Protocol Statistics**.

Accessing Interface Statistics

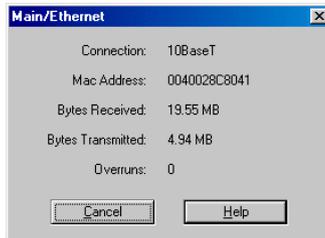


To access the statistics for an interface:

1. Bring up the main **System Statistics** screen.
2. Highlight the interface you are interested in, and click on the **Interface** button. The next screen displayed will be based on the interface selected.



Ethernet Interface



Connection

The physical connection used for the Ethernet on the 833IS.

MAC Address

The MAC address configured for this Ethernet connection.

Bytes Received

The total number of bytes received by this Ethernet connection for the 833IS since last start or reset.

Bytes Transmitted

The total number of bytes transmitted by the 833IS 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
Interface**
**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 833IS since last start or reset.

Bytes Transmitted

The total number of bytes transmitted by the 833IS 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.

ISDN BRI Line Interface

The statistics screen displayed is identical for both the BRI U and the BRI S/T interfaces.

BRI:	Interface status:	In Discards:	In Errors:	In Unknown Protocols:	Out Discards:	Out Errors:
1	Connected	0	0	0	2	0
2	Connected	0	0	0	0	0
3	Disconnected	0	0	0	0	0
4	Connected	0	0	0	0	0

Channel:	Mode:	Status:	Type:	Assigned:
IS101	DD	Idle	Idle	
IS102	DD	Idle	Idle	
IS103	DIVCB	Active	ISDN Digital	
IS104	DIVCB	Idle	Idle	
IS105	DI	Idle	Idle	
IS106	DI	Idle	Idle	
IS107	DIVCB	Idle	Idle	

Call Status: IS103	
User:	lyn
Department:	IP Address:
Group:	IPX Address: 83735E6
Bytes RX: 19.58 KB	MAC Address: 021212121200
Bytes TX: 38.67 KB	Time connected (hh:mm): 00:47

BRI

Indicates the interface number.

Interface Status

Status of the physical layer. The possible values for this field are connected or disconnected.

In Discards

The total number of received frames which have been discarded. The possible reasons are: buffer shortage.

In Errors

The number of inbound frames that contained errors preventing them from being deliverable to LAPD.

In Unknown Protocols

The number of frames with known TEI, but unknown SAPI (Service Access Point Identifier).

Out Discards

The total number of outbound frames which were discarded. Possible reasons are: buffer shortage.

Out Errors

The number of frames which could not be transmitted due to errors.

Channel

Indicates the interface number and channel number. For each channel, the following information is displayed:

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 - Callback.
- Disabled.

If the channel is in use, the valid modes are:

- Dial-In.
- Dial-Out.
- Callback.

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
- 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 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 833IS. 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.

Incoming Complete

Number of successful incoming attempts for this modem since system reset. The count is incremented when the modem has completed the training sequence successfully and has indicated to the 833IS that the carrier is active.

Fail

Number of unsuccessful incoming attempts for this modem since system 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 system reset.

Bytes TX

Number of bytes transmitted by this modem since system reset.

Retrains

Number of retrains experienced on connections with this modem since system 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 833IS. 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

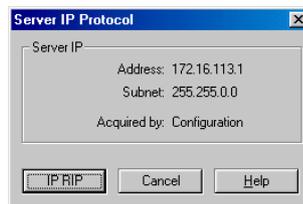
The number of bytes received on this modem during the current call.

Bytes TX

The number of bytes transmitted on this modem during the current call.

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:



833IS Manager Statistics

Address

The IP address of the Server.

Subnet

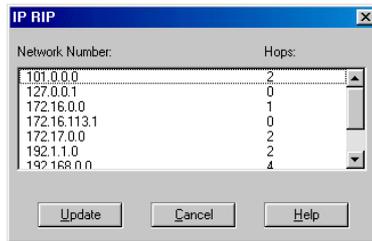
The subnet of the Server.

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 833IS.

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.



The screenshot shows a window titled "IP RIP" with a table containing the following data:

Network Number:	Hops:
101.0.0.0	2
127.0.0.1	0
172.16.0.0	1
172.16.113.1	0
172.17.0.0	2
192.1.1.0	2
192.168.0.0	4

At the bottom of the window are three buttons: "Update", "Cancel", and "Help".

Fields are as follows:

Network Number

The network number of the network that can be accessed.

Hops

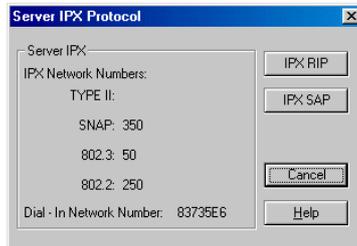
The number of routers that are between this network and the network that the 833IS is on.

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



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.

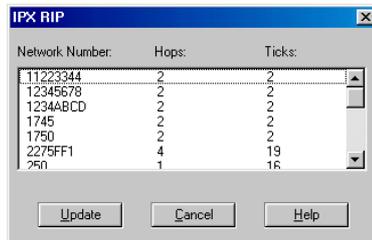
802.3

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:
11223344	2	2
12345678	2	2
1234ABCD	2	2
1745	2	2
1750	2	2
2275FF1	4	19
25n	1	16

Update Cancel Help

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 833IS is on.

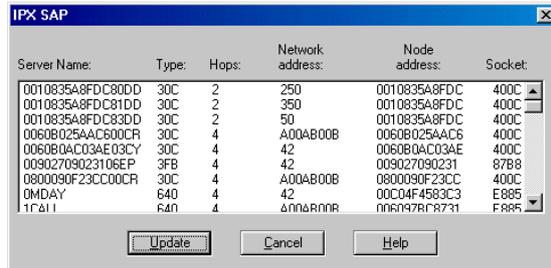
Ticks

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:
0010835A8FDC80DD	30C	2	250	0010835A8FDC	400C
0010835A8FDC81DD	30C	2	350	0010835A8FDC	400C
0010835A8FDC83DD	30C	2	50	0010835A8FDC	400C
00608025AAC600CR	30C	4	A00AB00B	00608025AAC6	400C
006080AC03AE03CY	30C	4	42	006080AC03AE	400C
00902709023106EP	3FB	4	42	009027090231	87B8
0800090F23CC00CR	30C	4	A00AB00B	0800090F23CC	400C
0MDAY	640	4	42	00C04F4583C3	E885
17ALL	640	4	800&R00R	006097B8731	F885

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 833IS server uses the number “26h” as its server type.

Hops

The number of routers that are between this Server and the network that the 833IS is on.

Network Address

The network address of this Server.

Node Address

The node address of this Server.

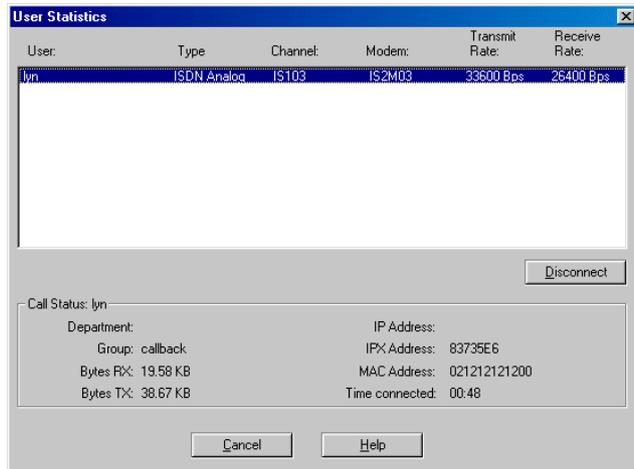
Socket

The IPX socket number that is used to communicate with this Server.

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 833IS. 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.

Disconnect User

Select a user with your mouse and click on the Disconnect button. This user will be disconnected from the 833IS.

Event Log

The 833IS has a non-volatile Event Log that is used to track key activities in the 833IS. This user log can be uploaded to the 833IS 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 restarts
- Internal 833IS errors

To access the Event Log, the 833IS Manager must connect to an 833IS 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 833IS 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 change the filtering of the type of events recorded by the 833IS.

These changes take effect immediately but are not maintained if the 833IS is powered off. For details on configuring Event Log Filters see page 194.

Clear Event Log

This will clear all the log data from the connected 833IS.

PPP Debug

This popup menu displays the following PPP Debug options. Enabling any of the following options, displays PPP level information in the Event Log for each dial-in connection.



