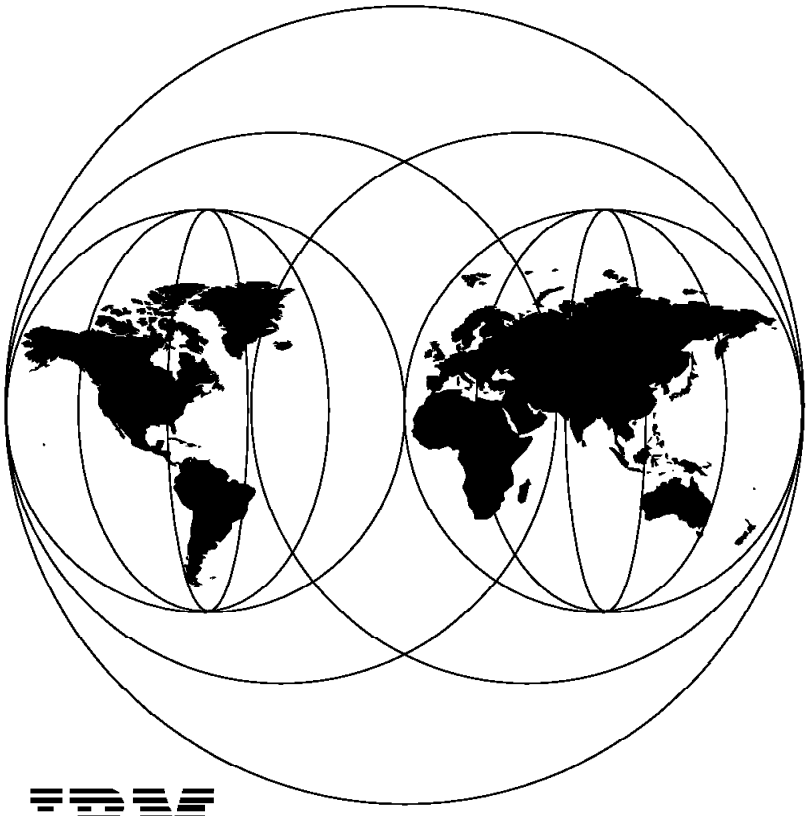
SG24-2132-00

IBM 8235-I40 Access Switch Concepts and Implementation

October 1997



IBM

International Technical Support Organization
Raleigh Center

International Technical Support Organization

SG24-2132-00

IBM 8235-I40 Access Switch Concepts and Implementation

October 1997

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, “Special Notices” on page 259.

First Edition (October 1997)

This edition applies to Version 4, Release Number 5 of the 8235-I40 Access Switch.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Preface

This redbook describes the 8235-I40 Access Switch and the basic principles and concepts of remote connection, including Dial-In, Dial-Out, and LAN-to-LAN routing. It also discusses the concepts of high-speed networking and how the 8235-I40 Access Switch handles remote calls from these networks.

A planning section will give you all the procedures necessary when designing and installing an 8235-I40 Access Switch and will help you build a high-speed network connection with your network provider.

This redbook also provides several installation and administration scenarios that include the 8235-I40 Access Switch with such functions as Dial-In, Dial-Out, and LAN-to-LAN. Detailed instructions are given on specific connection items, such as physical links, cards/modules, security and multiprotocol workstations, with special emphasis on implementation of the client workstation in different operating systems environments, with detailed configuration procedures and files for each of them.

This redbook will help you design and implement a remote LAN connection environment that will include not only the 8235-I40 Access Switch but also several multiprotocol workstations with different operating systems. A knowledge of networking and protocols such as IP, IPX, SNA and NetBIOS is assumed.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the Systems Management and Networking ITSO Center, Raleigh.

Ricardo Haragutchi is a Senior ITSO Specialist at the Systems Management and Networking ITSO Center, Raleigh. He writes extensively and teaches IBM classes worldwide on all areas of LAN Hardware and the Internet environment. Before joining the ITSO two years ago, Ricardo worked in the Field Systems Center (FSC), IBM Brazil as a Senior System Engineer.

Brenda Terry is an Advisory Marketing Support Specialist at the LAN and Campus National Technical Support Center in Raleigh, NC. She has seven years of experience in the networking environment. Currently she provides technical support and services for her customers worldwide for Remote Access, LAN and ATM Campus networks.

Leon Meyer is a Network Services and Availability Services specialist in IBM South Africa. He has four years of experience in networking products.

Wahyu Supriantono is a System Engineer at IBM Indonesia. He has four years of experience in the SNA mainframe environment and two years in the Networking field. He now works in the PC/NW/NWS Department, IBM Indonesia as an I/T Specialist.

Marshall Smith is a System Engineer in development in RTP. He has four years of experience in the Networking field. He has worked at IBM for two years. His areas of expertise include ISDN, Networking and Remote Access.

Thanks to the following people for their invaluable contributions to this project:

Gail Wojton
Mike Haley
Paul Braun
Systems Management and Networking ITSO Center, Raleigh

Pat Pierce
Steve Zundel
IBM Corporation

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in "ITSO Redbook Evaluation" on page 269 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

  For Internet users `http://www.redbooks.ibm.com`
  For IBM Intranet users `http://w3.itso.ibm.com`

- Send us a note at the following address:

  `redbook@vnet.ibm.com`

Chapter 1. High-Speed Networking

This chapter gives a brief overview of the high-speed networking concepts that are used by the 8235-I40.

The sample topology below shows how the architecture of high-speed networks can fulfill the current and future needs of customers, including:

- Integrating the private enterprise LAN and Internet.
- Providing employees access to client/server groupware applications, databases, and Internet from home offices or while traveling.
- Providing customers and vendors access to company intranets for inventory scheduling, product ordering, and other network-based services.
- Aggregating incoming traffic to Internet Service Providers, enabling them to provide Internet access to their customers.
- Providing single phone number for analog and ISDN access enhances end-user ease of use and manageability.
- Supporting mixed ISDN/analog sessions via multiple T1/E1/PRI access lines.

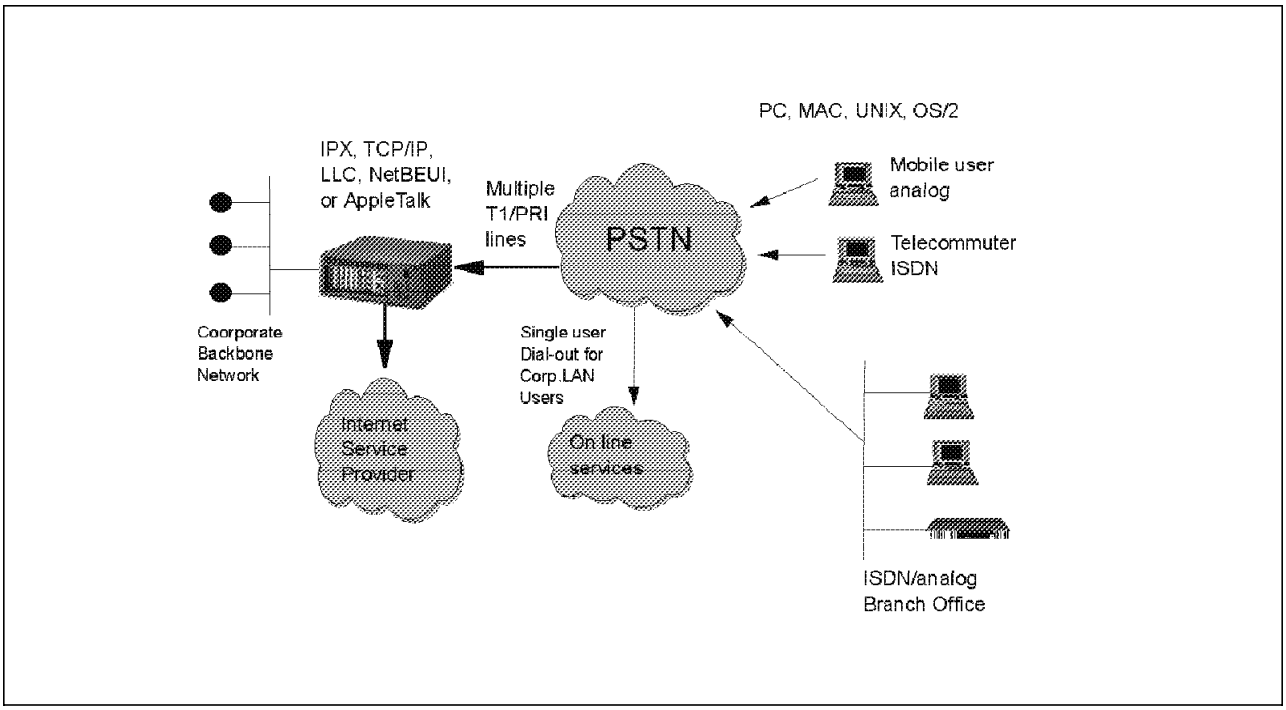


Figure 1. Sample Network Topology

1.1 Analog vs Digital Comparison

The table below compares analog and digital technology.

Table 1. Comparison of Analog and Digital Technology

Analog	**Digital**
Modems	Codec (decode PCM data)
Long setup time	short setup time
Poor signal to noise ratio	Good signal to noise ratio
Minimal error detection and correction	Error detection and correction
Low bandwidth (300Hz to 3.4Khz)	High bandwidth (depending on data rate)
100% Availability	70% Availability (growing)
Pay only on connection	Pay when call is placed

1.2 What is ISDN?

The Integrated Services Digital Network (ISDN) is a high-speed digital phone line that can carry voice or data. ISDN has the following capabilities:

- Basic Rate Interface

  ITU-T (formerly CCITT) standards committee allows service providers to offer two 64 kbps channels to customers as standard access along with a 16 kbps signaling channel. The two B channels carry voice and data, and the D channel provides signaling for services. Though becoming rare, it is the option of the service provider to deliver two 56 kbps B channels, with the D channel created by the two 8 kbps segments removed from the original 64 kbps B channel.

- Primary Rate Interface

  A Primary Rate Interface consists of 30 64 kbps B channels (23 in USA) and one 64 kbps D channel for signaling. While basic rate access is the ISDN equivalent of the simple telephone connection, larger customers may require access to many more connections for a PABX or computer bureau type of service. For this reason, existing interfaces within the ISDN have been modified to provide 1.536 Mbps in North America and 2.048 Mbps in Europe. These consist of multiple 64 kbps B channels with one 64 kbps D channel.

- Switch Characteristics

  When attaching a device to an ISDN network, it is important to know the switch type that you will be connecting to, because national and international ISDN standards have been slow to materialize. Some of the earlier switches (in particular the Nortel DMS100) used their own variations on the Q.931 signaling standards, and offer limited services to the user. Compatibility between your equipment and the switch is of vital importance. For example, a Nortel DMS100 can handle a maximum of two ISDN devices per line, with one attached to each B channel.

  In the USA, devices are given a Service Profile IDentifier (SPID), which is used to determine what services, and hence what bearer capabilities, the device can access. It is important that this SPID is configured correctly before any device will work. SPIDs are *not* used in Europe; MSNs are the closest equivalent.

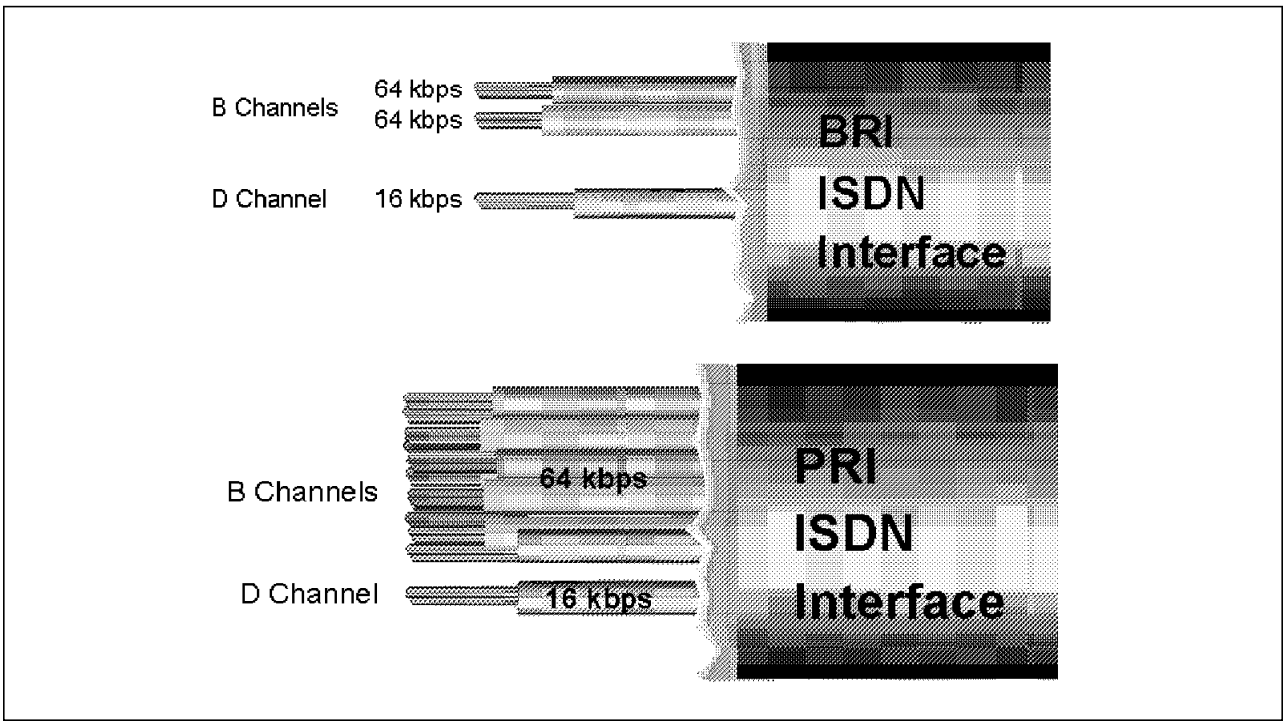


Figure 2. Basic Rate Interface ISDN vs Primary Rate Interface ISDN

1.3 What Is T1/E1?

T1/E1 terminology can be confusing since the terms are often used interchangeably. The correct definitions are as follows:

T1 is a 1.544 Mbps connection of 24 (64 kbps) circuits or channels, which are digital connections. The 8235-I40 can use a T1 as a fat pipe in a LAN-to-LAN type connection. Channelized T1 is a T1 line that has been provisioned so that the 24 channels can be accessed individually. The 24 channels can support analog calls, although it is still a digital connection (that is, digitized analog). The 8235-I40 supports channelized T1.

E1 is the European version of a T1 but consists of 32 (64 kbps) circuits or channels that provide an overall bandwidth of 2.048 Mbps. E1 (without ISDN) can be used as a fat pipe by the 8235-I40 in LAN-to-LAN type connections. Channelized E1 would be equivalent to channelized T1 where 32 channels are provisioned so that the 32 channels can be accessed individually. The 8235-I40 supports channelized E1.

Channelized T1 is the ability to allocate individual calls (digitized analog calls) over each of the 24 channels of a T1 line. For the 8235-I40, this means that a customer can connect a channelized T1 line to an I40 and be able to have 24 independant callers dial-in to the box at the same time (one caller per channel).

1.4 What Are CSU and DSU?

A Channel Service Unit (CSU) is a device used to connect a digital connection, such as a T1/E1 being delivered from a telephone company to network access equipment located on the customer premises. The CSU also generates the digital signal to boost clarity. Some devices include an integrated CSU/DSU.

A Data Service Unit (DSU) is a device used to connect a computing device (Data Terminal Equipment) to a digital phone line to allow for fully digital communications.

1.5 What is Robbed-Bit Signaling?

Robbed Bit is a concept used on T1 trunk signaling. It describes the signaling protocol used between the 8235 DIALs Switch and the central office telephone company switch for use with a T1 line. A T1 line with robbed-bit signaling provides 24 user channels or time slots for data transmission. With robbed-bit signaling, every channel on the T1 line carries both call signaling and call data. T1 lines use the least-significant bit of every sixth and twelfth frame of the data stream for signaling (to indicate the call control information, such as connect and disconnect commands). Typically in North America, each T1 robbed-bit channel provides a data throughput speed of 56 kbps.

You must select the supervision variant type used for the T1 signaling. Options are shown in Table 2.

Table 2 (Page 1 of 2). Supervision Variant Types used for T1 Signaling

Supervision Variant	**Description**
Wink-Start	E&M Wink Start signaling
Delay-Dial	E&M Wink Start signaling that allows the user to accept a standard delay in dialing after the central office switch confirms to the 8235 DIALs Switch that dialing can commence.
Immediate Start	E&M Wink start signaling in which dialing is assumed to begin immediately after the acknowledgment is received by the 8235 DIALs Switch.
Loop-Start	A protocol for dialing over lines that do not use E&M Wink Start signaling. Loop-Start requires AT&T switch type 5ESS. See AT&T publication 43081.
Ground-Start	Another protocol for dialing over lines that do not use E&M Wink Start signaling. Ground-Start requires AT&T switch type 5ESS. See AT&T publication 43081.
FXO Loop-Start	For use by the 8235 DIALs Switch when it is to be configured as a Foreign Exchange Originating device on a Loop Start line. FXO Loop-Start requires AT&T switch type 4ESS or 5ESS. To be compatible with the 8235 DIALs Switch, the central office switch must be configured to be a Foreign Exchange Subscriber device.
FXO Ground-Start	For use by the 8235 DIALs Switch when it is to be configured as a Foreign Exchange Originating device on a Ground Start line. FXO Ground-Start requires AT&T switch type 4ESS or 5ESS. To be compatible with the 8235 DIALs Switch, the central office switch must be configured to be a Foreign Exchange Subscriber device.

Table 2 (Page 2 of 2). Supervision Variant Types used for T1 Signaling

Supervision Variant	**Description**
Loop-Start with wink	A variation on the E&M Wink Start protocol (not commonly used). Loop Start with wink requires switch type 4ESS.
Loop-Start no wink	A variation on the E&M Wink Start protocol (not commonly used). Loop Start no wink requires switch type 4ESS.
Ground-Start with wink	A variation on the E&M Wink Start protocol (not commonly used). Ground-Start with wink requires switch type 4ESS.
Ground Start no wink	A variation on the E&M Wink Start protocol (not commonly used). Ground Start no wink requires switch type 4ESS.

Chapter 2. 8235-I40 Description

The 8235-I40 is a high-capacity remote networking switch which brings award-winning 8235 DIALs functionality to a new cooperative multiprocessing architecture with industry-standard high-speed buses and extensive call control capabilities. Uniquely designed to meet the needs of end-users, corporate enterprises and carriers/Internet Service Providers, the 8235-I40 DIALs Switch supports all major remote networking functionality including a flexible range of security choices, superior manageability, single user dial-in, dial-out for LAN based users, and LAN-to-LAN routing for branch/home office connectivity.

The 8235-I40 is an enterprise-level device that attaches to a LAN and has a high-speed communication line such as a T1, E1 or Primary Rate ISDN (PRI) interface. Unlike competitive offerings built on legacy architectures such as backbone routers, terminal servers, modem banks, and IP call terminators, the 8235-I40 DIALs Switch is designed from the ground up to meet the distinct requirements of large-scale remote networking with a unique combination of proven 8235 DIALs technology, data switching, PBX-style call control, and client/server system management.

The 8235-I40 adds T1 and E1 interfaces to the scope, but stays compatible with the existing client software. The IBM 8235-I40 has the potential to rival and surpass services offered by Internet providers.