Authentication

Displays all PPP authentication packets in the Event Log

Negotiation

Displays PPP packets that are transmitted and received during PPP startup (i.e. LCP and NCP options) in the Event Log.

MP

Displays Multilink PPP protocol messages in the Event Log.

CBCP

Displays Callback (CBCP) protocol message in the Event Log.

Packet

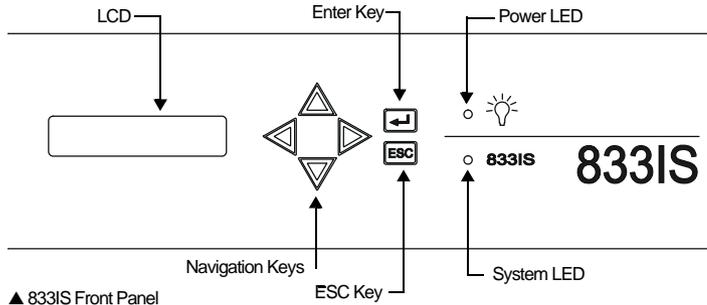
Displays in the Event Log all PPP packets being transmitted and received

Error

Displays protocol errors and error statistics associated with PPP connection negotiation and operation in the Event Log.

833IS Front Panel

The Front Panel consists of a keypad and LCD display at the front of the 833IS. It is used for the initial setup of the 833IS and monitoring the operational status.



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 833IS is powered up.

System LED

Blinks continuously when the 833IS is operational.

Front Panel Modes

The Front Panel operates in two different modes, Factory Default and Normal.

If the 833IS 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 833IS Manager.

Once the 833IS has been fully configured, the Front Panel is in Normal mode. In this mode, many of the statistics that are available from the 833IS Manager can be displayed on the Front Panel. You also have access to these control functions:

- Reset the entire 833IS.
- Reset the 833IS to Factory Default mode.
- Set the IP and IPX address of the 833IS.

These control functions can be password protected to prevent unauthorized access.

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.

833IS Front Panel

Enter Key

Accept changes and exit edit mode.

ESC Key

Discard changes and exit edit mode.

Appendix 1: Menu Descriptions and Maps

About Menu Descriptions and Maps

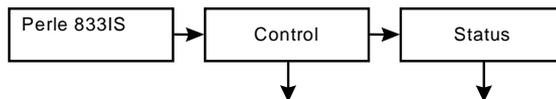
In this chapter you will read about:

- Front Panel Main Screen
- Control
- Status
- Card Status
- 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 224.

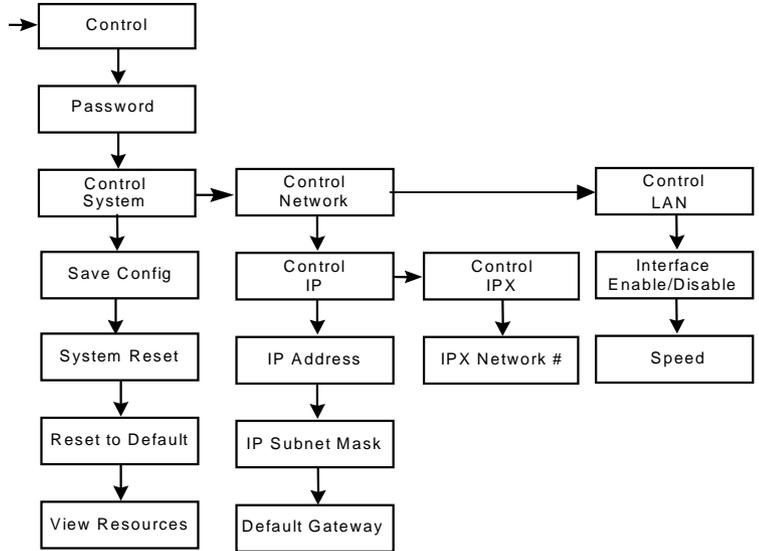
Status Menu Descriptions on page 226.

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.
Save Config	Saves your current configuration to NVRAM.
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.
Network	Network Control Displays.
IP	Select IP Settings.
IP Address	Set IP address of unit.
IP Subnet Mask	Set IP Subnet Mask of unit.
Default Gateway	Set address of Default Gateway.
IPX	Select IPX Settings.
IPX Network Number	Set WAN (internal) Network Number.
LAN	
Interface Enable/Disable	Select Enable or Disable to enable or disable your LAN connection.
Speed	Set your LAN speed. Select Auto Detect, 10 Mb or 100 Mb for Ethernet. Select 4 Mb or 16 Mb for Token Ring LAN.

Control Menu Map

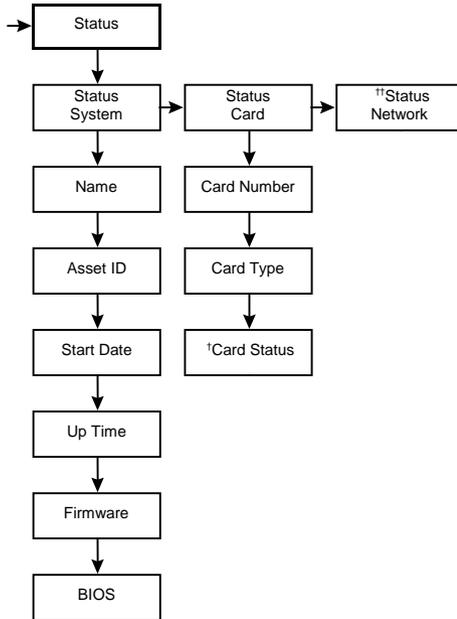


Status

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.
System	System 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.
Card Number	Select which card number to view.
Card Type	Indicates Card Type selected card number.
Card Status	Indicates the start of Card Status displays. Card Status is organized into LAN, Line, and Modem displays.
Network	Indicates the start of Network Status displays. Network Status is organized into IP, IPX, BCP, NetBEUI, and ARA displays.

Status Menu Map



†Card Status descriptions on page 228.

††Network Status descriptions on page 232.

Card Status

Status specific to each card type is detailed below.

Menu	Description
Card Status	
LAN Status	
LAN Type	Indicates whether the unit is configured for Ethernet or Token Ring.
Connection	Indicates if the card is connected to the Ethernet network.
MAC Address	MAC address of Ethernet card.
Port	Indicates one of the following ports, if the card is connected to the Ethernet network. This panel is only displayed for versions of the 833IS with a BNC Ethernet interface in addition to the RJ-45 interface. <ul style="list-style-type: none"> ■ RJ-45 ■ BNC
Speed	Indicates one of the following speeds, if the card is connected to the Ethernet network: <ul style="list-style-type: none"> ■ 10 Mbps ■ 100 Mbps or Indicates one of the following speeds, if the card is connected to the Token Ring network: <ul style="list-style-type: none"> ■ 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 229.

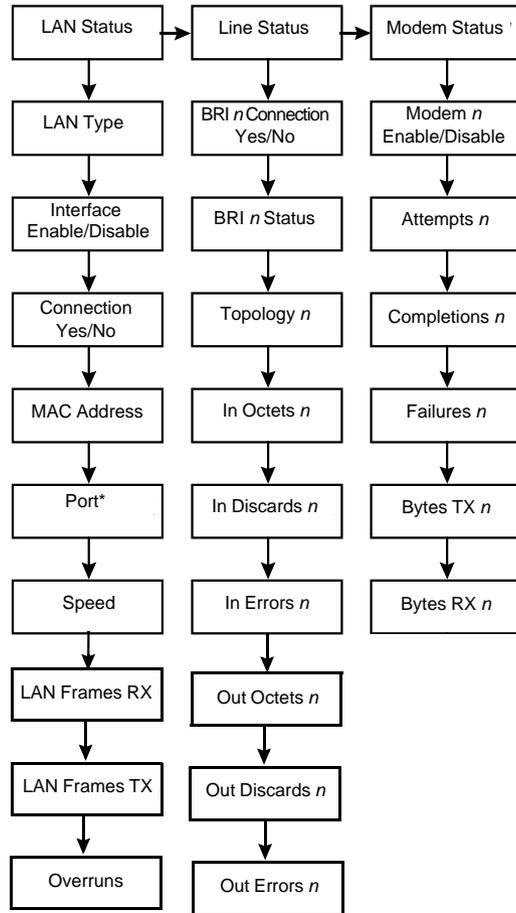
Card Status continued

Menu	Description
Line Status	Statuses are available for each BRI interface on the card. Use right and left arrow for each BRI interface selection.
BRI <i>n</i> Connection Yes/No	Indicates whether the BRI interface is connected to the telephone network or not.
BRI <i>n</i> Status	Indicates status of each B channel. Channel number followed by an Up or Down arrow or X for disabled (eg. 1 ↑ 2X).
Topology <i>n</i>	Indicates one of the following line topology for each BRI interface: <ul style="list-style-type: none"> ■ Point to point ■ Point to multipoint
In Octets <i>n</i>	Indicates the total number of octets received on this interface.
In Discards <i>n</i>	Indicates the total number of received frames which have been discarded. The possible reasons are: buffer shortage.
In Errors <i>n</i>	Indicates the number of inbound frames that contained errors preventing them from being deliverable to LAPD (D channel data link layer).
Out Octets <i>n</i>	Indicates the total number of octets transmitted on this interface.
Out Discards <i>n</i>	Indicates the total number of outbound frames which were discarded. Possible reasons are: buffer shortage.
Out Errors <i>n</i>	Indicates the number of frames which could not be transmitted due to errors.

Card Status continued

Menu	Description
Modem Status	Statuses are available for each modem on the card. Use right and left arrow for each modem selection.
Modem <i>n</i> Enabled/Disabled	Indicates whether the modem is enabled or disabled via configuration. The left and right keys will select the modem for the following: (<i>n</i> = the modem chosen)
Attempts <i>n</i>	Number of incoming call attempts for this modem since card Start-up.
Completions <i>n</i>	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 <i>n</i>	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).
Bytes Tx <i>n</i>	Number of bytes presented to the modem since Start-up.
Bytes Rx <i>n</i>	Number of bytes received from this modem since Start-up

Card Status Menu Map



* Display only when the unit includes both a BNC and RJ-45 Ethernet interface.

Network Status Display

Menu	Description
IP	
IP Enable/Disable	Indicates whether the IP is enabled or disabled.
IP Address	IP address of the 833IS.
IP Subnet Mask	IP subnet mask of the 833IS.
Address found by	Indicates how the IP address was determined: <ul style="list-style-type: none"> ■ BOOTP ■ RARP ■ Configured
RARP	Indicates whether RARP will be sent at startup to attempt to acquire the 833IS IP address.
BOOTP	Indicates whether a BOOTP request will be sent at startup to attempt to acquire the 833IS IP address.
# RIP entries	Current number of IP RIP entries.
IPX	
IPX Enable/Disable	Indicates whether the IPX is enabled or disabled.
IPX Type II By:	Indicates how the Network Number for Type II IPX frames was determined: <ul style="list-style-type: none"> ■ Automatically from network. ■ Configured ■ None (Type II disabled)
IPX Type II #	Type II IPX frame network number.
IPX SNAP by:	Indicates how the Network Number for SNAP IPX frames was determined: <ul style="list-style-type: none"> ■ Automatically from Network. ■ Configured ■ None (SNAP disabled)
IPX SNAP #	SNAP IPX frame network number.

Menu	Description
IPX 802.2 by:	Indicates how the Network Number for the 802.2 IPX frames was determined: <ul style="list-style-type: none"> ■ Automatically from Network. ■ Configured ■ None (802.2 disabled)
IPX 802.2 #	802.2 IPX frame network number.
IPX 802.3 by:	Indicates how the Network Number for the 802.3 IPX frames was determined: <ul style="list-style-type: none"> ■ 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.
BCP	
BCP Enable/Disable	Indicates whether the BCP is enabled or disabled.
NetBEUI	
NetBEUI Enable/Disable	Indicates whether the NetBEUI is enabled or disabled.
ARA	
ARA Enable/Disable	Indicates whether the ARA is enabled or disabled.

Factory Default Mode

Menu	Description
Perle 833IS	Appears for 5 seconds on power up.
Manager Status	Indicates whether the Perle 833IS Manager is communicating with the server and which protocol is used for communication. If the 833IS receives an IP ping command in Factory Default mode, this message will display, with the address of the device that sent the ping command.

Factory Default Setup

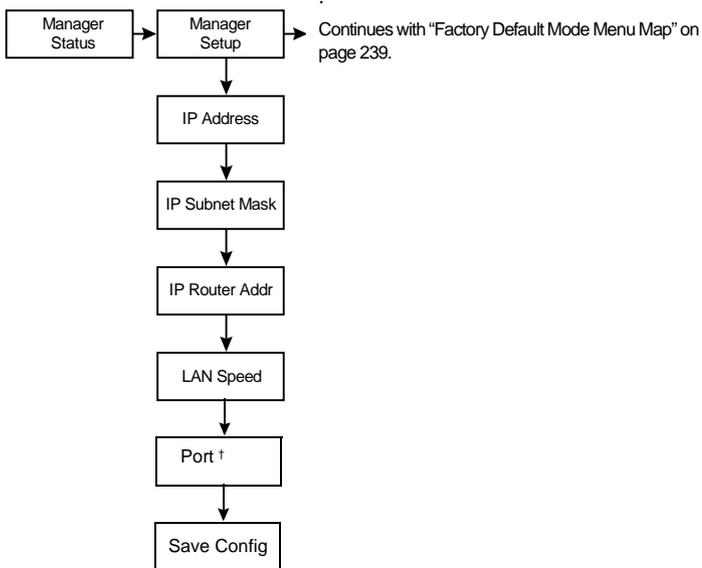
Provides the base configuration for the 833IS so that it can communicate with the Manager.

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 833IS 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 833IS will use a subnet mask of 255.255.255.0
Default Gateway	Set IP default router address for the 833IS. This will be required if the 833IS is not on the same segment as the 833IS Manager.
LAN 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 833IS will not attempt to get on the ring.

Factory Default Mode and Setup Map

Menu	Description
Port	Options are BNC, RJ45, Auto Detect. This panel is only available for versions of the 833IS with a BNC Ethernet interface in addition to the RJ45 interface.

Factory Default Mode and Setup Map



† Can be configured only when the unit includes both BNC and RJ-45 Ethernet interface.

Factory Default Mode

Indicates start of Factory Default Mode Displays.

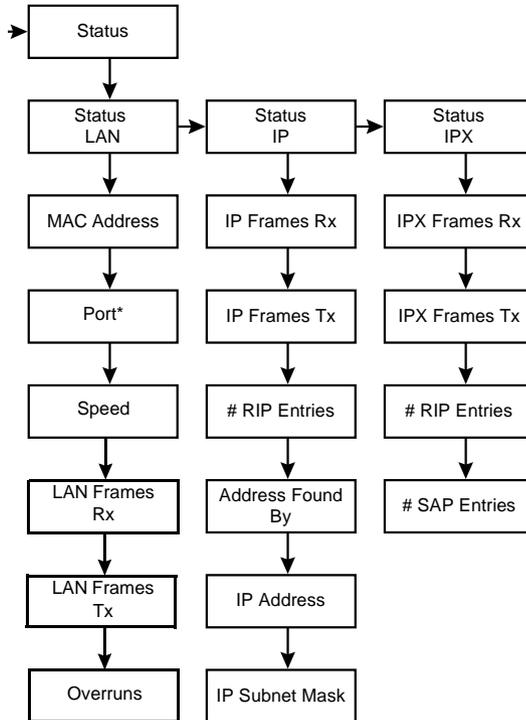
Menu	Description
LAN	
MAC address	MAC Address of the LAN adapter.
Port	Port type. Display only when the unit includes both BNC and RJ-45 Ethernet interfaces.
Speed	Speed of LAN. Display only when the unit includes Token Ring interface.
LAN Frames Rx	Number of frames received by the LAN adapter since 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: <ul style="list-style-type: none"> ■ BOOTP ■ RARP ■ Configured ■ Default
IP Address	IP address of the 833IS.
IP Subnet Mask	IP subnet mask of the 833IS.
IPX	

Factory Default Mode

Menu	Description
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 236.



* Displayed only when the unit includes both BNC and RJ-45 Ethernet interfaces.

Factory Default Mode Menu Map

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 Interface. 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 an ISDN line and a standard phone line, the 833IS 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 Commands

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.

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 833IS.
- 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 833IS.
- 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 - RLSA (DCD)
Option**

The modem controls the RLSA output in accordance with the parameter supplied.

&C0 RLSA remains ON at all times.

&C1 RLSA 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

ERROR If 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.