2.1 Product Description

The 8235-I40 supports large numbers of dial-in users via analog or digital services for dial-up to either an Ethernet or token-ring LAN. With the I40, dial-in users can make direct connection to PRI ISDN and T1/E1 lines from their regular analog and ISDN lines at the home or on the road. The call handling (switch) functions are handled by the I40 switch. With the 8235-I40, as with the base 8235 models, the dial-in clients are supported for multiple protocols (IP, IPX, NetBios, LLC and AppleTalk) as well.

It is populated with cards via a Peripheral Component Interconnect (PCI) bus just like a PC. The base unit houses two cooling devices (fans) and a board with a PCI bus (133 Mbps data throughput) to receive up to 11 cards.

The 8235-I40 is positioned as the premier enterprise remote LAN access switch and the Internet Service Provider′s (ISP) access server, providing high connectivity and performance for remote access to the customer′s network resources or the Internet. With a single unit, the LAN administrator or ISP can handle over 70 users dialing in, and multiple units can be managed from single location, accommodating hundreds of dial-in analog and digital calls. This model reduces line costs and operational costs by providing high connectivity and support for virtual connections. It completes the 8235 product line from the small office to the large enterprise.

2.2 Product Overview

The 8235-I40 has been available for Ethernet networks since May 1996, with token-ring support added in August 1996, and now in 1997 all functions from the base models are supported.

- Physical specifications
  - Width: 440mm (17.3 inch, for mounting in 19 inch racks)
  - Depth: 406mm (16 inch)
  - Height: 178mm (7 inch)
  - Weight: 14kg (30 lb)
- Operating environment
  - Temperature: 10 (degs) to 40 (degs)C or 50 (degs) to 104 (degs)F
  - Relative humidity: 20% to 80%
  - Wet bulb: 29.6 (degs)C or 85.3 (degs)F
  - Electrical power: 0.5 KVA
  - Noise level: 29 dBa
  - Starting current: 3.5 ampere
- Operating capabilities
  - Full compatibility with other 8235s
  - Single Management facility
  - Reduce Network traffic (routes for IP, IPX and bridges for NetBIOS/LLC)
  - T1/E1/ISDN PRI Adapters
  - Digital Modem Card (DMC - contains 12 modems)
  - Chassis assembly (includes power supply, fans and planar board)
  - Ethernet and token-ring CPU/Network Cards
  - Customer setup box (CSU)
  - One-year warranty
- Function Capabilities
  - Multiprotocol support (bridges and routes)
  - Multiplatform support (DOS, OS/2, AppleTalk ARA 2.0, Windows 3.X, Windows 95, Windows NT)
  - Dial-in, Dial-out, LAN-to-LAN
  - Wide range of security choices (8235 specific and third party - RADIUS)
  - Comprehensive and easy-to-use management (for device using the 8235 Management Facility, and centralized using NWays Campus Manager)
  - T1/E1 voice and Primary Rate ISDN signaling
  - Channel Aggregation (not bonding)
  - Can receive up to 96 analog and digital calls
  - Automatic call discrimination

2.3 Hardware Overview

Here we discuss the hardware components of the I40, They are:

- Chassis
- Slots
  - Slots 1-3, dedicated, PCI only
  - Slots 4-11, multipurpose, ISA or PCI
- Cards
  - CPU card
  - LAN card (Ethernet or token-ring)
  - WAN cards (single, dual, and quad (T1 only), T1 and E1)
  - Modem card (DMC)
- Bus connections between the cards

2.3.1 Chassis

The 8235-I40 has the size and shape of a desktop PC (rack-mountable) and is populated with cards. This base unit mainly houses some front-panel LEDs, an auto-detecting power supply, cooling devices and a board with a PCI bus (133 Mbps data throughput) to receive up to 11 cards. These cards actually carry out the functions of the machine. For a view from the top refer to Figure 3.

There are two groups of slots: 1-3 and 4-11.

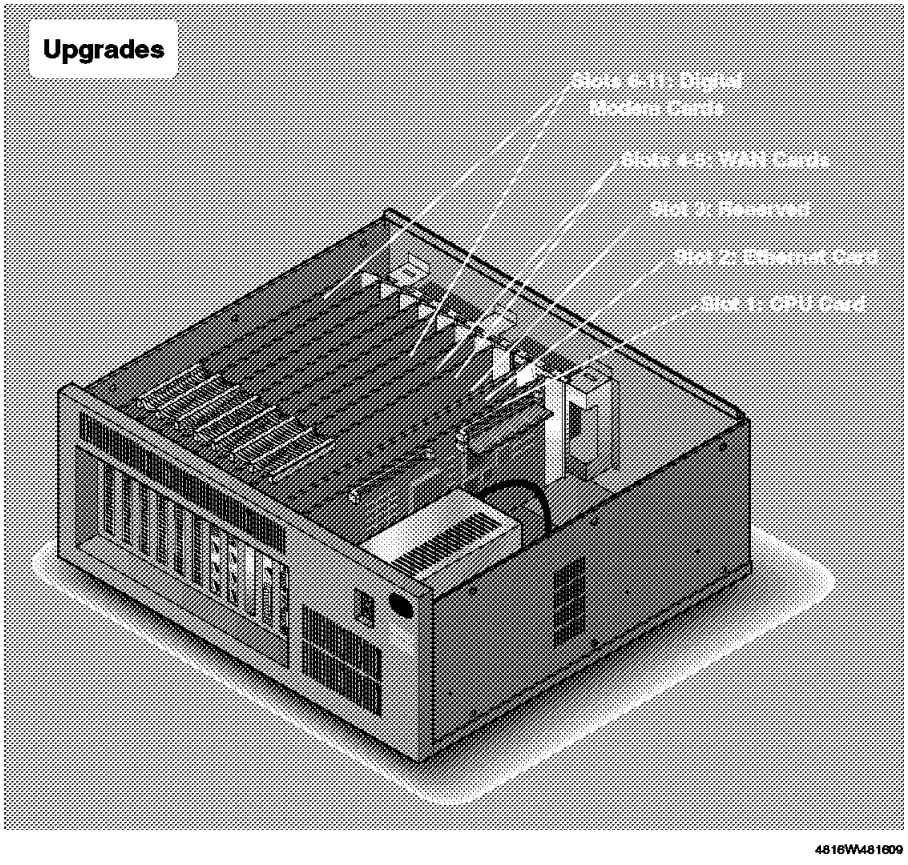


Figure 3. 8235-I40 Top View with Upper Cover Removed

2.3.2 Slots 1-3

These slots are PCI only and for dedicated purposes only:

- Slot 1 must be equipped with the main CPU card, carrying the main processor and its memory.
- Slot 2 must take the LAN adapter either token-ring or Ethernet. The token-ring adapter is a 16/4 autosense PCI card. The Ethernet adapter has two connectors: 10Base-T and AUI (10Base-5). Only one of these interfaces on the Ethernet card may be used at a time.
- Slot 3 is reserved for future use and must be empty.

2.3.3 Slots 4-11

These slots each have a PCI connector and an ISA connector, so either a PCI card or an ISA card may be installed into these slots. For cooling reasons (fan airflow) the ISA WAN cards (T1 or E1) must be installed in slots 4 and 5. The remaining six slots can be used to install DMCs (Digital Modem Cards).

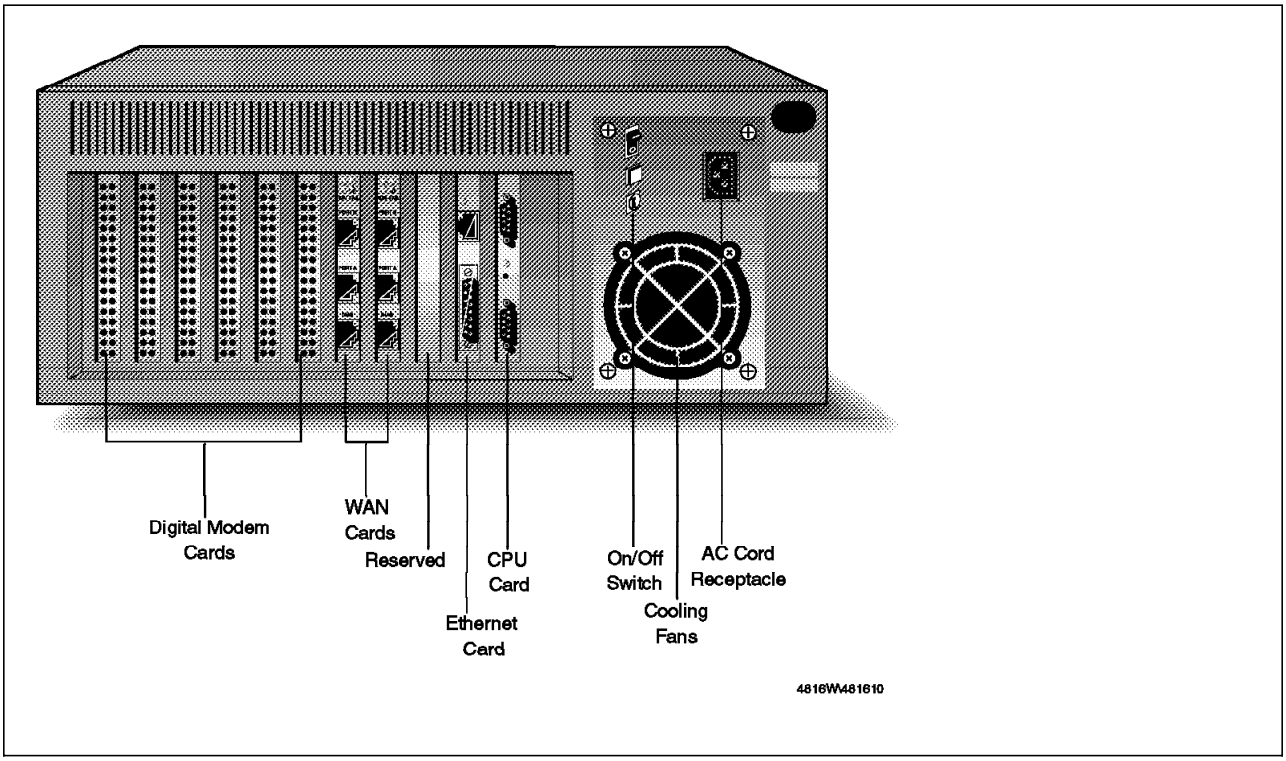


Figure 4. 8235-I40 Front View - Sample Configuration

Note: There is no On/Off switch on the I40.

2.3.4 Cards

There are four types of cards. See Figure 2 for their placement and faceplate layout.

1. The CPU card carries the main processor, a Motorola 68060, two asynchronous serial ports for out-band management, and the system memory. There are several types of memory, as follows:
   - Flash memory. One part of this is permanent VROM (PVROM); this can only be replaced by a flash upgrade. The other part is upgradeable VROM (UVROM); it holds the firmware VROM and image. This can be replaced by selecting **Clear and Download** from the Management Facility.
   - Dynamic RAM (DRAM). This is a special 32-bit, EDO, 50 ns memory. There is 4 MB on board; 4 MB SIMMs can be added up to a total of 64 MB. The box may be shipping with some SIMMs already installed.

     Attention

     Never attempt to use any off-the-shelf memory here. This is likely to be destructive.

VROM and image code are loaded here for execution. Transmits to and receives from the LAN card are stored here and all data buffering takes place here.

- Static RAM (SRAM). This stores data that is to be retained when the machine is powered off. Among these are configuration data, the IP address of the device and the user list. This memory is battery-backed.

Figure 5 shows a sample display provided by the Management Facility Device Info function, giving details on these memory types.

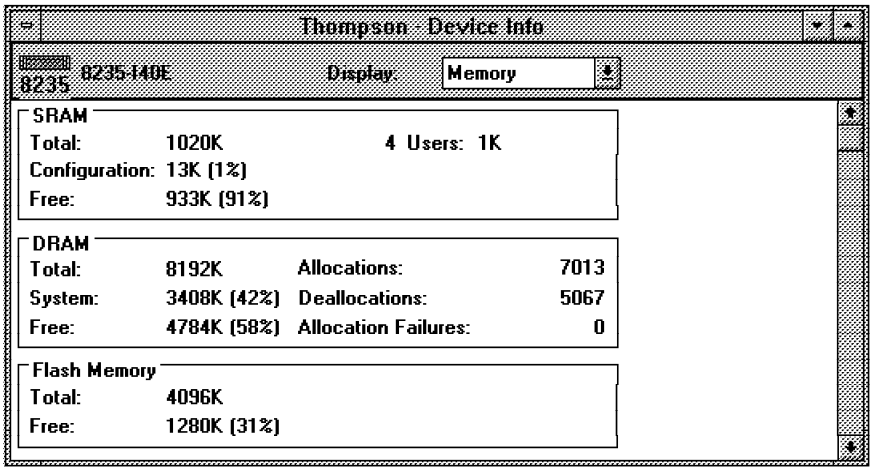


Figure 5. Device Info Page - Memory

2. The LAN card must either be the Ethernet or token-ring card. Unlike other models of the 8235, the LAN connection is not a fixed, built-in interface, but a removable, replaceable card.
3. There are several different types of WAN cards. They all have multiple RJ45 connectors at the back.
   - Quad T1

     Card with software-selectable CSU/DSU and channelized T1 support
   - Dual PRI/T1 interface

     Card with software-selectable CSU/DSU and channelized T1 support
   - Dual PRI/E1 interface

     Card with E1 service with PRI ISDN
   - PR Single PRI/T1 interface Card supporting either digital or analog connection with CSU/DSU
   - PR Dual PRI/T1 card Card supporting either digital or analog connection with CSU/DSU
   - PR Single E1 (Primary Rate Interface - Single E1 WAN card)

     This card has one physical E1 interface. It does not required a CSU; however, it has straps where the CSU could be placed. These straps must not be removed.
   - PR Dual E1 (Primary Rate Interface - Dual E1 WAN card)

     This card has two physical E1 interfaces. It does not require CSUs; however, it has straps where the CSUs could be placed. These straps must not be removed.

   Note: For the PR series of cards, there are three ports on the face of the card, marked Port B, port A and Diagnostics Port from top to bottom. Depending on the type of card (single or dual), either port A is inactive and only port B is active (single) or both ports are active (dual). Port A corresponds to line 1 in the WAN card configuration page; port B corresponds to line 2. Consequently, a single WAN card has only a line 2, not a line 1. The Diagnostic port is not used for data transfer and is not described here.

4. There is one type of Digital Modem Card (DMC). It has a PCI connector. It carries 12 Rockwell V.3 chipsets, accounting for 12 analog modems. Each modem ships supporting a 28.8 kbps (V.34) connection. The card has a dedicated microprocessor and is flash-upgradeable to 33.6 with Version 4.5.

2.3.5 Bus Connections

In addition to the Peripheral Component Interconnect (PCI) bus, there is a second connection, only between the WAN cards and the DMCs. This is the Multi-Vendor Integration Protocol (MVIP) flat cable bus. The MVIP connectors are located near the top edge of these cards, so the cable runs across the top of the vertically inserted cards in slot 4 to 11 (see Figure 6).

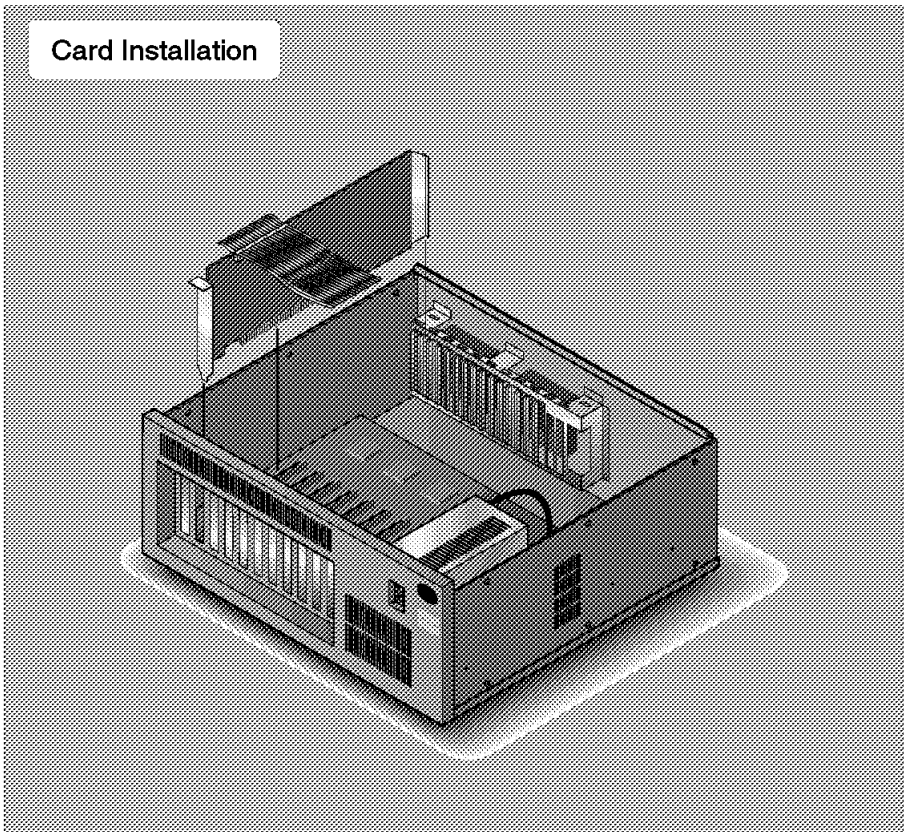


Figure 6. 8235-I40 Card Insertion (MVIP Flat Cable)

MVIP is an industry-standard TDM bus technology, carrying 256 64 kbps full-duplex channels, yielding 16 Mbps overall throughput capacity. This MVIP bus is being used for communication between DMCs and WAN cards for analog calls that require modem processing. When an analog call comes in, the WAN card is capable of detecting this and routing it to a modem. The modem (one out of 12 residing on a DMC) does the DSP processing and then, in turn, routes the data stream, which is now digital, to the main CPU over the PCI bus. When a digital call comes in, the WAN card directly forwards the data to the main CPU. This way there is no additional impact on the PCI bus imposed by analog calls as compared to digital calls, even though analog calls require more processing. (See Figure 7 for the data flow.)