ERROR otherwise.

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.

AT Commands

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).

2. <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 automodding down from V.32 bis 14400 bps.
3. <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 bps.

<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.

Error Detection and Data Compression Commands

In error correction mode, the modem will signal a break through the active error correction protocol, giving no indication of the length.

\B1-\B9 Break length in 100 ms units. (Default = 3.) (Non-error corrected mode only.)

Result Codes:

OK If connected in data modem mode.

NO CARRIER If 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 WAN 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 WAN 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 WAN 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

S-Register Definitions

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 (0000011b)
 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.

AT Command Set Summary

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.
 OO 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.

AT Command Set Summary

&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.

AT Command Set Summary

+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	67 x 430 x 310 mm 2.6 x 16.9 x 12.2 inches
Weight	5.5 kg/ 12 lbs maximum

Physical/Electrical Specifications

Operating Temperature	0° - 40° C 32° - 104° F
Relative Humidity	0% - 95%, non condensing
Power	100 - 125 VAC, 50 - 60 Hz, 0.5A 200 - 240 VAC, 50 - 60 Hz, 0.25A
BTU Output	100 BTU/hour maximum
MTTR	30 minutes
MTBF	100,000 hours

Chassis

- 19" rack mountable, 1.5U high
 - 2 slots, rear loading
 - 1 System card
 - Optional expansion card can double number of BRI and modem resources
- Power Supply**
- Auto sensing power supply
 - ON/OFF switch
- LCD Panel**
- 2 rows by 16 characters backlit display
- Keypad**
- 6 keys used for system setup and status inquiry.
- Status LEDs**
- Power
 - System Active
 - LAN status

Memory

- System Card**
- 8 meg RAM in SIMM sockets for RAM expansion.
 - 4 meg Flash for Firmware storage in SIMM sockets.
 - 128K non volatile log
- Expansion Card**
- 4 meg RAM in SIMM sockets for RAM expansion.

LAN Interfaces

- Ethernet**
- 10/100 Mbps Ethernet Network interface with hardware MAC address range filtering.

Protocols Supported

- 10Base-T
- 100Base-TX

Connectors

- RJ45

LAN Wiring Supported

- 10Base-T: Category 3, 4, 5 Unshielded Twisted Pair
- 100Base-TX: Category 5 Unshielded Twisted Pair or Type 1 shielded twisted pair

Token Ring

- 4/16 Mbps Token Ring Network interface with hardware MAC address range filtering.

Protocols Supported

- Early token release at 16 Mbps

Connectors

- DB15 (AUI)
- RJ45

Token Ring LAN Wiring Supported

- Shielded twisted pair types 1, 2, 6, 9
- Unshielded twisted pair type 3, 4, 5

ISDN BRI Interface

Physical Connection

- Cable
- U interface: 2 Wire
- S/T interface: 4 Wire
- Network connectors - four, RJ-45

Framing Formats

- U interface: 2B1Q
- S/T interface: I.430

Line Formats

- 2B1Q
- S/T interface: Pseudo Ternary

PerleDSP Modem Interface

- ISDN Network Protocols Supported**
- US NI-1
 - AT&T 5ESS
 - NT DMS100
 - Japan INSnet64 BRI
 - EuroISDN ETSI Net3

PerleDSP Modem Interface

- Data Modulations Supported**
- V.90
 - 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**
 - U-Law and A-Law Supported
 - DTMF Signaling Supported

Approvals

CE Mark

- Safety**
 - Canadian Standards Association (CSA)
CAN/CSA-C22.2, No. 950-95, Third Edition
 - Underwriters Laboratories (UL)
UL Standard for safety for Information Technology Equipment, UL1950, Third Edition
 - Europe Laboratories (UL)
IEC 950, Amendments 1-4
 - TUV Rheinland (GS Mark)
EN60950:1992+A1+A2+A3
 - IEC 950 (1991) Second Edition with Amendments 1, 2, 3 and 4

- Emissions**
 - USA
FCC Part 15, Class A
 - Canada
Industry Canada ICES-003, Issue2, Class A
 - Europe
EN 55022, CISPR 22
 - Australian and New Zealand approval
AS/NZS 3548 Class A
 - Japan
VCCI Class 1
 - EN 50082-1: 1992 (EMC Directive 89/336/EEC)

- Telephony**
 - Europe
European Harmonized Standard CTR3
 - USA
FCC Part 68
 - Canada
IC CS03
 - Australian Communications Authority Technical Standard: TS-031 (1997)

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
- Windows Communication Interface (COM port redirection)

Security

- PPP**
 - PAP, CHAP
 - Callback authentication
 - Password aging function
- Authorization Servers**
 - Novell Netware Bindery, NDS
 - RADIUS
 - Windows NT Domain
- Token Authorization**
 - Security Dynamics SecureID
 - Axent

Management

- 833IS Manager connected via IPX or IP enables configuration and management through LAN and dial up
- Manager supported on Windows 95/98/NT/2000 Workstation

RFCs Supported

- SNMP support
- Cisco mode management via Telnet and TFTP
- 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 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 833IS 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 833IS making the request.
60	CHAP-Challenge	CHAP challenge sent to client by the 833IS.
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 833IS 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	Service-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 833IS) m = hop count
25	Class	This value is sent to the accounting server unmodified by the 833IS.
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 be included by the 833IS 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 833IS 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**.

Appendix 5: Cisco Configuration Mode

In this manual you will read about:

- Introduction to Cisco Configuration Mode
- Overview of 833IS
- Differences between 833IS and Cisco Products
- Command Overview
- Installation and Configuration of 833IS in Cisco Configuration Mode
- Monitoring the 833IS
- Differences between 833IS Manager and Cisco Management

Introduction to Cisco Configuration Mode

The Cisco Configuration Mode is designed to allow personnel, trained in installation and configuration of Cisco™ products, to manage and configure the 833IS using the same techniques applied to similar Cisco units. Information within this manual is aimed towards people who are thoroughly trained in installations of Cisco products. For others, it is strongly recommended that you follow the standard installation and configuration procedures to manage the 833IS unit.

The Cisco Configuration Mode was designed to present a familiar model and concepts similar to Cisco products. The same procedures and commands that are used to manage the installation and configuration of a Cisco device can be used to configure and manage the 833IS. For example, access to the program storage on flash on a Cisco router is handled like a disk drive. The firmware and configuration storage on the flash on the 833IS can also be accessed like a disk drive through various Cisco commands.

Although the Cisco Configuration Mode for the 833IS is similar to managing Cisco products, there are several unique features of the 833IS that the user should be mindful of. Initial configuration of the 833IS is performed on the front panel instead of a direct serial connection to establish LAN connections. Also, the 833IS unit powers up in a factory default mode from the *bootFlash* volume. This volume is read-only and protects the unit from any modifications to the factory default firmware files in flash memory.

Similar procedures and commands for managing the installation and configuration of Cisco products are incorporated into Cisco Configuration Mode. Familiar key sequences and Cisco commands, wherever possible, are used to manage and configure the 833IS through a Command Line Interface accessed via Telnet. Perle commands, similar in format to Cisco commands, can be used whenever Cisco commands are not applicable for configuring the 833IS unit.

In Cisco Configuration Mode, simple raw commands are required to configure the 833IS unit. However, there is no equivalent Cisco “Setup” script to initially configure the unit. Therefore, it is recommended that the 833IS Manager, a Windows-based application, be used to create an initial configuration for the 833IS. This Manager software has intelligent defaults that will meet the needs of most installations. The configuration can then be customized and updated using Cisco Configuration Mode.

Regardless of the method with which you configure the 833IS unit, you can view the statistics and current status of the 833IS via Telnet. Using standard Cisco commands and/or a Syslog server, events occurring on the 833IS can be monitored and analyzed.