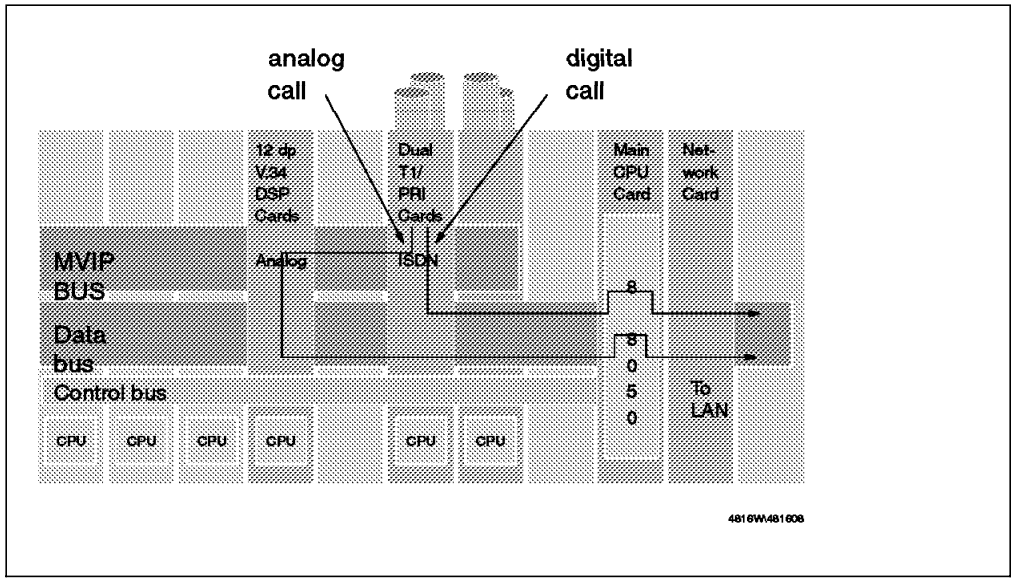


Figure 7. 8235-I40 Data Flow

2.4 Shared Memory Allocation

Care was taken in both the hardware and software design of the 8235-I40 to ensure that the memory on the I/O cards could be accessed by other cards in the box. This means that the main processor can write directly into the memory of one of the I/O cards, such as to add a PPP packet header to data received from the LAN interface. This data can then be sent directly to one of the WAN boards via the PCI bus, without ever entering main memory. The only work needed by the main processor is adding the header and sending the messages (not the data) to the cards to arrange the DMA transfer. This offloads work from the main processor allowing it to process more transactions. It also lowers the latency of data transfer, as data is rarely copied inside the box from one part of the product to another. Here are the details:

- 4 MB flash RAM (not PC SIMM)
- 8 MB DRAM (expandable to 64 MB)
  - 4 MB on board (good for first 30 calls, store while executing the callup after setup)
  - 4 MB SIMM
  - Controller runs at 50Mhz
  - VROM and Image
  - Ethernet or token-ring transmit and receives
  - All data buffering
- 1 MB SRAM (expandable to 4 MB) stores:
  - Code for Ethernet and token-ring, T1/PRI, E1/PRI, DMC
  - Configuration
  - IP address
  - User list
  - Battery backed up
- EPROM (MAC address assigned to CPU)

  Note: This MAC address is only used for the Ethernet card. The token-ring card has its own MAC address and does not use the address assigned to the processor card.

2.5 Feature

The 8235-I40 offers the following features.

2.5.1 WAN Communication Features

1. T1/PRI
   - 23 digital or digitized analog calls
   - Four T1/PRI interfaces per 8235-I40
2. E1/PRI
   - 32 digital or digitized analog calls
   - Three E1/PRI interfaces per 8235-I40
3. Analog - Modems on DMC (up to 84)
   - Automatic Call Discrimination on ISDN line provisioned to accept analog calls
4. Dial-In
   - Asynchronous (modem) Dial-In, PPP, ARA, TCP/IP, IPX, NetBEUI, 802.2/LLC, SLIP, or Terminal Server
   - Synchronous Dial-In using PPP
   - Multilink PPP (MP)
   - LAN-to-LAN Originate and Answer
   - LAN-to-LAN Answer with MP

2.5.2 LAN Communication Feature

- Only one LAN connection per 8235-I40
- Ethernet or token-ring

2.5.3 Management and Security Features

- 8235 Security and other third-party (SecurID, TACACS, TACACS+, Digital Pathways Server, etc.)
- 8235 Management Facility
- Remote Authentication Dial-In User Service (RADIUS)
- NWays Campus Manager V1.1 (Windows NT and AIX for I40)

2.5.4 Unsupported Features

- AppleTalk Zone Filtering
- Leased Line Operation (US and European)
- MP without locally configured telephone numbers

2.5.5 Cards/Modules

There is a difference between the Ethernet and token-ring CPU cards. The CPU card has a slot that contains a SIMM which is either a token-ring or Ethernet SIMM. The SIMM is the only difference on the CPU card. This SIMM is nonstandard size and is located at the rear of the card near the top; it is normally referred to as the flash.

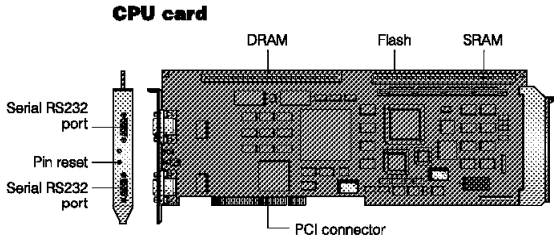
If you want to convert a token-ring I40 to an Ethernet I40, you would *have to change* the LAN card *and* the SIMM on the CPU card.

European and North America differences: There is a difference in the way the phone networks treat digitized analog data. The North American method is called *mu-law* (Greek letter *mu*); the European method is called *A-law*. The DMC card has a jumper to set this, shown on the diagram of the DMC card in the next section. It comes set for *mu-law*, so Europeans must change it. In addition, there is a parameter in the Additional Configuration page. We set it like this:

```
[PRIDriver]
AlawAnalog=true
```

2.6 The Picture of the Cards/Modules of 8235-I40

The following are examples of the 8235-I40 cards/modules:



CPU Card - Note: Need Flash change for upgrade to token-ring

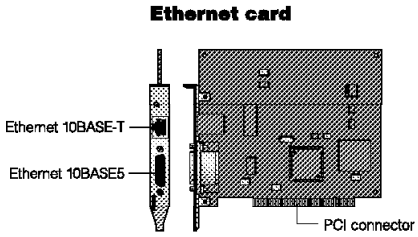


Figure 8. LAN Card (Ethernet) One LAN type per 8235-I40

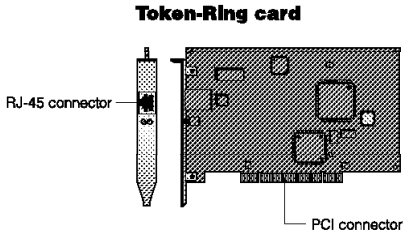


Figure 9. LAN Card (Token-Ring) - Auto senses ring speed

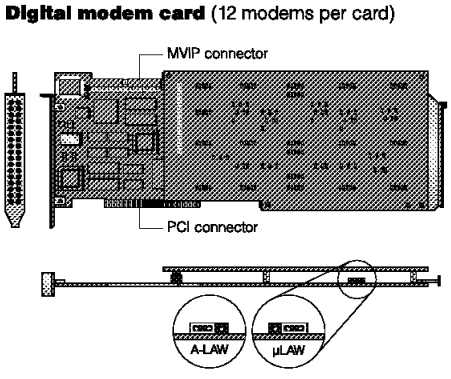


Figure 10. Modem Card - Up to 7 (12 modems per card, only 6 supported) per 8235-I40

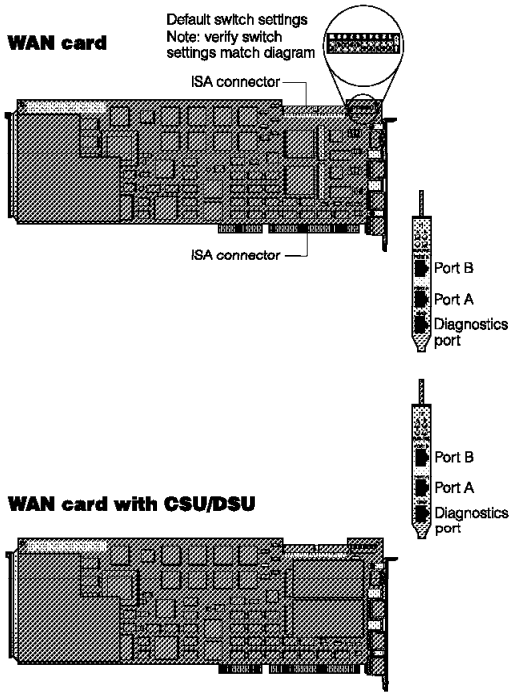


Figure 11. WAN Card

Note: Switch settings must match the pattern shown above, or the card may not be recognized by the 8235-I40 as a valid adapter.

2.7 ISDN Switches and Adapter Support

In the Switch area, you must specify two parameters (Type and Variant) that identify the type of switch, as follows:

Note: The Type and Variant parameters apply to ISDN only; the signaling type must be set to PRI.

- In the Type parameter, select a switch type from the list. The following table describes the available options; 4ESS is the default switch type.

Table 3 (Page 1 of 2). 8235-I40 T1/E1 Switch Types

Switch Type	Description
4ESS	AT&T 4ESS (Lucent Technologies)
5ESS	AT&T 5ESS (Lucent Technologies)
DMS100	Northern Telecom DMS100 (Nortel)
DMS250	Northern Telecom DMS250 (Nortel)
MD220T1	Ericsson MD 110 for T1 (US)
MD110E1	Ericsson MD 110 for E1 (International)
EWSD	Siemens EWSD (US)
NTT	Nippon Telephone and Telegraph (Japan)
EuroISDN	Most European Switches

Table 3 (Page 2 of 2). 8235-I40 T1/E1 Switch Types	
Switch Type	**Description**
ITR6	Germany (being phased out for EuroISDN)
VN4	France
Others	Any unknown switch conformant to CCITT standards

- In the Variant parameter, select the Q.931 national or vendor-specific code set extension used with the telephone switch indicated by the switch Type parameter. The following table describes the available options; ATTCustom is the default Variant.

Table 4. 8235-I40 T1 Switch Variants	
Variant	**Description**
ATTCustom	In publication AT&T PUB 41449
NTICustom	In publication Northern Telecom NIS A211-1
NAT1	Bellcore National ISDN-1 for BRI
NAT2	Bellcore National ISDN-2
JATE	JATE-compatible as define for INS-1500 for Japan
NET5	NET-5 ETSI standard for PRI in Europe
1TR6PRI	1TR6 standard for PRI for Germany
VN3	VN3 for France
ITU-T	General ITU-T (Former CCITT) Q.931 conformance
Q933	ITU-T Q.933 based on Frame Relay Forum implementation agreement
Q933T123	ITU-T Q.933 supporting T.123 subset of D-channel messages

- The following table identifies which switch types and switch variants are used together. This means if you will use a specific switch type, check the switch variant also to make sure the two selections are compatible. For example, if the DMS110 is chosen for switch type, the switch variant should be NI-2 or NT Custom.

Table 5 (Page 1 of 2). Valid Switch Type and Variant Combination	
Switch Type	**Switch Variant**
AT&T 4ESS	National ISDN-2 or AT&T Custom
AT&T 5ESS	National ISDN-2, AT&T Custom, or Q.933/T.123
Nortel DMS110 & DMS250	National ISDN-2 or Windows NT Custom
MD-110 (T1 or E1)	General ITU-T
Siemens	NET-5, ITR6 (PRI)
NTT	JATE (INS-150), General ITU-T

Table 5 (Page 2 of 2). Valid Switch Type and Variant Combination	
Switch Type	**Switch Variant**
Any switch conforming to ITU-T standard	NET-5

The following are the terminal adapters supported for 8235-I40 serial ports:

- Motorola BitSURFR
- Motorola BitSURFR Pro
- ADTRAN ISU Express
- ADTRAN ISU 128
- 3Com Impact
- Hayes ISDN TA 2.0
- US Robotics Courier I-modem

Note: Other ISDN TAs may function with the I40 serial ports if they respond properly to AT commands.

2.8 Software Ship Group for I40 Switch

The following items are offered to customers:

1. Hardware
   - Base Chassis
   - Cards/Boards/Module, consisting of CPU, LAN, DMC and WAN cards
   - Ethernet or token-ring
   - Shielded power cord
   - Telescoping rack slides and mounting brackets
   - Wrist strap (grounding)
   - MVIP cable
2. Software
   - 8235 Management Facility Version 4.53
   - 8235 DIALs Client:
     - OS/2 Client V.4.52
     - Dial-In for DOS V.4.02
     - Dials for Windows V.4.52
     - Windows 95 (IBM DIALs V.5.01 and 8235 Security pack for Windows 95 v1.30)
   - 8235 Dial-Out Client:
     - DOS V.4.02
     - OS2 V.4.52
     - Microsoft (Windows, Windows 95 and Windows NT V.5.0)
     - LAN Connect 4.0 (Windows and MAC)
3. Documentation
   - CD-ROM 85H9008 (also with upgrade kit)
   - 8235-I40 Hardware Installation Map
   - 8235 DIALs-In Access to LANs Servers for Token-Ring and Ethernet Installation Guide
   - Quick Reference (8235 Dial-In and 8235 Install/Setup)
   - 8235-I40 Service Guide Information Card. It consists of 8235 Identification, Contact Information, Slot Information, CPU Card LED States, Ethernet Card LED States, T1/E1 WAN Card LED State, Where to Call, Technical Support and more.

Chapter 3. 8235-I40 Call Handling

This chapter explains how Call Discrimination, Digital Analog Processing and Call Flow work.

3.1 Call Discrimination

The I40 Access Switch use a PRI interface to connect to a local exchange switch in order to receive modem and ISDN calls. The I40 can automatically distinguish between incoming ISDN calls and incoming modem calls.

The I40 receives calls from ISDN users through one or more ISDN B channels that are transported over a PRI line. These calls are purely digital and are presented to the I40 using High Level Data Link Control (HDLC). The I40 can receive calls from modem users as *digitized analog* calls. In other words, the modem's analog carrier is sampled using PCM and transported to the I40 over an ISDN B channel. Analog calls can come in over an ISDN PRI line and can be autodiscriminated and sent to one of the analog modem cards.

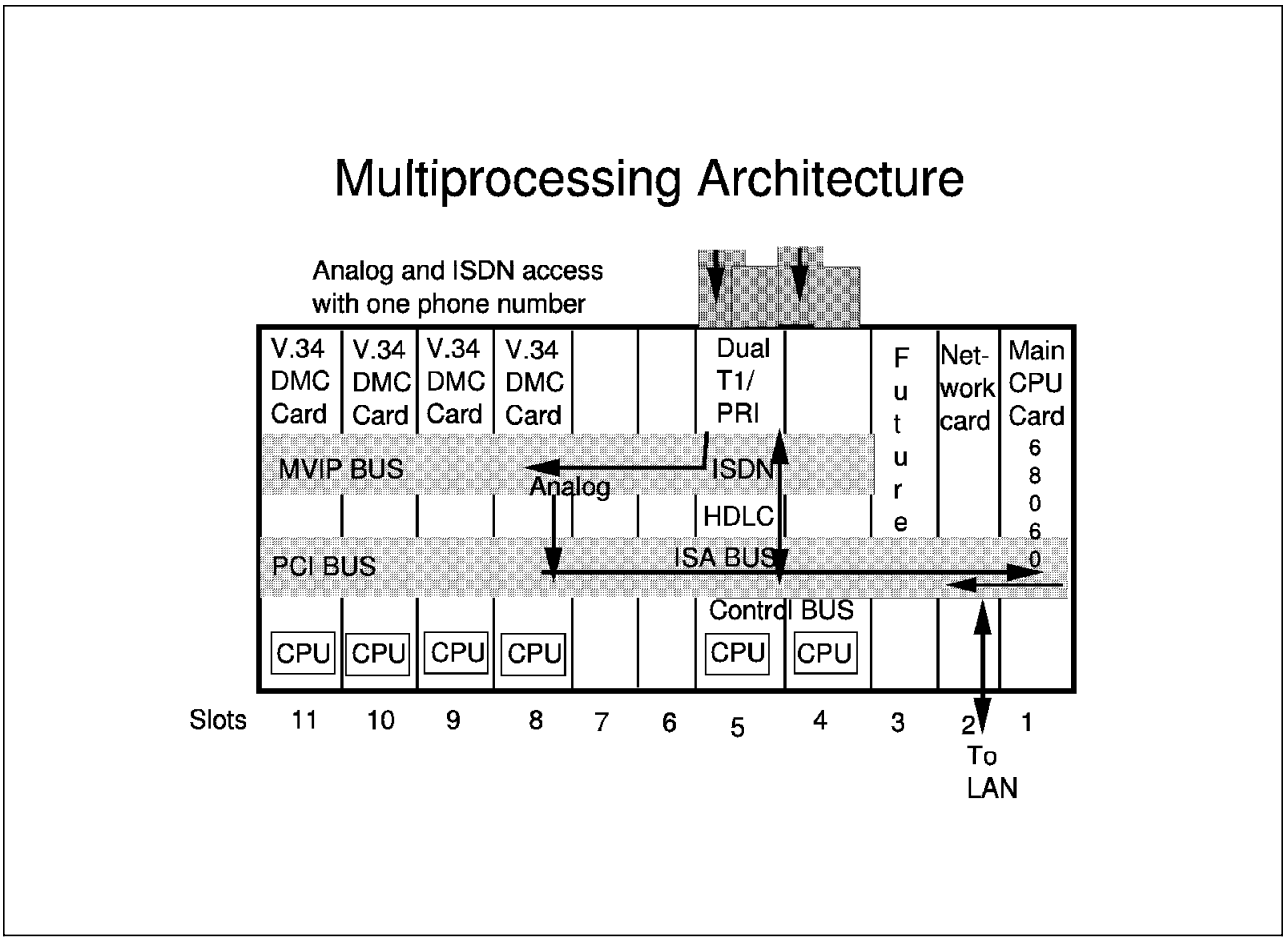


Figure 12. Call Handling on the 8235-I40

Table 6. Pure Analog Connections

# Single T1/E1 Cards	# Dual T1/E1 Cards	# Modem Cards (12 Modems per card)	# Calls Handled
1		1	12
1		2	24
2		3	36
2		4	48
3		5	60
	1	1	12
	1	2	24
	1	3	36
	1	4	48
	2	5	60
	2	6	72
1	1	3	36
1	1	4	48
1	1	5	60
1	1	6	72

Table 7. Pure Digital Connections

# Single ISDN-P Cards	# Dual ISDN-P Cards	# Calls Handled in US	# Calls Handled in Europe
1		23	30
2		46	60
	1	46	60

Table 8. Mixed Analog & Digital Connections

# Single T1/E1	# Single ISDN-P	# Dual T1/E1	# Dual ISDN-P	# Modem Cards	# Digital Calls in US	# Digital Calls in EMEA	# Analog Calls
1	1			1	23	30	12
1	1			2	23	30	24
2	1			3	23	30	36
2	1			4	23	30	48
	1	1		1	23	30	12
	1	1		2	23	30	24
	1	1		3	23	30	36
	1	1		4	23	30	48
		1	1	1	23	30	12
		1	1	2	23	30	24
		1	1	3	23	30	36
		1	1	4	23	30	48

Table 9. Quad T1 Card Support

# Quad T1 Cards	# Modem Cards (12 Modem)	# Calls Handled
1	6	72

Note: The quad T1 card can support 96 connections; however, only seven modem cards are supported. To fully take advantage of the quad T1 card, we would need modem cards with higher density.

3.2 Digitized Analog Processing

The CPU expands the data using STAC decompression (if compressed on the dial-in side), determines where the data goes, and routes it out the LAN card.

The I40 Switch is able to differentiate between incoming ISDN and analog calls and handles them with one phone number. For example, when an analog call comes in to the PRI card, the I40 is able to detect that it is from an analog source by the data on the D Channel. The call is then switched via the high-speed MVIP bus to an available digital modem on one of the DMC cards. The DMC then converts the PCM digital data to analog and passes it to the modem. The modem then converts the analog data to digital data and buffers it in on board memory. The CPU then pulls the buffered data across the PCI bus in a parallel data stream to another buffer, which is then sent to the LAN card for routing.

If the incoming call is ISDN, it is processed by the HDLC controller on the PRI card and then switched out to the network via the PCI and main CPU.