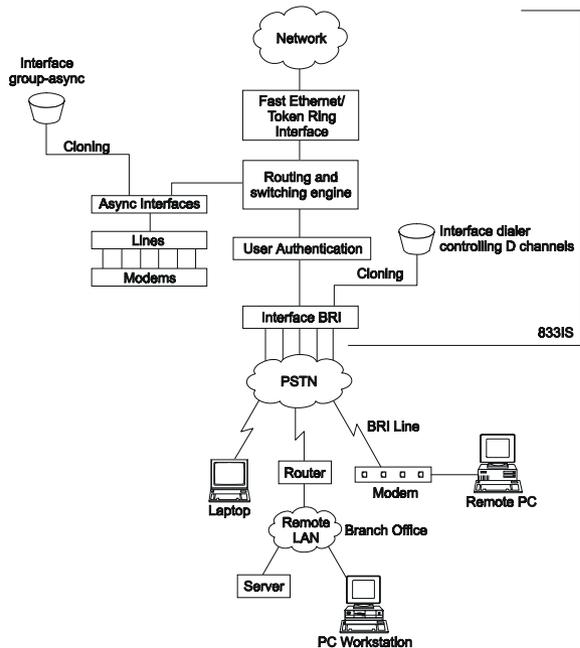
Overview of 833IS

The 833IS allows Remote Users access to the LAN via telephone lines. The Remote Users can then accessed network file servers, printers, e-mail or any other servers on the LAN. It can even act as a Dial-In gateway to another network, such as the Internet.

The 833IS unit is designed with the following features:

- 10/100 Mbps Ethernet or 4/16 Mhz Token Ring LAN connection
- up to 8 ISDN, BRI lines with either ‘U’ or ‘S/T’ interface, each supporting up to 2 simultaneous phone calls (analog or digital) allowing for a total of 16 simultaneous calls.
- designed with 4 MB flash memory with a 512K *bootFlash* volume (ROM) and *flash* (Read/Write) volume.
- NVRAM on the unit has a 64K *nvrAm* volume which the “startup-config” is stored.

Similar to Cisco products the dial topology for the 833IS is illustrated by the following diagram.



Initially, the 833IS unit powers up using the *bootFlash* volume which contains the factory default firmware for the unit. The factory default firmware is the limited code required for the unit to function. This factory default firmware would be equivalent to Cisco's bootstrap system software.

The *flash* volume is a Read/Write flash memory where versions of firmware or configuration files for the 833IS can be stored.

The 833IS can be updated by downloading a new release firmware image to the *flash* volume using the 833IS Manager or TFTP. The release firmware filename convention that is used for the 833IS are as follows:

pcc6600s.img :BRI Line with 'S/T' interface

pcc6600u.img :BRI Line with 'U' interface

Differences Between 833IS and Cisco Products

The startup configuration is a text file stored on the *nvr*am volume on the 833IS. Similar to Cisco products, the “startup-config” is applied upon bootup of the unit. Downloading configuration files using the 833IS Manager will update the “startup-config” file but requires the user to reboot the unit for the configuration changes to be applied. However, through a Telnet session, any dynamic changes to the configuration are stored in the run-time configuration or “running-config” and most modifications take effect immediately. In order to save these new configuration parameters for bootup, the file must be saved to the “startup-config” file.

The 833IS can hold up to two Feature cards. The card in Slot 1 is called the System card and the card in Slot 2 is called the Expansion card. The system card is the main processing card and must be present in the 833IS in Slot 1 but the Expansion card is optional.

The 833IS has a maximum of 8 BRI lines with 4 BRI lines on the System card and optionally another 4 BRI lines on the Expansion card. Each of these interfaces are mapped to a specific number. The interface mapping is 0 based, from 0 to 7, with 0 being the first interface on the System card and 4 being the first interface on the Expansion Card in Slot 2.

The Interface dialer condenses the configuration process and applies common configuration parameters to all BRI interfaces. The 833IS’s group-asynchronous interface also applies generic configuration parameters as a single entity to all asynchronous interfaces. This method is used instead of individual configuration for each asynchronous interface on the 833IS.

Individual users can be configured and authenticated upon each dial-in connection. The user configuration can organize users based upon department and allow individual users specific privileges. User features like expiration date and inactivity timers can also be specified for each user.

Differences Between 833IS and Cisco Products

Although the design concepts and dial-in topology between the 833IS and Cisco router products are similar there are specific differences that the users should be aware of.

As explained in the Overview section, the 833IS is powered up and initially has a default Factory firmware and configuration. Although various firmware versions can be stored in flash memory, the default Factory firmware is stored in the *bootFlash* (read-only) volume which users cannot modify. This protects the 833IS unit from any corruption to the factory firmware. For instance, if a user deletes all

firmware versions from *flash* volume, the 833IS will then still run in factory mode upon bootup.

Instead of initial configuration being performed over a direct serial connection, the 833IS configures IP parameters through the front panel of the unit. The 833IS is able to configure the IP Address, gateway, subnet mask and LAN speed from the front panel enabling connections to be established across the LAN (Ethernet or Token Ring). The 833IS can then be accessed by a console through a Telnet session.

Although Cisco products allow access to internal resources such as queues and buffer sizes, Perle has protected these internal resources and restricts users from modifying them to maintain the integrity and quality of the product.

The interface mapping on the 833IS differs from that on the Cisco router. The card's BRI interfaces are 0 based from 0 to 7 (e.g. the first 4 BRI interfaces are located on card 1 mapped 0-3, the second 4 BRI interfaces are on card 2 mapped 4-7). On the 833IS, commands that are applied to a specific interface will be applied all interfaces that reside on the card. When interactively executing commands to a specific interface, notification messages are displayed indicating which interfaces have been modified. For example, the following command at the global configuration level will set all interfaces in the router to Northern Telecom DMS-100 switch type:

```
isdn switch type basic-dms100
```

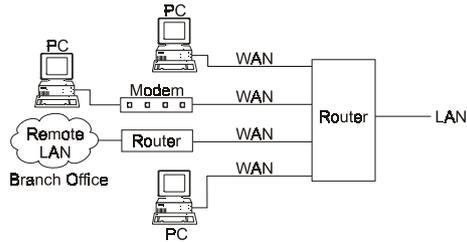
The following commands will set the BRI interfaces 4-7 to DMS-100 and sets interfaces 0-3 to 5ESS since the `interface bri 0` command applies to all interfaces residing on the same card.

```
isdn switch type basic-dms100
interface bri 0
    isdn switch type basic-5ess
```

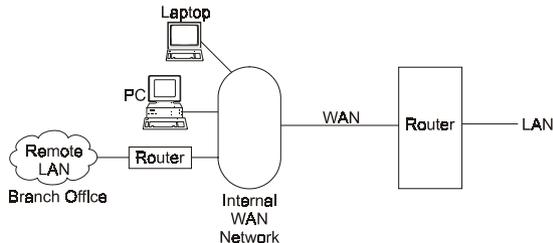
A notification message will be displayed indicating what interfaces have been modified:

“Parameter change applies to all interfaces numbered from 0-3.”

The 833IS handles WAN interfaces differently than Cisco products. Cisco configures IP parameters for each individual WAN interface on the unit. Each WAN interfaces on a Cisco product is considered an individual entity connected to a router which then routes to a device on a LAN.



For IP, the 833IS looks like a router between two networks. The first network is comprised of the devices on the LAN. The second network, referred to as the "Internal WAN network", is comprised of all IP clients and routers that are dialed into the WAN ports.



Setting up a basic 833IS IP configuration requires the following:

- Defining the network on the LAN side, and defining the address of the LAN router port.
- Defining the network on the WAN side, and defining the address of the WAN router port.

All clients dialed into the WAN, see the same address for this WAN router port.

- Each client dialing in requires a unique IP address. The 833IS supports multiple methods for defining and supplying IP addresses to clients.

If a router dials in to the WAN, the 833IS can route traffic from the dial in router to the LAN. This feature is referred to as "LAN-to-LAN". Note that it is not possible to route from this dial in router to a client or router on the Internal WAN network.

Command Overview

Cisco commands used to configure and manage the 833IS are based upon the command structure of Cisco IOS™ version 12. Equivalent Cisco commands may have additional parameters that are not present in the 833IS version. If the additional parameters are included with the command and are executed from a file no error messages will be displayed. Depending upon the parameter entered, one of the following scenarios occurred:

- an intelligent default has been used for the additional parameter
- the command is not supported and was not executed
- the command was executed, however, the additional parameter was ignored

However, if commands are entered interactively through a Telnet session, an error message will be displayed indicating the action taken and/or corrections necessary to execute the command. Some Cisco commands may require additional Perle parameters. These Perle parameters can easily be identified as they start with a “_” (underscore) character.

The Cisco command set does not accommodate all the configuration and management features for the 833IS. Therefore, Perle commands have been developed to modify these features on the 833IS unit which are not present in a Cisco environment. The Perle commands use a similar syntax as Cisco commands but are uniquely identified by the “_” (underscore) character preceding the command. A complete set of supported Cisco and Perle commands can be found on Perle Systems Ltd. website www.perle.com.