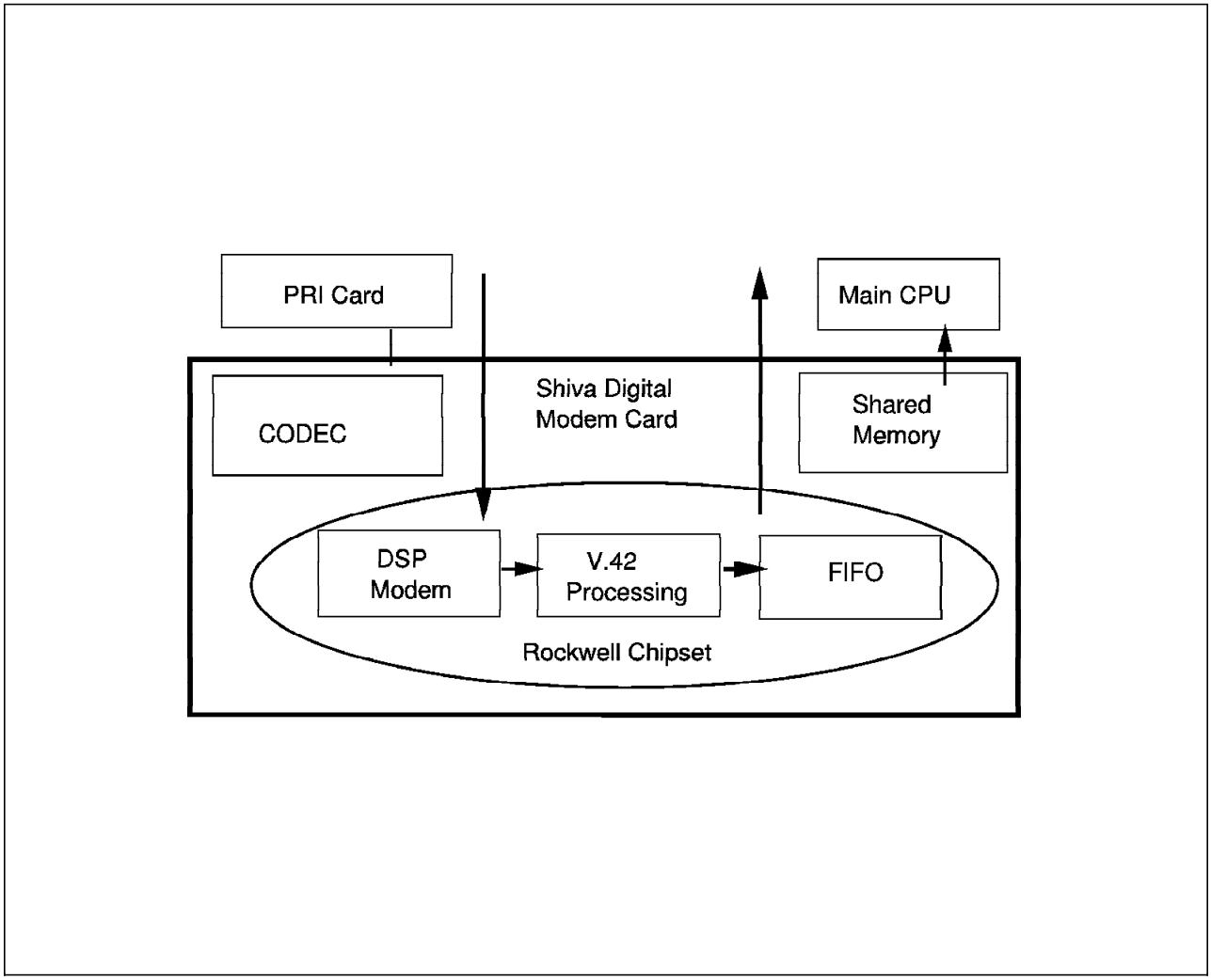


Figure 13. Digitized Analog Processing on the 8235-I40

3.3 Call Flow

Digital call signaling (ISDN) includes information as to the call type (analog vs digital). The I40 looks at this signaling information to determine how to handle the call. If the signaling indicates that the call is an analog call (digitalized-analog to be precise), then the I40 allocates a modem to the call, routing it over the I40 MVIP bus. If the call signaling indicates that the call is digital, it is handled directly by the WAN card.

Attention

There are several limitations that may apply. The overall limitation is 72 concurrent calls (of which a maximum of 60 can be digital). The 8235-I40 support PRI only (8235-031/032 models can support BRI connections).

Chapter 4. Planning the 8235-I40 Installation

The installation of an 8235-I40 is not a simple task, but can be simplified if certain information is available when setting up the product. This chapter will give the information necessary to set up and configure the I40 for use.

4.1 Planning Activities

Total planning time is significantly reduced when the worksheets for line provisioning and site preparation are given to the customer when the order is signed.

These worksheets guide the customer through negotiations with their telephone company of choice. After the sheets have been completed, they can be submitted to the IBM Service Delivery representative who will implement the 8235-I40 solution. A conference call will be conducted with the designated customer representative to review the worksheet contents, then a date for installation can be set.

If this process is followed, the 8235-I40 can be installed in one hour, configured and tested within five hours. If the line is not provisioned correctly, the installation cannot continue and another date must be established.

4.2 Planning Categories

In the planning phase we will talk about all Installation Plan Categories. However, the most important one is the customer worksheet, which must be completed for a smooth installation.

- Site Information
  - Site name and address
  - Primary contact information
  - Secondary contact information
- Line Provisioning
  - Service Provider contact name and phone number
  - Telephone number for T1 and E1 service (analog modem or remote testing, would be Internet access or not, etc.)
  - Switch Type
  - Variant
- Security
  - IP address
  - Third Party, if desired
  - 8235-I40 Security
- General Configuration
  - PC or UNIX management
  - DHCP

  - IP and or IPX
  - AppleTalk
- BootP/TFTP Configuration
  - Operating System
  - Windows installed
  - IP address, Subnet mask
  - Router information
- Client Workstation
  - BRI line installed
  - BRI line provisioning
  - Protocols
  - OS
  - ARA or MACPP/MAC Slip version

  Plan for software installation and configuration before you install and configure the 8235-I40 Dials Switch software. Use the worksheet below to gather important site information.

  Not all sections of the worksheet must be filled in for the I40 to be set up properly. Fields needed for a minimal configuration are marked like **this** on the worksheet.

Table 10 (Page 1 of 2). Installation Plan Worksheet

Category		
Site Information	Site Name	
	Site Address	
	Address line 2	
	Address line 3	
	Primary contact name	
	Primary contact telephone number	
	Primary contact fax number	
	Primary contact cell telephone number	
	Primary contact e-mail address	
	Secondary contact name	
	Secondary contact telephone number	
	Secondary contact fax number	
	Secondary cell phone number	
	Secondary contact e-mail address	
Line Provisioning	Service provider contact name	
	Service provider telephone number	
	T1/E1/PRI telephone numbers	
	T1/ISDN PRI service	
	Phone number 2	
	Phone number 3	
	Phone number 4	
	Number of bearer channels/time slots on each line	
	Line 2	
	Line 3	
	Number of digits from the telephone company switch provided to T1/E1/PRI lines	
	If the PRI/T1 lines are not installed, date they will be installed	
Security	Type of third party used	SecurID, Digital Pathways, TACACS, TACACS+, RADIUS
	IP address if IBM User List Server	
	IP address of security server	
	UDP port of security	
	Radius Version	
	Novell NetWare Bindery server name	

Table 10 (Page 2 of 2). Installation Plan Worksheet		
Category		
General Configuration	Is the NetWare Bindery dial-in group defined on the server?	
	Do you have PC or UNIX management software?	
	IP address of I40	
	Subnet mask	
	Default router on the network	
	Are you using DHCP?	
	DHCP server address	
	IPX frame type	Ethernet 802.3, Ethernet 802.2, Ethernet II, Token-Ring, Token-Ring SNAP
	For AppleTalk networks, circle the mode you are using with the I40	End / Seed router / Conforming router
BOOTP/TFTP Configuration	What operating system is your BOOTP and TFTP server running	
	IP Address of the BOOTP server	
	Subnet mask	
	Do you currently use TFTP and BOOTP?	
	Is TFTP configured and working correctly?	
	Is BOOTP configured and working correctly?	
	Is the BOOTP server the same as the TFTP server?	
	Do the BOOTP server and the TFTP server reside on the LAN segment as the I40 Dials Switch?	
	Do the routers on the network support UDP helpers for BOOTP?	
Client Workstations	Do you have a BRI line installed for testing?	
	What type of BRI line provisioning do you have (1 or 2 B-CHANNELS, data, voice or both)?	
	What protocols on the dial-in client do you want to use?	IPX, IP, NetBEUI/LLC, ARA 2.0
	Client WS op.sys. version	
	ARA or MACPPP/SLIP Version	

4.3 8235-I40 Configuration Description

This section describes some basic items you have to be aware of when installing the 8235-I40. In addition, it shows some initial configuration panels used when configuring the 8235-I40 with the 8235 Management Facility program.

4.3.1 Type of Service

When you start working with the 8235-I40, you will have to know what service you need, T1 or ISDN.

- Tell the telephone company that you want a T1 line for analog calls or an ISDN line to support all digital calls or a combination of digital and analog calls, with all of the 24 channels provisioned for voice and data calls.

  Note: Fractional T1s or leased lines are not currently supported.

  The telephone company will give you a full 1.54 Mbps T1/PRI link that accommodates all 24 channels operating at 64 kbps. Two channels can be aggregated/multilinked together to get 128 kbps per connection instead of 64 kbps.

  For a T1 line, all 24 channels will be available for the calls. On the other hand, PRI lines need 1 channel (D) for signaling, call setup and tear down. Therefore, 23 B channels remain for ISDN or digitized analog calls.

- Decide if you will supply your own CSU (for T1) or purchase one from the telephone company. If you supply an external CSU, it should adhere to the national standard for ISDN support with RJ-48 USOC (ISO8877) connectors. There are many to choose from (IBM, Motorola and Racal to name three). You will need to configure parameters based on what the CSU requires.

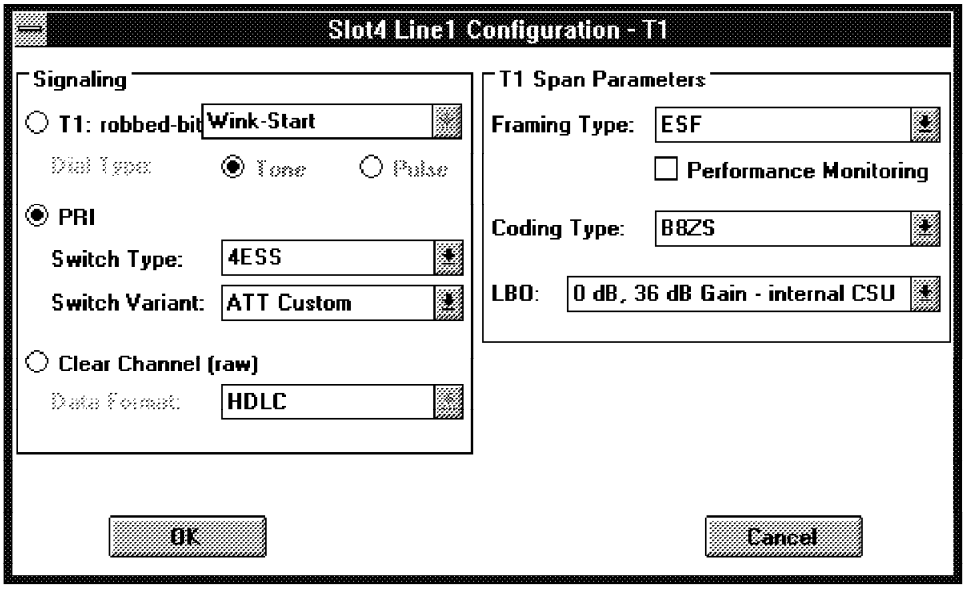
  Note: With external CSUs, the service provider will not notice any change in the line status if the I40 is unplugged, and disable the line.

  If you have purchased an I40 card with an integrated DSU/CSU, then the connector should be RJ-45. Customers should select WAN cards to suit their remote access environment.

  Note: 72 connections is an IBM test statement. The cards can actually handle more than 72 connections, but the maximum has not been determined. It is known that there will not be a performance impact on up to 72 connections (maximum of 60 digital). Clients using analog modems can continue to use the regular telephone service and analog modems. Some clients may also need to establish a Basic Rate ISDN (BRI) service and have the line provisioned for voice and data, and decide if they will need one or more phone numbers (aggregate/multilink their two B channels together to use 128 kbps instead of 64 kbps per B channel).

4.3.2 Sample of Basic Configuration

This Configuration Page (see Figure 14 on page 34) allows you to enable the T1 line, and the Signaling Type will determine if this card will be used for a T1 line (Robbed Bit) or as ISDN over T1 (PRI). Below is the sample.



ISDN (shown as PRI for ISDN)

Figure 14. Enable the Line for T1 robbed bit or

After configuring the line properly for the WAN card, it is now necessary to add a Phone Group to bind to this WAN link. In configuring the Phone Group, select protocols that will be supported in this Phone Group, whether to enable virtual connections, Datalink (check HDLC for PPP access, and Shell for user access), and Call Type (Use Force Call Type and select the type of calls supported on the WAN card to answer or select Use Switch's Call Type for the WAN card to answer digital or analog calls and autodiscriminate.

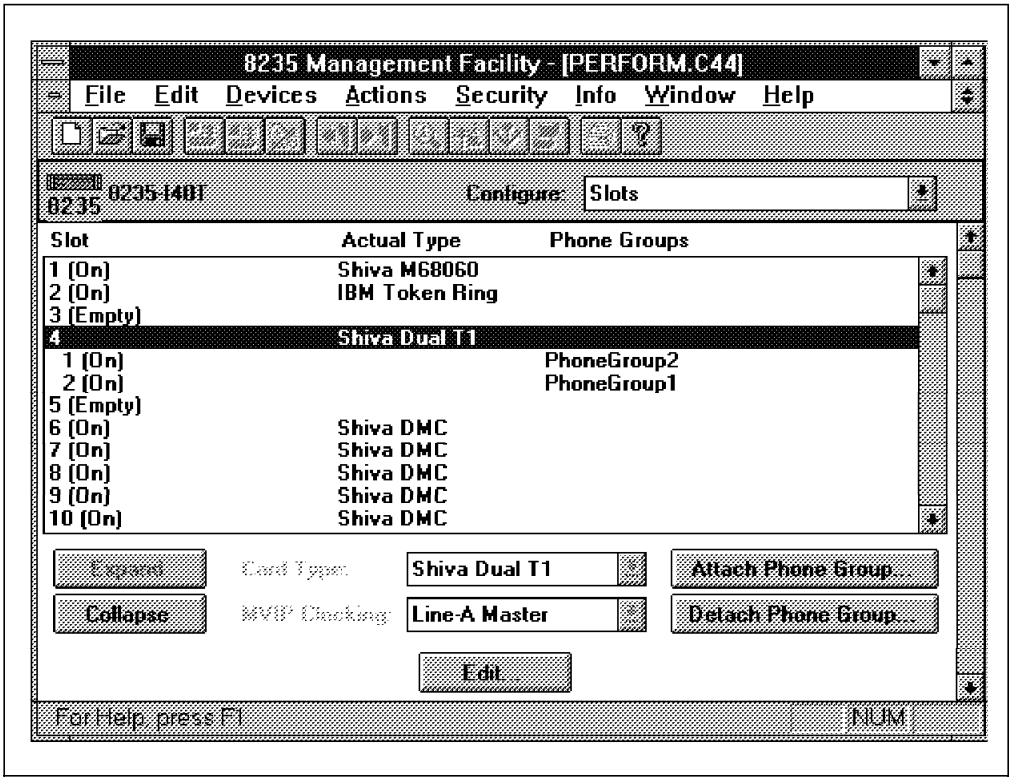


Figure 15. Attach Phone Group

Note: This next screen allows you to select the number of timeslots/channel to be used in PhoneGroup2 for the card in slot 4 on line 1, which is configured for signaling on a PRI T1 line.

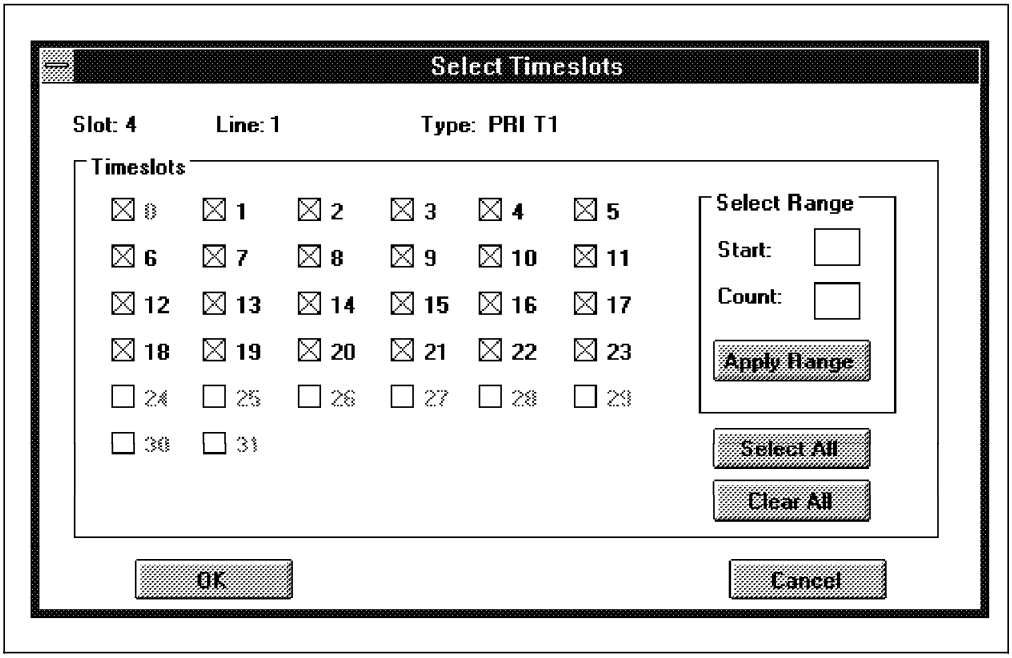


Figure 16. Timeslots Configuration Page for PRI T1 service

The customer will determine how many phone numbers are needed or if a PBX System will be used. The telephone company will tell the customer the switch type and variant to be used and configured on the 8235-I40.

Note: PBX (Private Broadcast Exchange) is any privately owned switching system. The telephone lines are still supplied by the telephone company, but line consolidation and routing is performed by the PBX.

The telephone company assigns a telephone number, installs the telephone jack in the customer's facility and supplies the cable to connect to the T1 service.

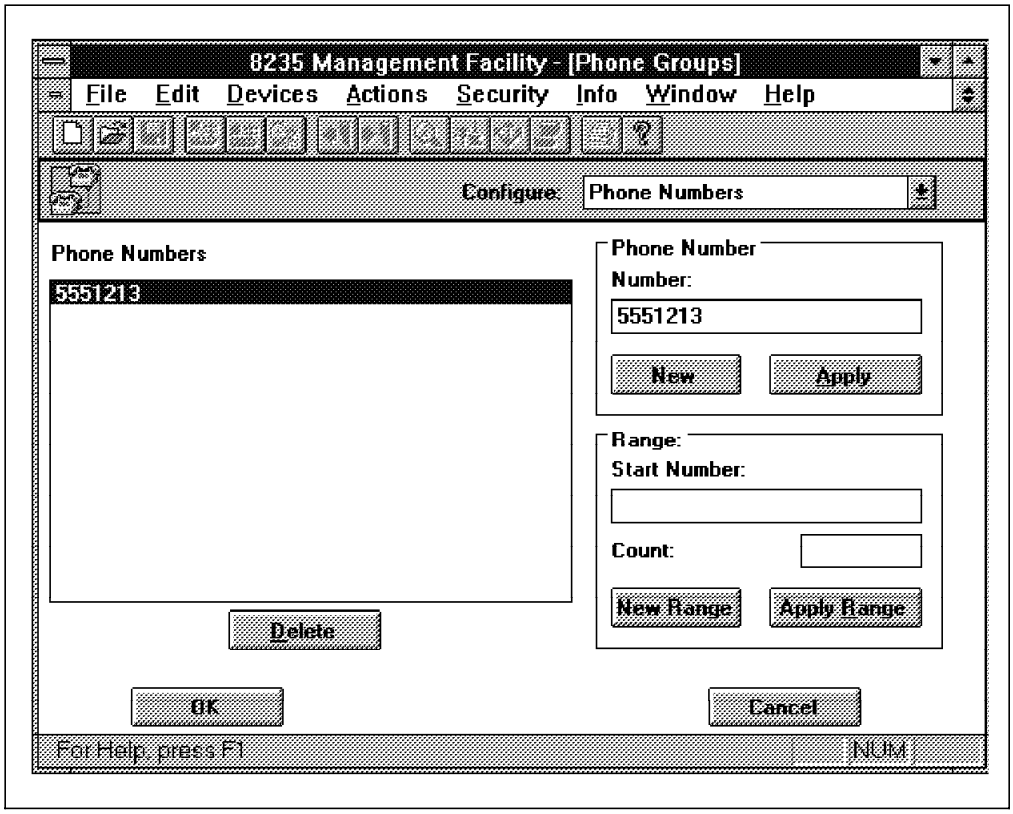


Figure 17. Define Phone Number

4.3.3 Cable Pin and Signal

These pin-outs are also listed on the installation map that comes with the 8235-I40. Sometimes it is necessary to construct a crossover cable to reverse the receive and transmit pins to connect the telephone system jack to the 8235-I40 WAN card.

- **T1 termination on the PRI Board**

1	Receive Ring
2	Receive Tip
3	NC
4	Transmit Ring
5	Transmit Tip
6	NC
7	NC
8	NC

NC=Not Connected

Note: Cables are not supplied with the IBM 8235 Access Switch.

- **Serial Port Diagnostic Port**

1	NC
2	NC
3	NC
4	GND
5	RXD
6	TXD
7	NC
8	NC

NC=Not Connected

With CSU	Without CSU
0 = 1.5 db	0 = 0 db
1 =-7.5 db	1 = -7.5 db
2 = 0 db	2 = -1.5 db
3 = 0 db	3 =-22.5 db
4 = NC	4 =-30 db
5 = NC	

NC=Not Connected

4.4 How to Pin Reset the 8235-I40

The pin reset switch on the 8235 can be used to perform the same as the Clear and Download command on the Actions menu.

On the 8235 server, the pin reset switch is located on the back of the machine near the network connection.

The pin reset function on the 8235 DIALs Switch is accomplished by performing the following steps:

- Attach an Asynchronous terminal or PC to the serial port through a null cable. Use the following setting: 8,1,n at 19.2 bps.
- Power on the Dials Switch.
- When the 8235 is booting press Ctrl+E within 10 seconds. This redirects the messages to the terminal's display.
- A password prompt appears. Press Enter to proceed.
- Answer Yes when asked whether you wish to load PVROM.

  Note: Optionally, if the I40 is already in a running state, the previous three steps can be replaced by depressing the recessed black button on the processor card. This button is located between the two serial ports on the card. Note that pressing this button does not automatically clear the image and configuration from memory. The next question must be answered before the timeout for a complete clear of the memory to take place.
- Answer Yes when asked whether you wish to load PVROM.
- You will have to wait while the Dials Switch loads the permanent VROM and initializes the box.
- Wait till you receive the message Device discovery.
- Now you can go to the management machine and download the image file.
- After this is done the 8235 is ready to be configured.

Chapter 5. Installation Steps

In this chapter, we talk about the general installation steps, including more detail about the Management Facility and Configuration.

5.1 Initially Setting Up 8235-I40 Hardware

- Remove the cover (2 types of screws) - refer to GX27-4030
- Unscrew the metal retainer
- Install the cards and MVIP cable
- Replace the metal retainer
- Replace the cover
- Attach to the LAN
- Plug into power receptacle

5.2 8235 Management Facility

The 8235 Management Facility is a device management application that allows you to configure and manage your 8235s and devices. Using the 8235 Management Facility, you can configure, manage, and monitor the 8235s on your network, create user lists and manage the security of your 8235s. The Management Facility is provided with all 8235s.

5.2.1 Hardware and Software Requirements

The 8235 Management Facility can be run from several operating systems like Windows 3.1, Win-OS/2 or Windows 95. A 486 or higher PC or laptop with mouse is recommended. The 8235 Management Facility needs an IP or IPX protocol stack.

To run the 8235 Management Facility in an IP environment, you need a supported Winsock-compatible Internet Protocol (IP) stack. The 8235 Management Facility operates with IBM TCP/IP for DOS V2.1.1 with PTF, TCP/IP stack from Novell, Inc. (NetWare Client V1.1 and LAN WorkPlace V4.2) and FTP, as well as the default TCP/IP stack in Windows 95. Other IP stacks may function properly but have not been thoroughly tested for use with the Management Facility.

5.2.2 Installation of the 8235 Management Facility

To install the 8235 Management Facility, run SETUP.EXE from diskette #1. Follow the procedures and reboot your PC or laptop when requested. The 8235 Management Facility defaults to the IPX protocol when you initially install it.

If management over IP is required, you need to open the 8235 Management Facility application, choose **Preferences**, select **Management protocols** from the list and click on **IP**. The community name defaults to public and is used for device discovery and polling. Set the timeout and attempts parameters and click on **OK**.

You are ready to use the 8235 Management Facility to manage your devices over your preferred protocol.

5.2.3 8235-I40 Management Facility Menu Bar

Following is a summary of menus and selections on the Management Facility:

- File Menu
- Edit Menu
- Device Menu
- Actions Menu
  - Get and Set configuration
  - Reset ports and sessions
  - Set date and time
  - Clear activity log
  - Clear and download microcode
- Security Menu
  - Get and set user configuration
  - Set an administration password for the I40
  - Select and set up bindery security
- Information Menu
  - Activity Log
  - Get information (general, port detail)
  - Routing table

5.2.4 Methods of I40 Management

In addition to the network (in-band) management via the Management Facility, the following methods can be used to configure the I40:

- Shell Access (serial port, TELNET, Dial-Out)
- Terminal Access (Connected to RS-232 port on the CPU card)
- Use a crossover cable on the Ethernet network adapter

5.2.5 Information on the 8235 Management Facility

If you run the 8235 Management Facility over IPX and your network contains over 200 IPX networks or IPX SAP-capable devices, such as NetWare servers, IBM recommends that you add a [LOOKUPS] section in the IBM8235.INI file to improve performance. The IBM8235.INI file is distributed with your 8235 on Disk 1 of the Management Facility and installed in the IBM8235 directory. The [LOOKUPS] section in the IBM8235.INI file contains the following parameters:

```
[LOOKUPS]
Devices=Shiva
Filters=Active
Networks=Specific
```

Device=Shiva: This entry limits device lookups to 8235-only devices. The default setting is ALL, for which the Management Facility first searches for 8235 devices by type, then sends out an ALL TYPE lookup.

Filter=Active: This entry minimizes the amount of memory consumed by the Device List and reduce the amount of processor time consumed by SAP processing. The device type filter is changed to Active, from a default setting of Display. The device type filters are the devices selected in the Device Type drop-down list on the main Management Facility screen. Currently, the Management Facility maintains an array of all IPX devices in the background and creates the displayed device list from that array. If the filter parameter is set to Display, all SAP packets are processed, and the information is stored internally, even if the device is not shown in the Device List. If the Filter parameter is set to Active, the Management Facility still looks at each SAP packet that it receives, but it only stores and displays entries that pass the current device type filter.

Networks=Specific: This entry changes the IPX RIP processing to process only selected networks. The default setting of ALL causes Management Facility to maintain a table of routes to all IPX networks. When set to Specific, the Management Facility starts with a network list that contains the workstation′s network. If a device is selected, the Management Facility searches for a route to the device and adds that information to the network list. Once a network is added to the network list, SNM processes any RIP updates that are related to that network. If the user performs a refresh, the network list starts over with just the workstation′s network. Using specific network processing minimizes the amount of memory consumed by the network list and reduces the amount of processor time consumed by RIP processing.

If your LAN contains multiple segment with many IPX network numbers, you may need to modify the 8235 to enable and lock a specific network frame type rather than allowing the 8235 to auto-sense. When set to auto-sense the 8235 listens to IPX frames on its network segment to determine the frame type to use and the IPX network number associated with each. When there are many choices the 8235 can experience problems with IPX traffic to/from the Management Facility, even when it appears to have auto-sensed the correct frame types and numbers. A common symptom of this problem is the message `Unable To Communicate with 8235 in Management Facility` when trying to GET or SET the configuration or user list.

To enable and lock the frame types for your LAN, you first need to determine which ones to use. If you have a NetWare server on the same segment as the 8235, you can find out by checking the AUTOEXEC.NCF file on the server. Note which frame types are in use and what IPX network number is bound to each. If

you don't have a NetWare server to reference, then check with your network administrator for the information. Modify the NetWare page of the 8235 configuration by enabling each frame type to use (for example Ethernet_802.2 and Ethernet_SNAP), and by entering the IPX network number and checking locked for each type.

If you are following this procedure because you already have difficulty communicating with the 8235, you may need to move the 8235 and Management Facility station temporarily to an isolated segment so you will able to GET and SET Configuration. You would also need to isolate them if you accidentally enable the wrong frame types or assign incorrect IPX network numbers for the 8235's LAN segment. The problem arises that the devices are transmitting on two different network numbers without an IPX router between the two devices. When isolating the two devices onto a separate segment, first power on the device with the locked frame type and network number, usually the 8235. After this machine has finished powering on and attached to the network, power on the other device. This allows the second device to detect the frame type established on the network by the first device. The 8235 can now be managed by the Management FAcility PC.

Warning

Because the adapter is an autosense card, the 8235-I40 with token-ring feature cannot be the first device on the network.

If you are using the Windows 95 Dial-Up Networking client and have difficulty transferring data to or from the LAN using the NetBEUI protocol, add the following to the Additional Configuration page of the 8235's configuration (click on **Get Configuration** in Management Facility):

```
[Serial*]
MTU=1500
```

Be sure to click on **Set Configuration** after making the change. This parameter corrects a problem that Windows 95 sometimes has in negotiating the frame size, particularly to a token-ring 8235. By default the 8235 uses a maximum size of 1500, and this parameter will force Windows 95 to accept this size.

5.3 Configuring the 8235-I40 (Overview)

Even though the I40 is a completely new hardware platform compared to all other 8235 models, it maintains full compatibility with the existing 8235 DIALs clients. The Management Facility has remained unchanged in many parts; only those configuration aspects that are specific to the I40 were added. The Ports configuration page, which does not apply to the I40, was removed from the drop-down list of an I40 configuration and replaced with the Slots page. However, there is only one version of the Management Facility for all models. It will display the applicable configuration pages for each model respectively.

The I40-specific configuration options are:

- Slots
- Phone groups
- Phone group pools

5.3.1 Slots

By definition, a slot is a place where cards or modules are attached (see 2.3.1, “Chassis” on page 10).

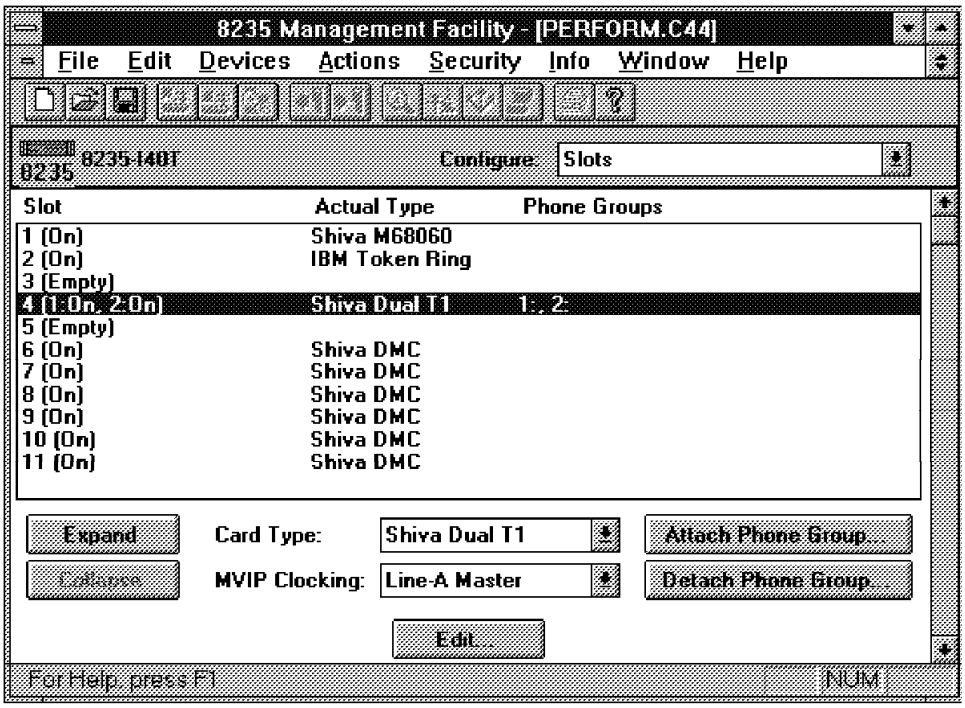


Figure 18. Slots General Configuration Page

5.3.2 Phone Groups

A phone group is the logical abstraction of the non-I40 model ports. It is based on the phone numbers and does not have any physical correspondence to slots (neither to their position, nor to their number). The physical resources are the slots, the interface cards which are inserted in them, and finally the timeslots of their framed interface (in the case of WAN cards). There is no fixed relationship between these physical resources and the logical resources phone groups, as

there is with non-I40 models between ports and port pools defined by names given to the port. When a call is established, a dynamic temporary binding between physical and logical resources takes place.

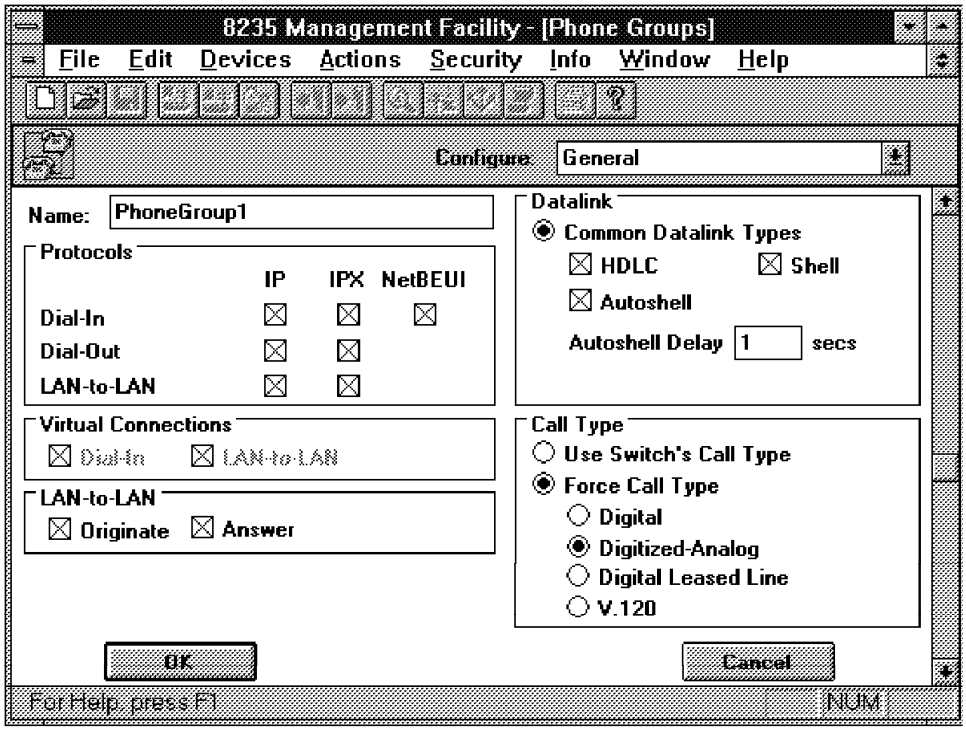


Figure 19. Phone Groups General Configuration Page

Phone groups consist of the following items:

- A set of one or more phone numbers
- A set of one or more timeslots (64 kbps channels)
- Configuration information for the phone numbers and timeslots in the group.

Phone groups allow you to associate phone numbers and their characteristics with a physical interface in the 8235 DIALs Switch. A physical interface can be one of the following types:

- A telephone line
- A single timeslot
- A set of timeslots

Phone groups can be configured to perform a variety of functions. Their flexibility includes options that allow you to specify acceptable protocols, virtual-connection capabilities, call type (digital or analog), dial type (tone or pulse), a phone number or range of phone numbers that are acceptable, and the configuration of the modem a call is using.

Note: Phone groups are numbered logically. There is no limit to the number of phone groups that can be created and configured.

The possible phone group configurations include:

- Allowing only digital calls over a specified line

- Allowing only analog call over a specified line
- Dedicating a set of timeslots specifically for LAN-to-LAN connections

Although there is no set limit to the number of phone groups that can be created, generally there are fewer than 10, and frequently only 1. It is often the case that one phone group will be created with all incoming phone numbers assigned to this group, which is then bound to the appropriate interfaces. This allows one phone group to be set allowing for universal dial-in and dial-out capabilities and privileges.

As well, more phone groups can be added to reserve a specified number of timeslots for dial-in and another specified amount for dial-out. Suppose we have a single PRI T1 line where we want six channels reserved for dial-in and six more for dial-out. We do not care if the other eleven are used for dial-in or dial-out; they can be assigned to calls as needed. Here we would create two phone groups — one for dial-in on timeslots 0-17, and one for dial-out on slots 6-24. This can be done in other methods; implementation methods may vary by environment.

When configuring phone groups, you can map:

- One phone number to one timeslot (simple case)
- Many phone number to one timeslot (rotary)
- One phone number to many timeslots (800 number or hunt group)
- Many phone numbers to many timeslots (a block of phone numbers can be used with any timeslot or block of timeslots)

Note: A phone number can be used in only one phone group.

5.3.3 Phone Group Pools

Phone group pools are an IBM 8235-I40 feature that allows phone groups to be clustered based on specific characteristics that the 8235 DIALs Switch might not have the ability to configure, such as aspects of the line provisioning or the tariffing. The 8235 DIALs Switch has no knowledge of tariffs, or other characteristic network administrators associate with their lines. Pooling provides a general mechanism to group phone groups in ways that are most useful to you. For example, if the lines attached to the I40 are provisioned with In WATS (WATS - Wide Area Telephone Service, may not apply outside the US) and Out WATS lines, allowing for lower tariffing in certain directions, it makes sense to assign the phone groups into InPools and OutPools matching the tariffing.