Installation and Configuration of 833IS with Cisco Configuration Mode

The 833IS unit can be configured using the 833IS Manager. It is recommended that this Windows application be used to initially setup the 833IS for standard configurations required by most installations.

Initially, the 833IS is in Factory Default mode, or simply Factory mode, and is running a factory default configuration which has all WAN interfaces disabled. The operating firmware and configuration for the 833IS must be downloaded to the Server from the 833IS Manager or through a Telnet session.

However, before the operating firmware and configuration can be downloaded the LAN parameters must be configured. In Factory Default mode, the Front Panel lets you:

- Set the parameters needed for communication with the Management PC or Telnet/TFTP session
- Monitor the 833IS's operation on the network to verify correct configuration and provides information to diagnose network problems.

To navigate through the Front Panel screens the following keys are used:

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 IP Address:

Press 

Manager Setup

Press 

IP Address

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

IP Address
233.233.233.011

Use   to select the digit to change. Use   to change the digit.

When completed, press **Enter** to accept the new IP Address and the 833IS unit new IP configuration takes effect immediately

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 833IS 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 

Default Gateway
000.000.000.000

Enter the IP address of the default router if required.

Press ▼

LAN Speed

Set the value to match your LAN speed set to 4 or 16 Mbps for Token Ring or set to Auto, 10 or 100 Mbps for Ethernet.

Press ▼

**Port
RJ45**

If you have an Ethernet interface on the card installed in slot 1, this panel may be displayed. Some versions of the 833IS contain a BNC Ethernet interface in addition to the RJ45 interface. For these units, you can use this panel to override the auto port detect feature of the 833IS. Once set, the 833IS will no longer try to auto detect this port, even after a restart of the unit. The only way to re-enable the auto detect feature is via this menu item.

Set the value to the desired port (RJ45, BNC, or Auto Detect).

Once the IP parameters have been changed, the 833IS is now running with a minimum configuration containing the new IP Address. You will be prompted to save this configuration as the startup configuration file so it will be loaded each time the unit is rebooted. This minimum configuration is required to establish a Telnet/TFTP session and for downloading firmware and/or configuration files.

Press ▼

Save Config

If you wish to save your configuration to NVRAM then press Enter.

**Save Config
Confirm**

Press Enter again to confirm the saving of this configuration.



This configuration takes affect immediately and does not require an IPL of the 833IS.

At this time you can connect to the 833IS through a Telnet session on your PC. The front panel of the unit can be used to verify that communications between the PC and the server are operational. A simple ping command to the unit's IP Address will display the following text on the front panel of the 833IS:

Ping	5
172.017.006.016	

This text on the front panel indicates it has received 5 ping requests from the PC with the IP Address of 172.017.006.016. If you send ping requests from the PC and do NOT receive any replies to these requests, you can check the front panel to see whether the 833IS received any of the ping requests. If the front panel does not display your PC's IP Address, then no ping requests were received and modification to the network configuration on your PC is required in order to communicate with the unit. However, if the unit displays the IP Address of the PC originating the ping requests then the default gateway and/or subnet mask on the 833IS unit is incorrect. Changes to these IP configuration parameters can be made through the front panel for your network configuration.

Once connected to the 833IS through a Telnet session, only the necessary set of commands are available and are listed in the help of your Telnet session by executing the ? command.

At this time, you can download the operating firmware from the 833IS Manager or TFTP server. For example, with a TFTP server running on the PC with IP Address 172.17.6.16, the following command will download the new firmware image file pcc6600u.img from your PC to the *flash* volume on the unit:

```
router #copy TFTP://172.17.6.16/pcc6600u.img flash:new_firmware.img
```

Modification to the 833IS configuration by using various Cisco and Perle commands can now be executed through the Command Line Interface via Telnet. Configuration text files and versions of firmware can be stored in flash and accessed similar to other Cisco products.

The new firmware image can now be loaded from the *flash* volume using the command

```
router(config)# boot system flash <filename>
```

This command is used by the router to determine which image <filename> to load at startup or when the **reload** command is executed.

Monitoring the 833IS

In Cisco Configuration Mode, you are able to monitor statistics and the status of the 833IS. During your Telnet session, you can execute the **show** commands which retrieve the latest statistics and are displayed on your Telnet interface.

The 833IS can also send Event Log messages in real time to up to 4 Syslog servers concurrently. These Syslog servers can be attached to either the LAN or the WAN interfaces. Configuration of the Syslog servers can be performed through the 833IS Manager or using the following Cisco command:

```
logging <syslog host>
```

To trap specific event messages such as critical or informational events you can use the following Cisco command:

```
logging trap <trap level>
```

For further detailed information regarding the logging Cisco commands, please refer to the complete set of supported Cisco and Perle commands found on Perle Systems Ltd. website www.perle.com.

Differences between 833IS Manager and Cisco Configuration Mode

The 833IS Manager is a Windows software application designed specifically to configure and manage the 833IS unit. However, the Cisco Configuration Mode provides an easy transition for personnel trained in Cisco configuration to manage and setup the 833IS. Some of the methods and procedures used by the 833IS Manager are handled differently than commands used in Cisco Configuration Mode.

In Cisco Configuration Mode, the onboard flash is treated as a disk drive. Firmware images and configuration files are written to the flash as files and are managed with TFTP commands. This allows the full capacity of the flash to be utilized with multiple configuration and firmware images. However, once files have been written to flash it cannot be erased unless the entire flash volume is erased. Although,

through Cisco commands you can delete files from the flash, the files are hidden and still consume space on the *flash* volume. Until the entire flash is erased, the memory is still consumed by the hidden files.

If configuration of the 833IS is performed using the 833IS Manager, maintenance on the *flash* volume is not necessary. The Manager stores a single firmware image in the flash volume and a single configuration file in the nvram volume. If the Manager detects additional files in the *flash* volume, a warning message is displayed and you will be given the option to erase the entire *flash* volume or abort the download.

When configuration is performed in Cisco Management Mode, there is not extensive checking done on the new configuration parameters. As each command is executed, the configuration changes takes effect immediately. The advantage of building up a configuration interactively is having each modification take immediate effect. However, these command actions have no validity mechanism to ensure a logical configuration is operating and not causing any disruption to the online session.

When the 833IS Manager downloads a new configuration to the 833IS it performs a validity check on the configuration file beforehand. This prevents illogical configuration parameters from being downloaded to the unit. Once a valid configuration is successfully downloaded, the unit is required to be rebooted in order for the new configuration to take effect. Unlike the dynamic interaction of the configuration of 833IS using Cisco Configuration Mode, the 833IS Manager maintains the unit's integrity through validation methods.

Telnet sessions is the means of modifying and managing the 833IS in Cisco Configuration Mode. Although this method is effective there are certain limitations that Telnet has, which can affect the capability of certain Cisco and Perle commands. Telnet restricts the text to characters that are supported by the 7 bit ASCII character set. This restriction prevents the ability of entering "double byte" characters used in the Japanese language and accented characters presented in many other languages. This means that user names and passwords MUST contain only characters that are available in the ASCII character set.

The 833IS Manager was designed with many language versions to handle this scenerio. This Windows based application is available in 2 versions:

- 1) English Single Byte Character Set version which is available for all countries except Japan.
- 2) English Double Byte Character Set version which supports text field entry of Japanese Kanji characters and is only available for Japan.

The Manager is able to enter, view and download accented and "double byte" characters. However, when these characters are viewed through a Telnet session they will be incorrectly displayed.

Differences between 833IS Manager and Cisco Configuration Mode

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

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 a WAN 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.

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 02FFFFFFF00 for Ethernet, and 400000000000 to 40FFFFFFF00 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 Beaconsing*

Beaconsing

When a Token Ring adapter has sent a beacon frame indicating a serious network problem, it is said to be beaconsing. *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.

Callback

A Security feature where the Perle 833IS calls back the User at a predetermined number defined in the User's account. *See Fixed and Roaming Callback*

CBCP (Callback Control Protocol)

A callback protocol defined by a RFC.

Central Site

A generic term that refers to the Perle 833IS 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.

CSU (Channel Service Unit)

A device that connects a digital telephone line to a multiplexer, bridge or router.

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.

Demarc 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.

DTMF Tones (Dual Tone Multi-Frequency)

Touch-tone dialing.

Dynamic

Refers to Hardware or Software that can respond instantly to changes as they occur.