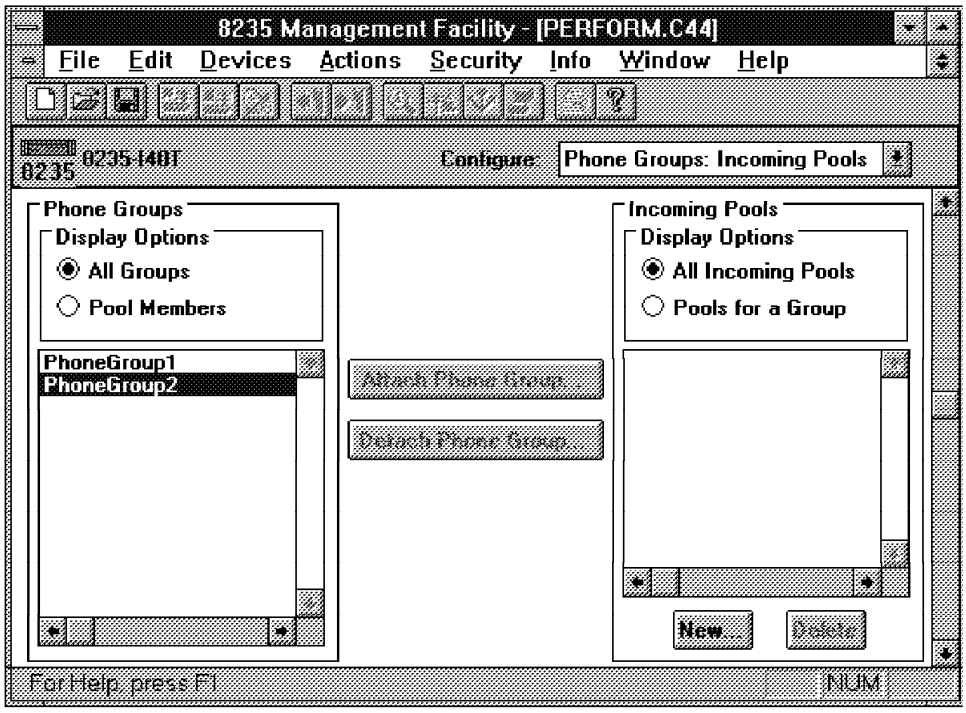


Figure 20. Phone Groups - Incoming Pools

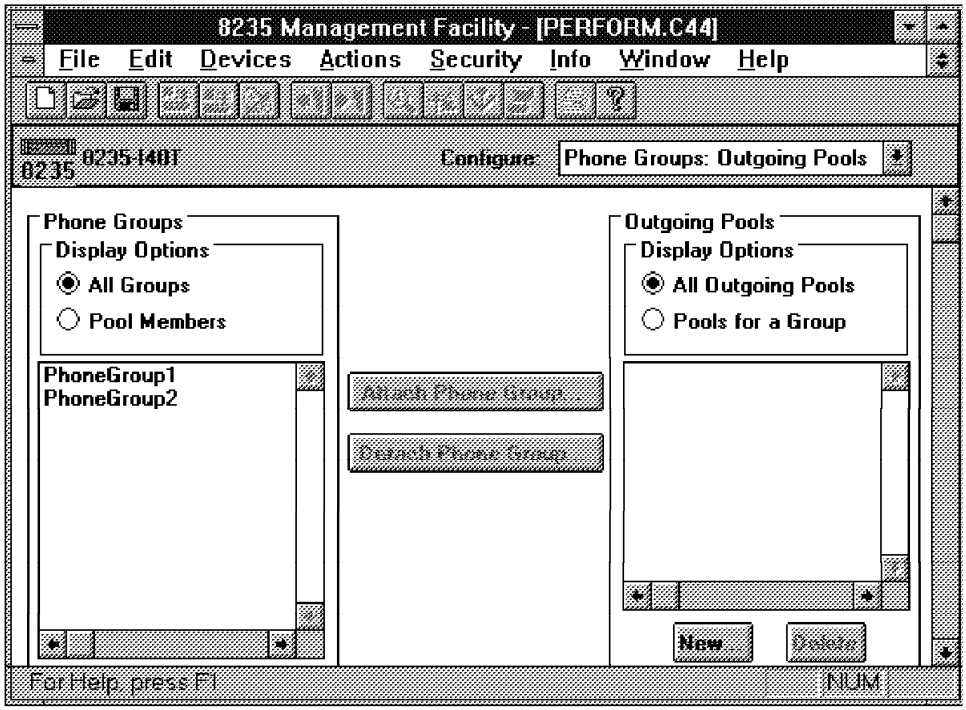


Figure 21. Phone Groups - Outgoing Pools

Note

Phone group pools are optional. You do not have to define phone group pools if there is no need for them.

There is no limit to the number of phone group pools that can be created. Phone group pools must be classified as either incoming pools or outgoing pools. Incoming pools contain phone groups that are used for incoming calls and the MultiLink Protocol (MLP) feature. Outgoing pools contain the phone groups that you prefer clients to use to make outgoing calls. Dial-back pools contain the outgoing pool phone groups to be used for dial-back connections.

5.3.3.1 Incoming Pools

The main purpose of incoming pools is to collect phone numbers to distribute for Multilink PPP (MLP) calls.

When a phone group receives an incoming call, the additional phone numbers that are distributed for an MLP connection must come from that phone group, or from another group in the same incoming pool.

For example, a remote user dials in with PPP (Point-to-Point Protocol) using MLP and DIALs Client PPP. The 8235-I40 uses a proprietary protocol called MCCP to send phone numbers back to the dial-in client to establish the next line in the MLP connection. It is possible to establish a MLP connection without MCCP, but users may run into problems, especially if one hunt group spans several devices.

MCCP allows remote users to dial one phone number (which could be a hunt group over several boxes) and, after receiving the call, MCCP passes back to the remote user another phone number that is specific to a line or group of lines that are connected to same I40. In this way, the second MLP connection comes into the same device as the original call.

Another example is if you call phone group 7, and phone group 7 is part of the incoming phone pool FRED (FRED is a group name and can be called any name) the 8235 DIALs Switch will look to the phone groups in FRED until it finds one with a free phone number. The 8235 DIALs Switch will issue that number and expect an incoming phone call.

Therefore, the phone groups pooled together should have similar capabilities. The FRED example will work only if all of the phone groups have PPP capabilities.

Note: Phone groups that do not have PPP should not be part of an incoming pool because PPP is the only network layer protocol that supports multilink incoming calls.

PRI and robbed-bit calls are typical examples of calls that should be in different phone groups and different phone pools. As an example, if you receive a T1 call that wants to use MLP, and you return the number of a PRI line, the operation will not function correctly.

5.3.3.2 Outgoing Pools

Outgoing pools are used mainly for dial-out. Refer to Chapter 8, “Dial-Out Client” on page 197 for further details.

5.3.3.3 Naming Phone Group Pools

Phone group pool names do not have any intrinsic meaning. There are no default pool names (unlike port pools in other 8235 models), and the only reserved name is Command Shell. Incoming pool names can be the same as the outgoing pool names, but for the sake of clarity, this is not advisable.

5.3.4 Slot Configuration

The I40 discovers all cards at startup and confirms that the discovered cards match the configured cards. If there is a mismatch then the slot is disabled, and labeled with MisCfg: on the Slots configuration page. In particular, care must be taken not to configure an ISA card in a PCI-only slot.

To configure the slots on a DIALs Switch:

1. From the Configuration drop-down list, select **Slots**.

   The Slots configuration page appears.

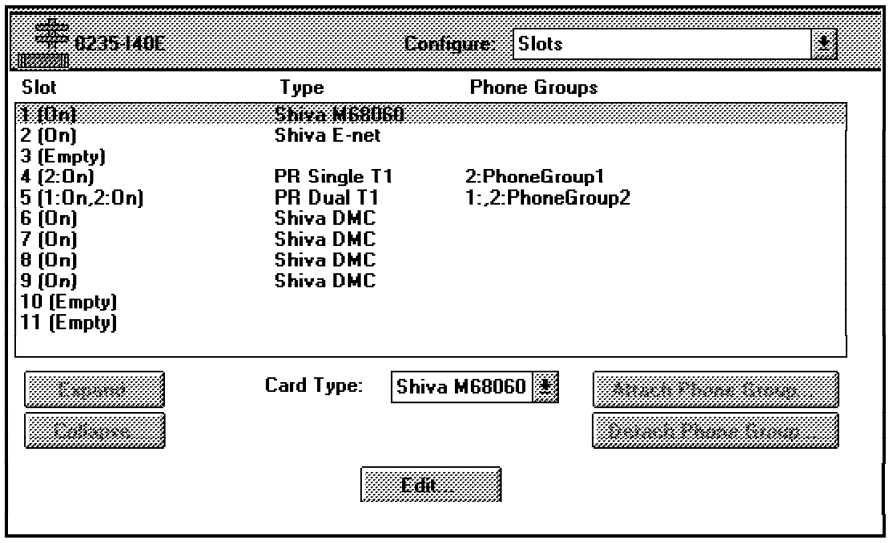


Figure 22. Slots Configuration Page

   The Slots configuration page lists the slots in the device, the type of card that is in each slot, and the phone groups that have been attached to lines in each slot.

2. Click on the slot that you want to configure. Use the Card Type drop-down list to select the type of card you want to put in the slot.

   You might want to configure a slot if you do not have a card for the slot available or if you plan to change the card in the slot. The following table describes the options available in the drop-down list.

Table 11 (Page 1 of 2). 8235-I40 Card Types

Type of Card	Description
PR Single T1	Primary Rate Interface — Single T1 WAN Card
PR Dual T1	Primary Rate Interface — Dual T1 WAN Card
PR Single E1	Primary Rate Interface — Single E1 WAN Card
PR Dual E1	Primary Rate Interface — Dual E1 WAN Card

Table 11 (Page 2 of 2). 8235-I40 Card Types	
Type of Card	**Description**
Shiva Quad T1	CSU/DSU and Channelized T1 Support, no dial-out support
Shiva Dual PRI/T1	Software selectable CSU/DSU, Channelized T1 Support
Shiva Dual PRI/E1	Card with E1 service with PRI ISDN
Shiva M68060	A 68060 CPU card
Shiva DMC	Digital Modem Card
IBM Token Ring	PCI autosense 16/4 token-ring adapter
Shiva E-net	Ethernet card
<Empty>	If no card is detected in a slot, the configuration displays <Empty>.

Note: In a DIALs Switch, slot 1 is reserved for a CPU card; slot 2 is reserved for a Network card. WAN cards or digital modem cards can be installed in slots 4 through 11. The firmware knows which slots are PCI-only and which are PCI/ISA, so this is not needed to be configured.

3. Select **<Empty>** from the Slot Type drop-down list if you want to remove a configuration from a slot.
4. Select each slot that contains a WAN card or a CPU card and click on **Edit** to perform additional configuration.

Note: Network cards and DMC cards do not require any configuration. If you select a slot containing an Ethernet LAN or DMC card, the **Edit** button is disabled.

Figure 23 shows a sample display provided by the 8235 Management Facility Device Info function, giving details and Ethernet statistics.

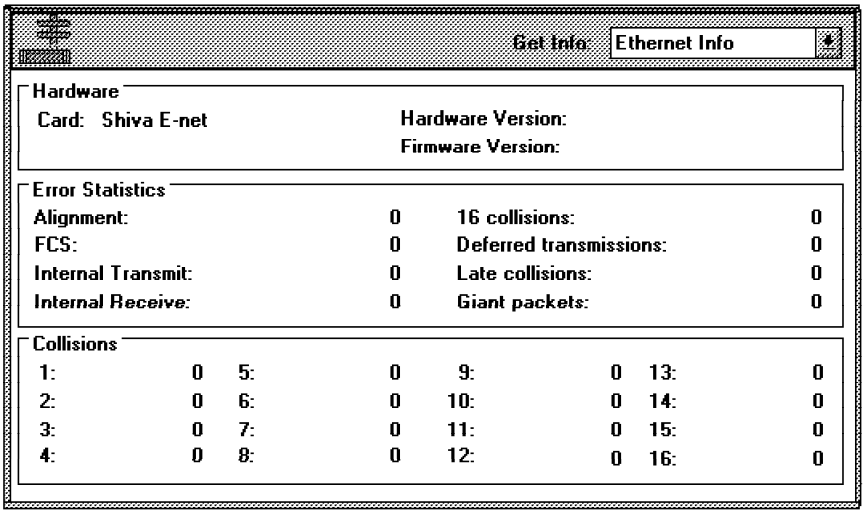


Figure 23. Device Info Page - Ethernet Info

Figure 24 on page 50 shows a sample display provided by the 8235 Management Facility Device Info function, giving details and statistics about the DMC. The modem information applies to the modem selected from the list to the left.

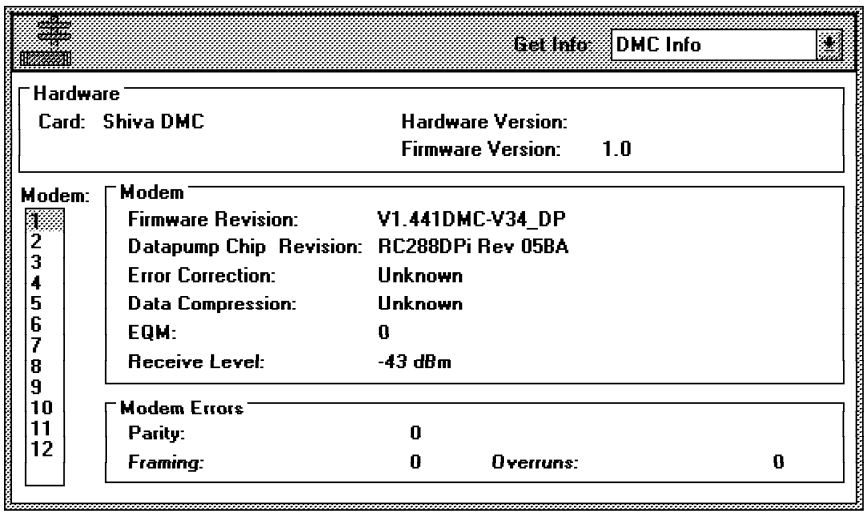


Figure 24. Device Info Page - DMC Info

Note: If the modem is not currently connected, the Error Correction and Data Correction settings will read Unknown, as these display the setting of the current connection.

Warning

If Firmware Revision and Datapump Chip Revision are blank, run tests against the modem card and attempt an update. If these fail, it is possible that the modem is bad.

The Firmware Revision is the level of code currently installed in the modem DSP. Version 1.441 (shown here) supports connections up to 28.8 kbps. A DMC update (execute `dmc mupdate all` in the command shell) is available with Version 4.5 to upgrade the modems to Version 1.600 or higher, which supports 33.6 kbps connections.

Note: A hardware upgrade is currently needed to upgrade to 56 kbps technology.

5.3.5 Configuring the CPU Card

The type of card configured for slot 1 does not really matter since slot 1 is required to contain a CPU card; if it doesn't contain a CPU card, then the I40 will not boot. I40 reports a CPU card in slot 1 no matter what the configuration indicates. What actually remains to be configured for slot 1 is the setup for the two out-band management serial ports, the so-called UARTs (universal asynchronous receiver/transmitter). They provide access via *direct connect* using a null modem cable and a terminal, or with a modem for dial-in access. The reason for two ports to exist is to offer both direct and dial-in at the same time without the need to reconfigure each time. You can have a modem permanently attached to one port for remote management and use the other port for on-site management, in case you no longer have access via in-band management.

The functionality usable on the UARTs is limited for security reasons. Specifically, virtual connections, dial-out and LAN-to-LAN are not allowed on the UART ports. These are disabled by default in the configuration, but the code

prevents use of these features even if the configuration enables them (for example, via the Additional Configuration page).

To configure a serial port on the CPU card in slot 1 of an 8235 DIALs Switch:

1. Select a slot containing a CPU card, usually slot 1 from the Slots configuration page (see Figure 22 on page 48).
2. Click on **Edit**. The Serial Port Configuration window appears.

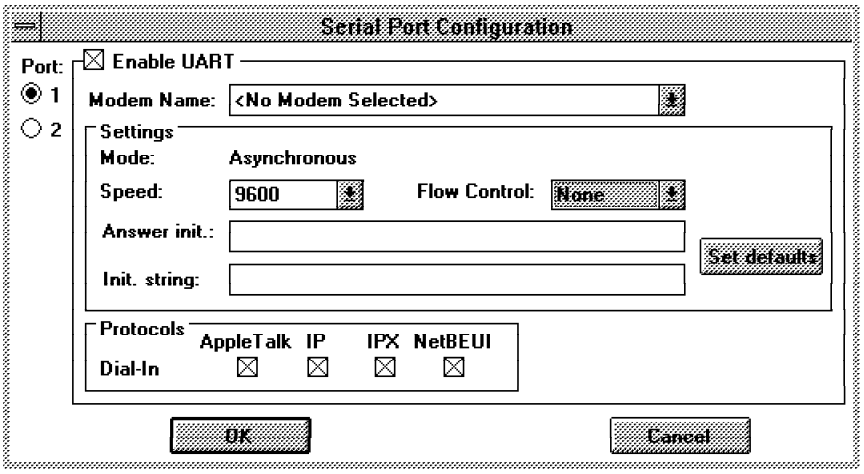


Figure 25. Serial Port Configuration Window

3. Select the UART radio button for the serial port (1 or 2) that you want to configure.
4. Select a modem from the Modem Name drop-down list. The Settings area displays the configured settings for the modem you selected.

   Note: If you select a modem for ARA 1.0, the following features are disabled on this port: compression, IP dial-in, IPX dial-in, and LAN-to-LAN answer.
5. Select a modem speed from the drop-down list.
6. Select the flow-control option that you want the modem to use:

   None Do not use any flow control.

   Software Use software flow control only.

   Note: You can use the software method with any cable. However, the XON and XOFF characters are lost when you use this method.

   Hardware Use hardware flow control only.

   Note: The hardware method requires a cable carrying the required signals (DTR/DSR), but it is reliable and there are no intercepted characters.

   Both Use both hardware and software for flow control.
7. The Answer init. field displays the modem initialization command string that the 8235 DIALs Switch uses when it answers a call. Change the default string if necessary.

8. The Init. string field displays the modem initialization command string that the 8235 DIALs Switch uses when it initiates a call (for dial-back). Change the default string if necessary.
9. In the Protocols area, enable the check boxes for the protocols you want the 8235 DIALs Switch to accept on dial-in connections over this modem. You can select IP, IPX, NetBEUI, and AppleTalk.
10. Click on **Set Defaults** if you want to change the modem settings to the standard default values for the modem.
11. Click on **OK** to save your changes and close the Serial Port Configuration window.

    Note: When using **<Null Modem>**, 19200 is the recommended setting. When the 8235-I40 is starting up, the port is automatically set at 19200 (for Ctrl-E access). If the configuration is the same as this default, then you do not have to change the speed on the PC to view data at different times during the boot sequence.

5.3.6 Configuring a T1 Interface Card

Recommendation

Use this section as a questionnaire. For most of the configuration parameters on the T1 configuration page (framing, coding, LBO, switch type and variant, signaling type) you will have to ask your service provider for the correct settings, which are dependent on their equipment.

The Single T1 WAN card supports a single line that you can configure. The Dual T1 WAN card has two lines that can be configured either the same or with two different configurations. The Quad T1 WAN card supports up to four lines.

The Slots configuration window also displays the phone groups that are associated with this interface. See 5.3.8.4, “Attaching Phone Groups to a WAN Interface” on page 67 for details.

To configure the lines for a T1 WAN interface card in an 8235 DIALs Switch:

1. Select a slot containing a T1 WAN card whose lines you want to configure from the Slots configuration page (see Figure 22 on page 48).

   If you want to configure the lines on a multiple line T1 card separately, click on **Expand** to select the line you want to configure. If you want all lines to have the same configuration, do not use the Expand button; the configuration you edit will apply to all lines.

2. Click on **Edit**. The Slot *x* Configuration - T1 window appears.

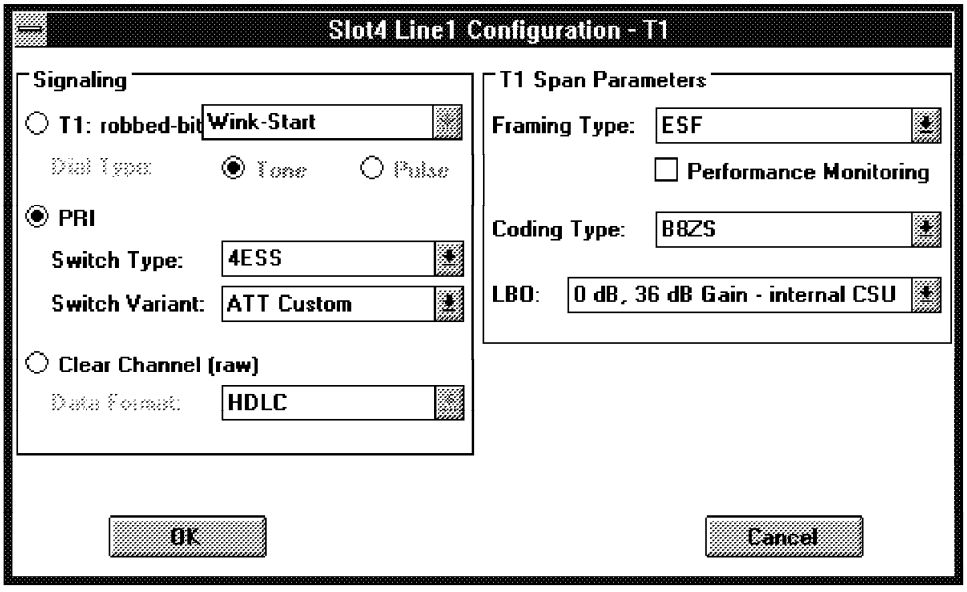


Figure 26. Slot x Configuration - T1 Window

3. Select the **Enable Line** check box.

Note: If any of this data is incorrect, click either **Custom...** or **Assistant...** to reconfigure the line. If you select **Custom...** you will see Figure 14 on page 34. Choosing **Assistant...** will talk you through a series of menus to configure your line instead of these steps.

4. In the T1 Span Parameters area, do the following steps:

   - In the Framing Type field, select the physical framing method used to format data that the service provider expects. The following table describes the options; ESF is the default framing type.

     Note: The framing method you select *must* be the same as that used by the service provider, the repeaters, and the device on the other end of the line. The framing signal in bit 0 of the 193-bit frame is used to locate the timeslots.

Table 12. 8235-I40 T1 Framing Types

Framing	Description
None	No Framing
SF	Super Frame (D4 channel bank) framing
ESF	Extended Super Frame framing
SFSLC96	Extended Super Frame SLC96 framing
ESFZBTSI	Extended Super Frame ZBTSI framing

   - If the framing type is one of the extended super-framing options (ESF or ESFZBTSI), you can enable the Performance Monitoring check box if you want the 8235 DIALs Switch to send performance monitoring information to the other end of the ESF stream.

5. In the Coding Type Selection, select an option from the drop-down list to specify the type of zero substitution used on the line. The following table describes the available options; B8ZS is the default coding parameter.

Table 13. 8235-I40 T1 Coding Types

Coding	Description
AMI	Alternate Mark Inversion
ZBTSI	Zero Byte Time Slot Interchange
B8ZS	Bipolar 8 Zero Substitution — Clear Channel

6. In the Signaling Type area, do the following steps:

   - Enable one of the three radio buttons: Robbed Bit, PRI, or Clear Channel (raw), to specify the protocol between the 8235 DIALs Switch and the WAN line to bring calls up and take them down on the line. The following table describes these options; robbed bit with wink start is the default signaling type.

Table 14. 8235-I40 T1 Signaling Types	
Signaling Type	**Description**
Robbed Bit	Use the line as a T1 trunk with E&M signaling and 10 pulse-per-second dialing. Select the signaling option for your line.
PRI	Primary Rate ISDN.
Clear Channel (raw)	No signaling. You must choose None if the call type is a digital leased line.

- If the signaling type is robbed bit, you must enable one of the Dial Type radio buttons: Tone or Pulse.
- If the signaling type is PRI, you must select the switch type and variant from the drop-down list. You should receive these settings from the telephone company.
- If the signaling type is Clear Channel (raw), you must select an option from the Data Format drop-down list to specify how the data bytes on the line are to be framed when there is no signaling. The following table describes the available options; HDLC is the default data format.

  Note: HDLC framing is contained in the configuration page, but is not supported by the I40 in the first release.

Table 15. 8235-I40 T1 HDLC Framing Types	
Data Format	**Description**
HDLC	Sends the data to a High-Level Data Link Controller for framing and deframing.
Inverted HDLC	Uses inverted HDLC that inverts data bits so that HDLC bit-stuffing rules enforce the 1s density requirements for the T1 line.
Raw	Does not frame the data bytes; does not send the data to an HDLC controller for framing or deframing.

7. In the LBO (Line Build Out) parameter, select a value from the drop-down list (a range of lengths, in feet, and a decibel value) that allows the interface to compensate for the length of wire connecting it to the service provider line.

   Note: The lengths apply to external CSUs, and the decibel values apply to internal CSUs.

   If this line has an internal CSU/DSI interface, the service provider should specify the loss in decibels based on the distance to the first repeater.

   If this line has an external CSU, such as a DSX-1 interface, select an LBO value based on the cable length in feet to the DSX-1 cross-connect port.

8. Click **OK** to exit the custom configuration.
9. Click **Done** to exit the slot configuration.
10. If the WAN card is expanded, click **Collapse** and ensure the card is selected.
11. In the MVIP Clocking parameter, select an option from the drop-down list; Internal/None is the default clocking parameter. In a digital-only

configuration, each WAN interface must be set to the default, Internal/None. In a configuration that accepts analog calls, one, and only one, of the WAN interfaces must be set to be a master MVIP clock. Use the line that is the most reliable and has the best clocking (if different providers are used for the different lines).

For a single-line card, the clocking parameter must be set to Line-B/Master. For a dual-line card, the clocking parameter must be set to either Line-A/Master or Line-B/Master. The clocking parameter on all other WAN interface cards must be set to Secondary for the appropriate lines. If a DMC card is found in a configuration, the 8235 Management Facility ensures that only one line is set to master.

If the MVIP master clock is not functional or not plugged in, the DIALs Switch may not function properly, especially for analog calls.

Note: The MVIP Clocking parameter applies to all lines on a multiple T1 card; you cannot set it for only one of the lines. (The MVIP clocking parameter is grayed out if you are configuring one line on a dual card.)

5.3.7 Configuring an E1 Interface Card

Recommendation

Use this section as a questionnaire. For most of the configuration parameters on the E1 configuration page (framing, coding, switch type and variant, termination resistance, signaling type) you will have to ask your service provider for the correct settings, which are dependent on their equipment.

The Single E1 WAN card supports a single line that can be configured. The Dual E1 WAN card has two lines that can be configured either the same or with two different configurations.

The Slots configuration window also displays the phone groups that are associated with this interface.

To configure the lines for an E1 WAN interface card in an 8235 DIALs Switch:

1. Select a slot containing an E1 WAN card whose lines you want to configure from the Slots configuration page (see Figure 22 on page 48).

   If you want to configure the lines on a dual E1 card separately, click on **Expand** to select the line you want to configure. If you want the two lines to have the same configuration, do not use the Expand button; the configuration you edit will apply to both lines.

2. Click **Edit**. The Slot *x* Configuration - E1 window appears.

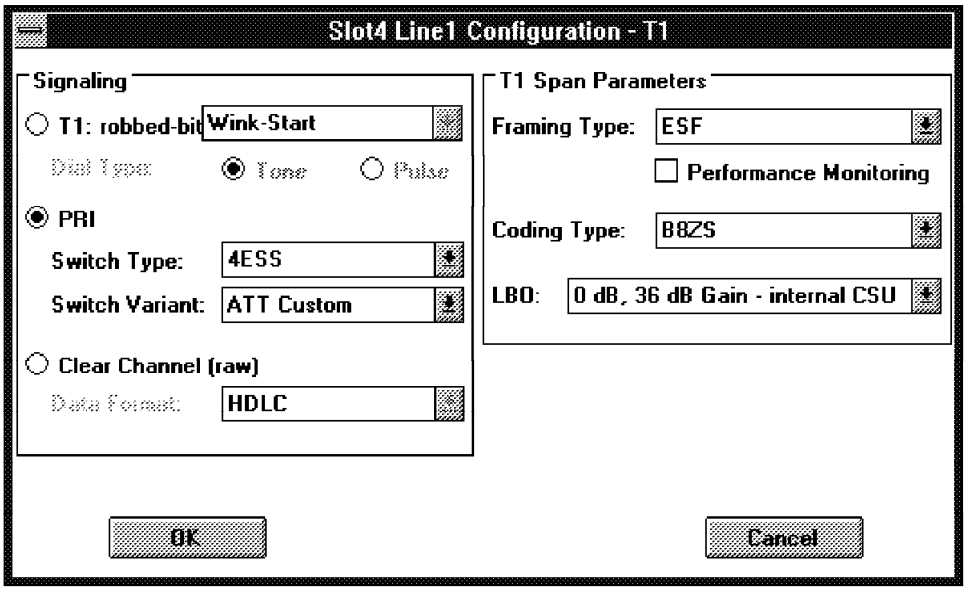


Figure 27. Slot x Configuration - E1 Window

3. Select the **Enable Line** check box.

   Note: If any of this data is incorrect, click either **Custom...** or **Assistant...** to reconfigure the line. If you select **Custom...** you will see Figure 14 on page 34. Choosing **Assistant...** will talk you through a series of menus to configure your line instead of these steps.

4. In the E1 Span Parameters area, do the following steps:

   - In the Framing Type field, select the physical framing method used to format data that the service provider expects. The following table describes the options; CRC4MFFEBE is the default framing type.

     Note: The framing method you select *must* be the same as that used by the service provider, the repeaters, and the device on the other end of the line. The framing signal in timeslot 0 is used to locate the timeslots.

Table 16. 8235-I40 E1 Framing Types

Framing	Description
None	No Framing
CRC4MFFEBE	E1 with CRC-4 multiframing with the Si bit set for Far End Block Error (FEBE) checking.
CRC4MF1	E1 with CRC-4 multiframing with the Si bit set to 1.
BF1	E1 with basic framing without CRC-4 and the Si bit set to 1.

5. In the Coding parameter, select an option from the drop-down list to specify the type of zero substitution used on the line. Only HDB3 can be used on E1 lines.

6. In the Signaling Type area, do the following steps:

   - Enable one of the radio buttons: PRI, or None, to specify the protocol between the 8235 DIALs Switch and the WAN line to bring calls up and take them down on the line. The following table describes these options; PRI is the default signaling type.

Table 17. 8235-I40 E1 Signaling Types	
Signaling Type	**Description**
PRI	Primary Rate ISDN.
None	No signaling. You must choose None if the call type is a digital leased line.

Note: If the signaling type is PRI, timeslot 16 on the interface is reserved for signaling on the ISDN D-channel. Also, the switch type and variant must be selected from the drop-down list. These settings will be delivered from the telephone company. Options are listed later in this section.

- If the signaling type is None, you must select an option from the Data Format drop-down list to specify how the data bytes on the line are to be framed when there is no signaling. The following table describes the available options; HDLC is the default data format.

  Note: HDLC framing is contained in the configuration page, but is not supported by the I40 in the first release.

Table 18. 8235-I40 E1 HDLC Framing Types	
Data Format	**Description**
HDLC	Sends the data to a High-Level Data Link Controller for framing and deframing.
Inverted HDLC	Uses inverted HDLC that inverts data bits so that HDLC bit-stuffing rules enforce the 1s density requirements for the E1 line.
Raw	Does not frame the data bytes; does not send the data to an HDLC controller for framing or deframing.

7. Click **OK** to exit the custom configuration.
8. Click **Done** to exit the slot configuration.
9. If the WAN card is expanded, click **Collapse** and ensure the card is selected.
10. In the MVIP Clocking parameter, select an option from the drop-down list; Internal/None is the default clocking parameter. In a digital-only configuration, each WAN interface must be set to the default Internal/None. In a configuration that accepts analog calls, one, and only one, of the WAN interfaces must be set to be a master VIP clock. Use the line that is the most reliable and has the best clocking (if different providers are used for the different lines).

    For a single-line card, the clocking parameter must be set to Line-B/Master. For a dual-line card, the clocking parameter must be set to either Line-A/Master or Line-B/Master. The clocking parameter on all other WAN interface cards must be set to Line A/Secondary or Line B/Secondary. If a DMC card is found in a configuration, the 8235 Management Facility ensures that only one line is set to master.

    If the MVIP master clock is not functional or not plugged in, the DIALs Switch may not function properly, especially for analog calls.

    Note: The MVIP Clocking parameter applies to both lines on a dual card; you cannot set it for only one of the lines. (The MVIP clocking parameter is grayed out if you are configuring one line on a dual card.)

11. In the Switch area, you must specify two parameters that identify the type of switch, Type and Variant, as follows:

    Note: The Type and Variant parameters apply to ISDN only; the signaling type must be set to PRI.

    - In the Type parameter, select a switch type from the drop-down list. The following table describes the available options; 4ESS is the default switch type.

Table 19. 8235-I40 E1 Switch Types

Switch Type	Description
4ESS	AT&T 4ESS
5ESS	AT&T 5ESS
DMS100	Northern Telecom DMS100
DMS250	Northern Telecom DMS250
MD110	Ericsson MD 110
EWSD	Siemens EWSD (United States)
NTT	NTT (Japan)
Other	Any unknown switch conforming to ITU-T standards

    - In the Variant parameter, select the Q.931 national or vendor-specific code set extension used with the telephone switch indicated by the switch Type parameter. The following table describes the available options; ATTCustom is the default Variant.

Table 20. 8235-I40 E1 Switch Variants

Variant	Description
ATTCustom	In publication AT&T PUB 41449
NTICustom	In publication Northern Telecom NIS A211-1
NAT1	Bellcore National ISDN-1 for BRI
NAT2	Bellcore National ISDN-2
JATE	JATE-compatible as defined for INS-1500 for Japan
NET5	NET-5 ETSI standard for PRI in Europe
1TR6PRI	1TR6 standard for PRI for Germany
VN3	VN3 for France
ITU-T	General ITU-T (former CCITT) Q.931 conformance
Q933	ITU-T Q.933 based on Frame Relay Forum implementation agreement
Q933T123	ITU-T Q.933 supporting T.123 subset of D-channel messages

12. In the Termination area, specify the resistance in Ohms for termination of an E1 line. This is required for E1 lines. It applies to E1 lines only, as indicated by the Framing Type. The default is 120 Ohms.

5.3.8 Configuring the Phone Group General Page

1. The Phone Groups configuration page lists the phone groups by name and gives their associated slot number, line number, and time slots. From this window you can edit or view, add or delete phone group configurations.
2. If you click on **Add** or **Edit**, the Phone Groups General configuration window appears.

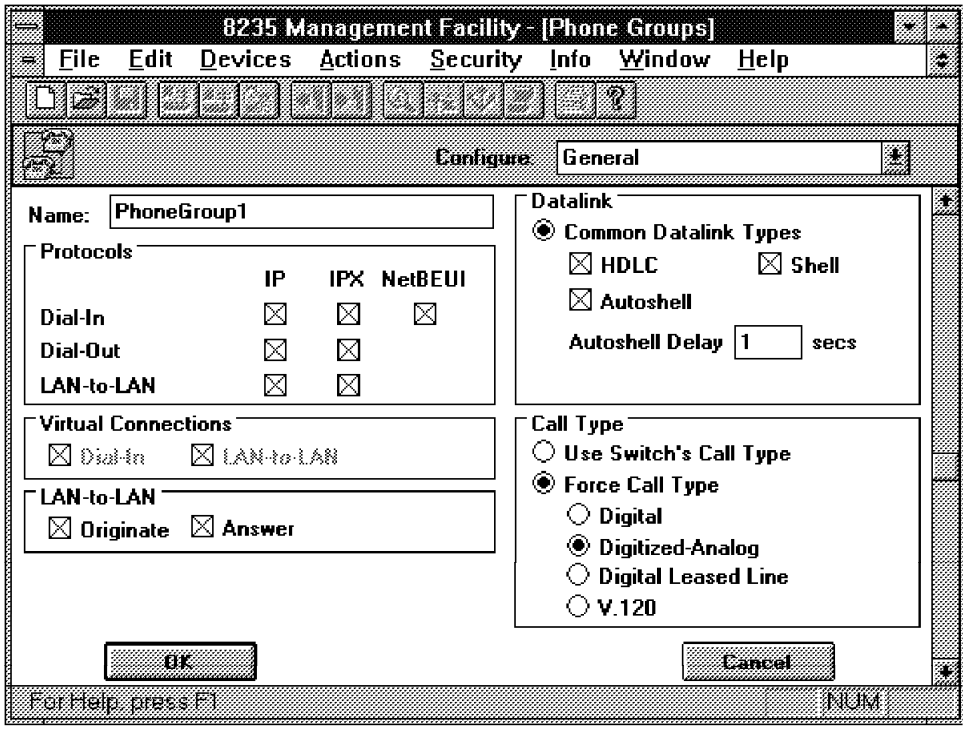


Figure 28. Phone Groups General Configuration Page

Note: AppleTalk is not listed because this capture is from a token-ring 8235-I40.

3. In the Name field, enter a unique name (unique to this 8235) to identify the phone group.
4. In the Protocols area, set the following parameters:
   - Enable protocols for dial-in connections: AppleTalk, IP, IPX, and NetBEUI.
   - Enable protocols for dial-out connections: IP and IPX.
   - Enable protocols for LAN-to-LAN connections: AppleTalk, IP, and IPX.
5. Set the following parameters if you want to support these features for the phone group:
   - Enable the **Dial-In** and **LAN-to-LAN** check boxes in the Virtual Connections area.
   - Enable the **Answer** and **Originate** check boxes in the LAN-to-LAN area.
6. In the Datalink area, select either the **Common Datalink Types** or the **ARA 1.0** radio button using the following criteria:

   Note: You must set the datalink parameter to allow the phone group to support the desired protocols. For example, IP dial-in requires that you

enable HDLC. If HDLC is not enabled in the phone group, the IP dial-in call will connect but LCP negotiation will fail.

- Enable **Common Datalink Types** if you want to use this phone group to answer or originate calls using IP, IPX, NetBEUI/LLC, ARA Version 2, or the command shell. This is the choice to be made in most cases.
- Enable **ARA 1.0** if you want to use this Phone Group to answer or originate AppleTalk Remote Access Version 1 connections. If you enable ARA V.1, no other datalinks can be supported by this phone group. (You must use a modem that supports ARA 1.0 for this option to work correctly.)