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.

Ethernet

A high-speed (10Mbps,100Mbps) cable technology that connects devices to a LAN, using one or more sets of communication protocols.

Feature Card

An optional circuit board addition that increases the capabilities of the 833IS. The card can be installed by the reseller. Available cards are Token Ring, Ethernet, ISDN BRI U, ISDN BRI S/T and PerleDSP Modem.

Fixed Callback

A method where the number used for callback is contained within the 833IS 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.

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.

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 833IS.

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*.

IP Subnet Mask

see *subnet mask*

LAN (Local Area Network)

A Network system that does not use Long Distance carriers. A LAN is usually limited by cable length restrictions.

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 833IS User database. When the remote Client connects, it will communicate with the 833IS using either the CHAP or PAP security protocols.

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 PC's, 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 833IS 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 833IS 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 Callback

A method where the client supplies the number for callback when they dial in.

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.

SPID (Service Profile Identifiers)

The Service Profile Identifier is a numeric string assigned to an interface or channel by the service provider. The SPID configured on the 833IS is sent to the service provider at start-up. This is used by the service provider to assign class of service to a channel.

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.

Thinner

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.

Index

Numerics

100Base-TX **16**
10Base-T **15**

A

Access-Accept Messages **280**

Accessing

Card statistics **202**

Security Screen **171**

Accounting Messages **282**

Account Request Messages **279**

add new Feature Card **72**

Addresses

Fixed MAC Address **144**

User IP address **144**

Use Standard Profile **140**

Agent ID **178**

Agent Key **177**

AIS **299**

Ambient, Temperature **271**

Analog **206**

ANSI **299**

Assemble

Hardware **27**

Rack Mount **28**

Asset ID **164, 299**

AssureNet **176**

Async Control **299**

AT% Commands **253, 259**

AT& Commands **251**

AT+ Commands **255**

AT command **299**

AT Commands **241**

ATP **299**

Attach

Ethernet Cable **29**

Token Ring Cable **30**

Attempts

Modem **207**

AUI **16, 299**

Autonomous Unit Interface see AUI **299**

Axent **176**

B

B8ZS **299**

Basic Rate Interface see BRI **299**

Bayonet-Neill-Concelman Connector
see BNC **299**

Beacon **299**

Beaconing **299**

BIOS

version **200**

BNC **299**
BOOTP **39, 299**
BOOTstrap Protocol see BOOTP **299**
BRI **1**
Bridge Filter **188**
broadcast filter **188**
BTU Output **271**
buffered port **44**
Burned In Address **77, 78, 300**
Bytes
 received **203**
 transmitted **203**

C

Cable
 Attach
 Ethernet **29**
 Token Ring **30**
 Ethernet **14**
 Planning **14**
 Telephony **19**
 Token Ring **17**
Cable Requirements **14**
Call **206, 208**
 Type **206**
Call Back **146, 183, 300**
 Enable Fixed **146**
 Enable Roaming **146**
 Phone Numbers **147**
 Preferred **147**
 Roaming **303**
Card
 statistic
 Ethernet **202**
 Modem **207**
 Token Ring **203**
Card Statistics
 Accessing **202**

CBCP **145, 300**
Central Site **300**
Channel **300**
 Mode **205**
Channels
 in group **186**
 main pool **185**
Channel Service Unit see CSU **300**
CHAP **169, 176, 300**
characters, Trigger **168**
Chassis
 Specifications **272**
Chassis Description **24**
Client Handling **64**
 Apple Remote Access Client **65**
 Bridge Client **65**
 Router Client **64**
Commands
 AT **241, 254, 259, 279**
 AT% **253, 259**
 AT& **251**
 AT+ **255**
 Basic AT **266**
 ECC **269**
 MNP 10 **269**
 Set Summary **266**
Compression **300**
Configuration, Off-line **57**
Configuration File
 Creating a new **68**
 Downloading **69**
 Opening **68**
 Saving **69**
 Uploading **68**
 Window **70**
Configure **300**
 Menu **53**
Configuring **75, 120, 122**
 Feature Card **75**

- Protocols **89**
- Security **171**
- Static Route Services **122**
- Connection
 - Ethernet **202**
- Connect Time **156**
 - Setting limit **142**
- CRC4 **300**
- Creating
 - new configuration file **68**
- CSU **300**

D

- Database **300**
- Date and Time
 - Setting **74**
- DB9 **30**
- Default
 - gateway **300**
- Defaults
 - Factory **54**
- Delay Start **300**
- Demarcation Point **19**
- Demark Point **300**
- DHCP **96, 102, 300**
- Dial in
 - Bridge filter **183**
 - PPP protocol setting **183**
 - User standard profile **183**
- Dial Modifiers **243**
- Dial Out **166**
 - Character Time Out **167**
 - Packet Size **167**
 - Trigger characters **168**

- Digital **300**
- Digital Pathways Assurenet **2**
- Dimensions **271**
- Disabled **300**
- Diskette Packet **21**
- Display
 - IP RIP Table **211**
 - IPX RIP Table **213**
- Download **69**
 - a configuration to an 833IS **69**
- DSX-1 **300**
- DTMF **300**
- Dual Tone Multi-Frequency see DTMF **300**
- Dynamic **300**
- Dynamic Host Configuration Protocol see DHCP **300**

E

- E & M **300**
- edit **76**
 - Feature Card's configuration **76**
- el **82, 84**
- Emulation **300**
- Enable **301**
- enable
 - roaming call back **156**
- Errored Seconds **301**
- Ethernet **29, 77, 202, 301**
 - Cabling **14**
 - Override MAC Address **77**
 - Overruns **202**
 - Server MAC Address **77**
 - Use Burned In Address **77**
- Ethernet II **115**
- Event Log **54**
 - Change Filter **54**
 - Clear **54**

Get **54**
viewing **54**

F

FAX Class 2 **269**
FDL **301**
Feature Card **301**
 add **72**
 Configuring **75**
 display **200**
 Edit **76**
Feature Cards **75**
File Menu
 Manager **52**
Filter **110**
 Bridge **188**
 broadcast **188**
 multicast **188**
Firmware **58**
 Download **54**
 download **43**
 loading **43**
 upgrade **58**
Flow Control **166**
 Hardware **167**
 No **167**
 Xon/Xoff **167**
Frame **301**
frames
 RX **38**
 TX **38**
Framing **301**
Front Panel **199, 220**
 Editing Fields **221**
 Modes **220**
 Navigating **221**
 Password **165**
 set up **33**

FXS **301**

G

Gateway **102, 301**
Ground Start **301**
Group **163**
 About **166**
 advanced
 bridge filter settings **187**
 dial out **187**
 PPP protocol **187**
 User standard profile **187**
 advanced settings **186**
 Call back **185**
 Dial in **183, 185**
 Dial out **183, 185**
 Enable **185**
 Name **185**
group
 preferred call back **156**
Grouping **2**
Group Settings **166**

H

Hardware
 Assembling **27**
 LAN cable **29**
 Power Cord **27**
Help
 Manager **56**

History **207**
Hot Swappable **301**
HP OpenView **189**
Humidity, Relative **271**

I

IEEE **301**
Incoming Call Handling **64**
Installation **7**
Installing
 Manager Software **45**
Institute of Electrical and Electronic Engineers see IEEE **301**
Integrated Services Digital Network see ISDN **301**
Interface **203**
Internet Packet eXchange see IPX **301**
Internet Protocol see IP **301**
IP **45**
 # Frames TX **39**
 # RIP entries **39**
 Address **39**
 address **32**
 connection
 Manager **32**
 requirements **32**
 Default Router **102**
 frames
 TX **39**
 Server Address **101**
 static routing **45**
 Status **39**
 subnet mask **32**
 WAN Address **96**
IP Filter Definition **110**
IP RIP, Display contents **211**
IPX **45, 114**
 # Frames RX **40**

 # Frames TX **40**
 # RIP Entries **40**
 # SAP Entries **40**
 AppleTalk **132**
 connection
 Manager **32**
 Dial in Network Number **116**
 Frame Type **115**
 Netbeui **133**
 RIP **213**
 SAP **214**
 Static Routing **117**
 Status **40**
IPX Filter **160**
IPX RIP
 Display contents **213**
ISDN **204**
 analog **206**
 digital **206**

L

L **84**
LAN **44**
 Cabling **14**
 frames
 RX **38**
 TX **38**
 MAC Address **38**
 Overruns **39**
 Port **38**
 Speed **38**
 Status **38**
 Using **43**
LAN cable
 Attaching **29**
 Ethernet **29**
 Token Ring **30**

Lantastic **89**
LAN-to-LAN **161**
List, Server **49**
Loop Start **301**

M

MAC **301**
Main Screen
 Manager **51**
Main screen **51**
Manager
 Connection
 IP **45**
 IPX **45**
 Setting up **45**
 functions **43**
 Installing **43**
 LAN Connection
 Requirements **44**
 requirements **43**
 software **43**
 Statistics **199**
 Accessing Card Statistics **202**
 Call Status **205**
 Channel Status **205**
 Ethernet **202**
 Modem **207**
 Protocol **209**
 Server Information **200**
 Token Ring **203**
 Viewing **199**
 System requirements **43**
 WAN Connection
 Requirements **44**
Manager software
 installing **45**
 menu descriptions **52**

MAU **37, 48, 301**
Media Access Code see MAC **301**
Menu
 Configure **53**
 File **52**
 View **53**
Menu Bar **52**
Menu Descriptions
 Card Type **224, 291**
 Control **224, 291**
 Factory Default Mode **235**
 Factory Default Status **237**
 Network Status Display **232**
 Setup **235**
 Status **224, 291**
Microsoft
 Windows NT Version 3.5 **44**
Mode
 Channel **205**
Modem **207**
 Assigned **207**
 Initialization String
 Modify **87**
 initialization string **301**
 Name **87**
Modem Initialization String **301**
Modems
 group **186**
 main pool **186**
MODulate/DEMmodulate see Modem
301
MTBF **271**
MTTR **271**
multicast **302**
 Filter **188**
multiplexing **302, 303**
 time division **303**

Multistation Access Unit see MAU **301**

N

NAK **302**
NDIS **65, 302**
nel **82**
NetBEUI **129, 133, 302**
NetBIOS **64, 133, 302**
NetBIOS Extended User Interface see
Net BEUI **302**
Network
 Broadcast Address **302**
 Number **302**
network address **214**
Network Basic/Input Output System
 NetBios **302**
Network Bindery
 Netware Group Name **172**
 Server Name **172**
Network Driver Interface Support
 NDIS **302**
Novell
 Server Types **214**
NT Domain **181**

O

ODI **65, 302**
Off-line Configuration **57**
Opening
 existing configuration file **68**
Open Systems Interconnection Model-
see OSI **302**
Operator Panel **24**
 keypad **24**
 LCD **24**
OSI **302**
Overruns
 Ethernet **203**

Token Ring **204**

P

Packet **302**
PAP **169, 176, 302**
Password
 Front Panel **165**
 Front panel **165**
PBX **302**
PC requirements **44**
Perle 833IS
 Features **1**
 Lan connection **29**
 system statistics **54**
Placement, Unit **13**
Point to Point Protocol see PPP **302**
ports
 serial **44**
Power
 Specifications **271**
 switch **27**
Power Cord **7, 27**
 Connect **27**
Power Switch **27**
PPP **129, 302**
 Compression **129**
 Time-outs **129**
PRI **80, 130, 302**
Primary Rate Interface see PRI **302**
Print **52**
 Preview **52**
 Setup **53**
Private Branch eXchange see PBX **302**
Protocol **302**
 Filter **302**
 Statistics **209**
Protocols
 Configuring

- AppleTalk **132**
- Bridge **126**
- IP **92**
- Netbeui **133**
- PPP **129**
- Protocol Stack **302**

Q

- Quick Buttons **51**

R

- Rack Mount **302**
 - Assembling **28**
 - Attaching **28**
- Radius **2, 96, 173, 302**
 - Security **173**
- RADIUS Server Attributes **279**
- RARP **39, 302**
- Recent File List **53**
- Reduced Instruction Set Computer
 - RISC **303**
- Relative Humidity **13, 271**
 - Operating **13**
- Remote Authentication Dial In Users
- Services see Radius **302**
- Remote Node **63, 302**
- Removing
 - Feature Card **73**
- Request for Comment see RFC **302**
- Requirements
 - Cable **14**
- Reverse Address Resolution Protocol
 - RARP **302**
- RFC **189, 302**
- RIP **302**
 - entries **39**

- RISC **303**
- RJ11 **303**
- RJ-45 **14, 303**
- RJ-48C **19, 303**
- Roaming Call Back **303**
 - enable **156**
- Router **303**
- Routing Information Protocol see RIP **302**

S

- SAP **40, 117, 214**
- Save **52**
 - configuration file **69**
- Save As **52**
- SecurID **2, 179, 303**
 - Master IP Address **179**
 - Security **179**
- Security **2, 169**
 - AssureNet **176**
 - Call Back **169**
 - Capabilities **169**
 - CHAP **169**
 - Configuring **171**
 - Local **171**
 - Netware Bindery **172**
 - Network Bindery **172**
 - PAP **169**
 - Radius **173**
 - SecurID **176, 179**
 - Static Routing **170**
 - User Authentication **169**
- Security Screen
 - Access **171**
- Serial Number label **27**
- Server **163, 200-??**
 - Asset ID **200**
 - Connecting **47**

- Dial-Out **163**
- Group **163**
- Group Settings **166**
- Main Screen **164**
- Name **200**
- Novell
 - Advertising Print Server **214**
 - Archive Server **214**
 - File Server **214**
 - Job Server **214**
 - Print Queue **214**
 - Print Server **214**
 - Remote Bridge Server **214**
- Up time **200**
- Server List **49**
- Service Advertising Protocol see SAP **303**
- Setting, Date and Time **74**
- Setup
 - Front Panel **33**
 - Perle 833IS **8**
 - Print **53**
- Shared User Database **160**
- Shielded Twisted Pair see STP **303**
- Simple Network Management Protocol
 - see SNMP **189**
- Simple Network Management Protocol
 - see SNMP **303**
- SNAP **115, 212**
- SNMP **169, 303**
 - Agent **189**
 - Community **191**
 - Manager
 - No Access **189**
 - Read/Write **189**
 - Read-only **189**
 - RFC Supported **189**
 - Trap Host **190**
- Sockets **122, 303**
- Speed
 - Modem transmit, receive **208**
 - Token Ring **203**
- S-Register Definitions **263**
- S-Registers **261**
- Standard Profile **303**
- Start
 - Delay **300**
- Static Route Services **122**
- Statistics
 - Accessing Card **202**
 - Get **54**
 - menu **199**
 - Protocol **209**
 - Viewing **199**
- Status **205–206, ??–208**
 - Call **206, 208**
 - Channel **205**
 - Lan **38**
 - Modem **207**
- Status Bar **51**
- STP **30, 303**
 - Token Ring **18**
- Subnet mask **303**
- Subnetwork Access Protocol see SNAP **303**
- Support **303**
- Switch
 - Power **27**
- System
 - Active **24, 25**
 - Card **25**
- System Requirements **44**
 - Manager **44**

T

- Tables, Community **191**
- TCP **303**
- TCP/IP **44, 303**
- Telephone
 - Attaching line **10, 42**
- Temperature Range **13**
 - Operating **13**
- Thinnet, Definition **303**
- Time Division Multiplexing
 - Definition **303**
- Time Out **141**
 - Inactivity **155**
 - setting inactivity time out **141**
- Token Ring **30, 203, 303**
 - Cable **17**
 - Server MAC Address **78**
 - STP **18**
 - UTP **18**
- Tool Bar
 - Commands **56**
- Transmission Control Protocol see TCP **303**
- Trap Host **190**
- Trigger Character **304**
- Type **206**
- Type, Call **206**

U

- Unit Placement **13**
- Unpacking **8, 22**
 - contents of box **21**
- Unshielded Twisted Pair see UTP **304**
- Uploading
 - a configuration from an 833IS **68**
- User
 - Call Backs **145, 156**
 - disabled **139**

- Password **304**
- Records **136**
- Standard Profile **187**
- User Authentication **169**
- User ID **2**
- User Profile **141**
- UTP **30, 304**
 - Token Ring **18**

V

- ventilation **7**
- version
 - BIOS **200**
 - Firmware **200**
- View Menu **53**
- Views **23**
 - Perle 833IS **23**

W

- WAN **44, 304**
- Weight **271**
- Wide Area Network see WAN **304**
- Window Menu **55**
- Windows 95 **44**
- Wink Start **304**