7. If you enable the **Common Datalink Types** radio button, you must enable one or more types of datalinks that can be used for calls associated with this phone group. Select one or more options from the following choices:
   - Enable **ARA 2.0** to support AppleTalk Remote Access Version 2 framing.
   - Enable **HDLC** to support protocols framed in HDLC, for PPP, including IP, IPX, NetBEUI/LLC, or AppleTalk. This is the choice that applies in most cases, in particular when DIALs clients are being used.
   - Enable **Shell** to support raw asynchronous data preceded by three carriage returns. This is what an asynchronous terminal or a terminal emulation software package will be using. You need this if you want to allow command line shell access.

     Note: You must enable the Shell datalink for a phone group if you want to access the command shell; it is not automatically available.
   - Enable **Autoshell** to force the command shell to pop-up after the specified interval.
8. In the Call Type area, select either the **Use Switch′s Call Type** or **Force Call Type** radio button using the following criteria:
   - Enable **Use Switch′s Call Type** if you want the 8235 DIALs Switch to use the information provided by the central office switch to determine the call type. For ISDN PRI lines this will be an information element in the call setup message.
   - Enable **Force Call Type** if you want to define a call type that this phone group requires. Incoming calls that do not comply with this call type will be rejected.

     If you enable Force Call Type in the Call Type area, select one of the call types described below to be the default call type:

     Digital — Direct ISDN over PRI. This call type uses synchronous HDLC framing. It does not require a modem. The caller uses a digital line.

     Digitized-Analog — Analog over T1/PRI or T1/robbed bit. This call type is used for digital data over an analog line that has been digitized. It requires a digital modem in the 8235 DIALs Switch and uses asynchronous HDLC framing. The caller uses an analog line and a modem.

     Digital Leased Line — This call type is supported only for a LAN-to-LAN connection. The connection is made automatically when the 8235 DIALs Switch boots up, and the

specified WAN interfaces timeslots are reserved for this LAN-to-LAN connection.

V.120 This selection forces the use of V.120 encapsulation over digital connections.

Note: If the call type is Digital Leased Line, the phone number configuration is ignored because no dialing is needed to bring up the leased line. The Signaling Type on the Slotx Configuration page for the associated WAN interface (see Figure 26 on page 53 for T1 and Figure 27 on page 57 for E1) must be set to None with HDLC or inverted HDLC data format.

- You can click on **OK** from any of the Phone Group windows (General, Timeslots, Phone Numbers, or Modes) to save the phone group. However, the General page alone is not sufficient, so you will want to move on to the Timeslots page.

5.3.8.1 Configuring the Phone Group Timeslots Page

This section describes how to configure WAN interfaces and their timeslots that are used by a particular phone group.

A timeslot is a 64 kbps portion of bandwidth on a WAN interface. It is the smallest usable subdivision of a line. There are 24 time slots on a T1 WAN interface and 32 timeslots on an E1 WAN interface. An ISDN B-channel uses one timeslot.

For an interface (line), you can configure each of the timeslots to be associated with a particular phone group.

To configure the WAN interfaces associated with a phone group (and optionally configure their timeslots) do the following:

1. Select **Timeslots** from the Configure drop-down list on any of this phone group′s configuration pages. The Phone Groups Timeslots configuration page appears.

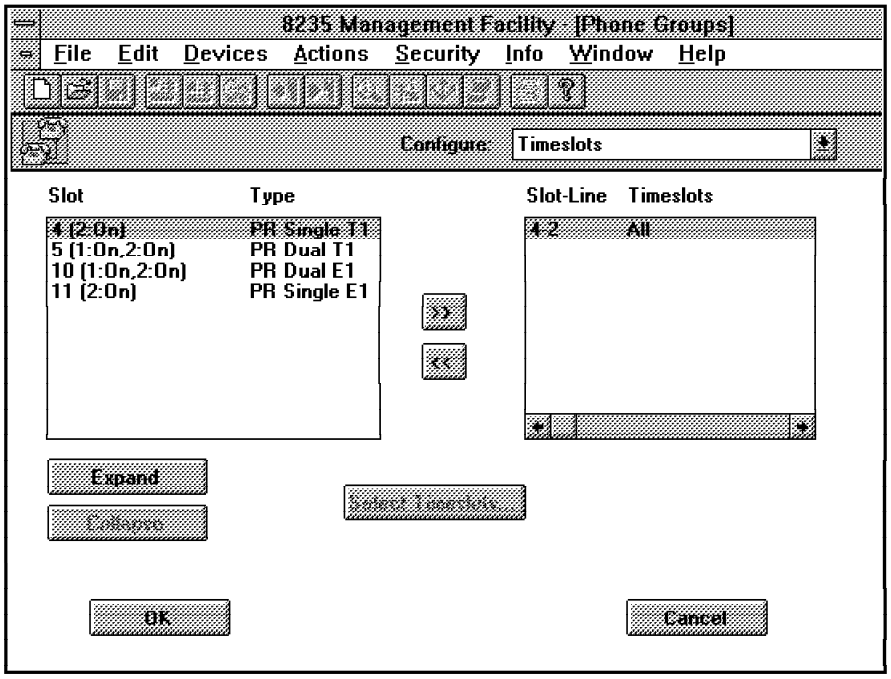


Figure 29. Phone Groups Timeslots Configuration Page

2. Select a slot containing a WAN interface from the list of slots and types.

   If the slot contains a multiple line interface and you want to select only one of the lines, click on **Expand** to view the lines on this interface. (Click on **Collapse** again to reverse this.)

3. To add one or more lines to this phone group, select the lines you want to add and click on the **> >** button. The lines are added to the slot-line timeslot list displayed on the right. This is the actual list of timeslots that currently belong to this phone group.

   The Select Timeslots button can now be activated by clicking on a line in the slot-line timeslot list.

4. To remove a line from this phone group, select the slot-line in the list on the right and click on the **< <** button.

5. To edit the timeslots for a line, select the associated slot-line number in the list on the right, and then click on **Select Timeslots**. The Select Timeslots window appears showing the slot, line and type of WAN card.

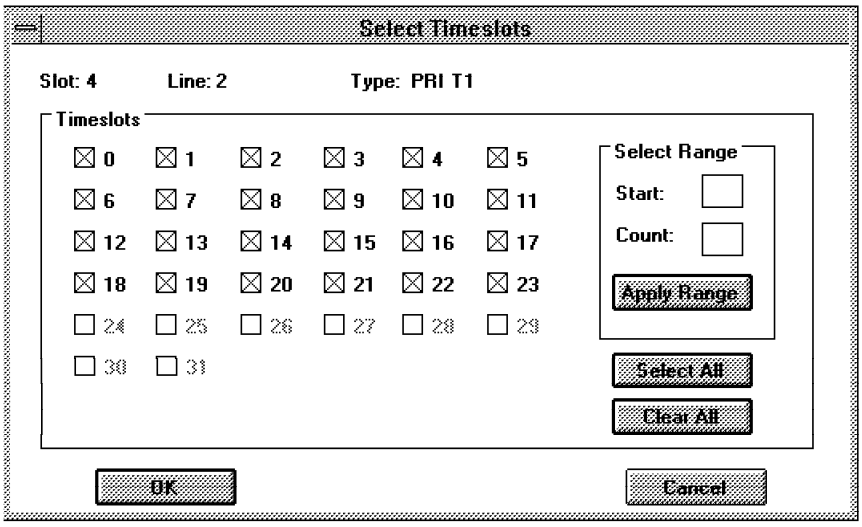


Figure 30. Select Timeslots Window

6. Select the individual timeslots that you want to be associated with this phone group. By default, all available timeslots on the line are selected.
7. You can select a range of timeslots that you want to be associated with this phone group by using the fields in the Select Range area.
8. To select all timeslots, click on **Select All**.
9. To de-select all timeslots, click on **Clear All**.
10. Click on **OK** to accept the changes and return to the Phone Groups Timeslots configuration page.
11. Click on **OK** to close the Phone Groups Timeslots configuration page and accept the changes. A dialog box appears if you have not yet configured any phone numbers. See 5.3.8.2, “Configuring the Phone Group Phone Numbers Page” for more information about configuring phone numbers for a phone group.

5.3.8.2 Configuring the Phone Group Phone Numbers Page

This section describes how to configure the phone numbers associated with a particular phone group. The configured phone numbers are the numbers for which the 8235 DIALs Switch is willing to accept calls over the configured WAN interfaces. They must match the phone numbers assigned by the service provider.

The phone numbers in a phone group must support the configuration described on the Phone Groups General configuration page (see Figure 28 on page 60). If the call type is Digital Leased Line, the phone number is ignored because no call is answered or originated.

You cannot enter the same phone number in more than one phone group.

Note: The 8235 DIALs Switch parses an incoming phone number from right to left, searching for a match in a phone group. It searches all phone groups that are associated with the line on which the call arrived. If an exact match is not found, the first phone group found with the longest match is used. If no match is found, the call is rejected and an error message is written to the log.

1. Select **Phone Numbers** from the Configure drop-down list. The Phone Groups Phone Numbers configuration page appears.

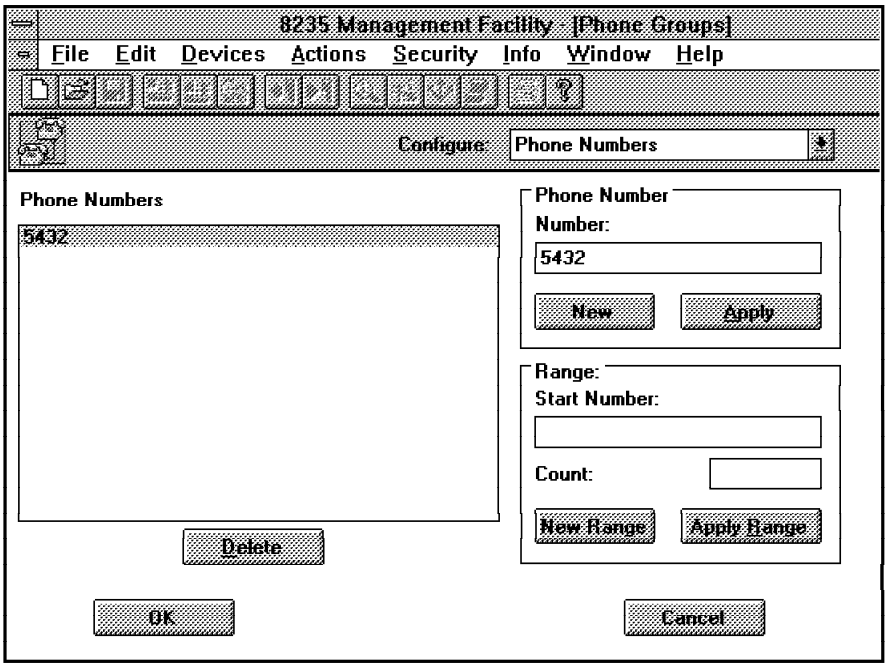


Figure 31. Phone Groups Phone Numbers Configuration Page

2. To add individual phone numbers to this phone group, do the following steps:
   - In the Phone Number area, type a phone number without punctuation in the Number field.
   - Click on **New** to add this phone number to the phone group. It will appear in the Phone Numbers list on the left.

   Note: You must enter at least one phone number for a phone group and you must not enter the same phone number in another phone group. If you configure a phone number in more than one phone group, the 8235 Management Facility displays an error.
3. To add a range of phone numbers to this phone group, enter the following information in the Range area:
   - Type a phone number in the Start Number field.
   - Enter a count value for the number of phone numbers you want to add.
   - Click on **New Range** to add this range of consecutive phone numbers to the phone group. The range of numbers will be displayed in the Phone Numbers list on the left in one single line.
4. To modify individual phone numbers configured for this phone group, do the following steps:
   - Select a phone number you want to change in the Phone Numbers list.
   - In the Phone Number area, type a new phone number.
   - Click on **Apply** to replace the selected phone number with the one you entered.
5. To modify a range of phone numbers configured for this phone group, do the following:

- Select a range of phone numbers listed in the Phone Numbers list.
- Type a phone number in the Start Number field.
- Enter a count value for the number of phone numbers you want to add.
- Click on **Apply Range** to replace the selected range of phone numbers with the new range.

6. To remove phone numbers from a phone group, use the **Delete** button on a selected single number or range of numbers.
7. Click on **OK** to accept your changes and close the Phone Groups Phone Numbers configuration page.

5.3.8.3 Configuring the Phone Group Modems Page

Note

If you configure the call type for a phone group as digital, you do not need to configure a modem; you must, however, configure a modem if the call type is digitized-analog or you elected to use the switch's call type.

To configure a modem for the phone group:

1. Select **Modem** from the Configure drop-down list. The Phone Groups Modem configuration page appears.

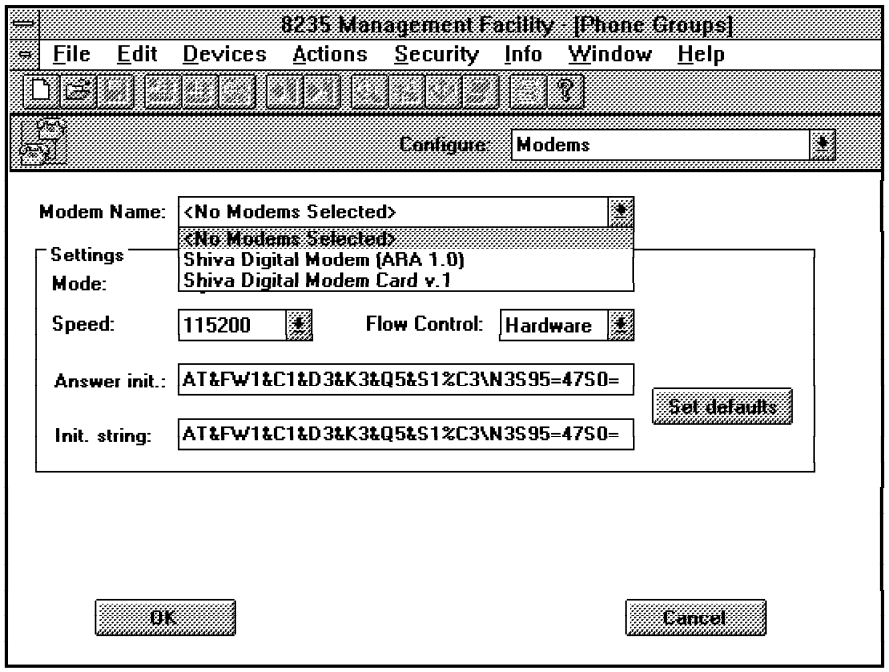


Figure 32. Phone Groups Modem Configuration Page

2. Select the correct modem name from the Modem Name drop-down list for the modems you are using. The initial default settings are displayed in the Settings area. If you are not sure, select **Shiva Digital Modem Card v.1**.

   Note: The digital modem card supports PPP, SLIP, ARA V2, and shell access.

3. If necessary, you might change the default settings for the speed, flow control, answer initialization, or the call initialization string.
4. Click on **Set Defaults** if you want to restore the initial default settings for the selected modem.
5. Click on **OK** to save the phone group configuration.

5.3.8.4 Attaching Phone Groups to a WAN Interface

There are two different ways to attach a phone group to a WAN interface. When a phone group is created, you cannot complete the configuration and save the phone group unless you have configured at least one WAN interface or a subset of its timeslots. You can always revisit this configuration page and apply changes (see 5.3.8.1, “Configuring the Phone Group Timeslots Page” on page 62).

The other method is from the Slots configuration page. To use this method to attach a phone group to a WAN interface, do the following:

1. Choose **Slots** from the Configure drop-down list.
2. On the Slots Configuration Page (see Figure 22 on page 48), click on the slot that contains an E1 or T1 WAN interface.
3. For multiple interfaces, you can click on **Expand** to select one of the lines if you want to attach only one of the lines to a particular phone group. Click on **Collapse** to reverse the expansion.
4. Click on **Attach Phone Group** to display the Attach Phone Groups window. The Attach Phone Groups window lists the available phone groups for this interface (line).

   Note: You must have created a phone group before.
5. From the Attach Phone Groups window, perform one of the following actions:
   - Select one or more phone groups and then click on **OK**.
   - Click on **Cancel** if you do not want to change the phone groups that are attached to this line.

Note: For multiple contiguous selections, hold down the Shift key while you make your selections. For multiple non-contiguous selections, hold the Ctrl key while selecting.

5.3.9 Configuring Incoming Phone Group Pools

There are no default incoming phone pools; you must assign phone groups to an incoming pool yourself.

The following procedures describe how to create an incoming phone group pool and attach phone groups to it.

To create a phone group pool:

1. Select **Phone Groups: Pools** from the Configure drop-down list.

   The Phone Groups: Pools configuration page appears.

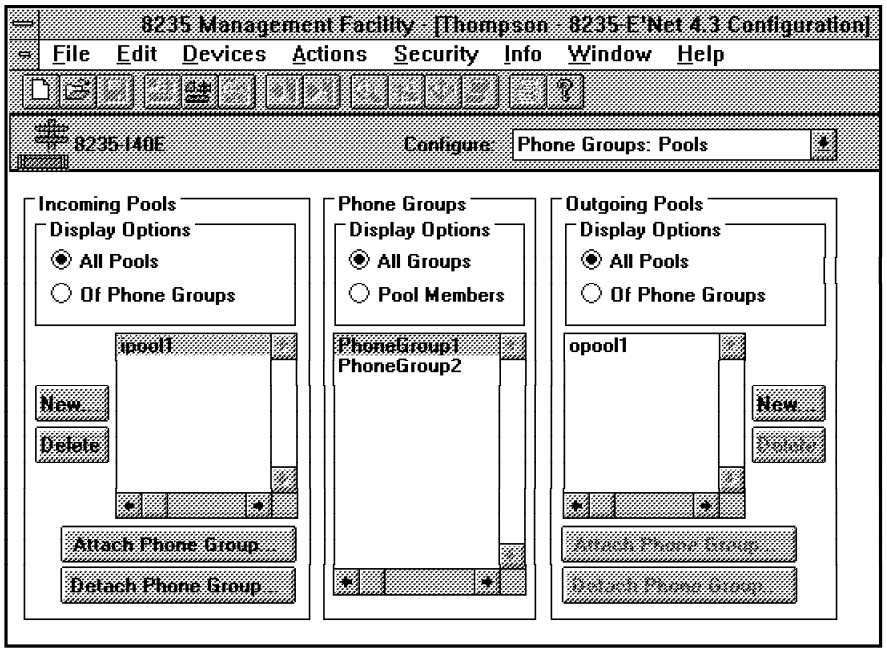


Figure 33. Phone Groups: Pools Configuration Page

2. Click on **New** to display the New Pools dialog box.
3. Type the name of the new pool in the Pool Name field and then click on **OK**. You have created a new, empty pool.

To attach a phone group to this pool, take these steps:

1. Select the pool name from the Incoming Pools area.
2. Select the **All Groups** radio button in the Phone Groups area.
3. Select the phone groups you want to include in the pool from the Phone Groups area. To select multiple phone groups, hold down Ctrl while you make your selections.
4. Select the **Attach Phone Group...** button next to the Incoming Pools list. A dialog box is displayed asking you to confirm whether the phone groups that are displayed are the ones you want to include in the incoming phone group pool. Click on **OK** to accept the list, or click on **Cancel** to reject it.

To detach a Phone Group from an Incoming Pool, follow the same steps respectively, using the **Detach Phone Group...** button.

To delete selected incoming pools, use the **Delete** button next to them.

5.3.10 Configuring Outgoing Phone Group Pools, Display Pools

Follow the same steps as for incoming pools respectively with the corresponding buttons within the Outgoing Pools Area of the Phone Groups:Pools configuration page (Figure 33).

To display all members of a pool:

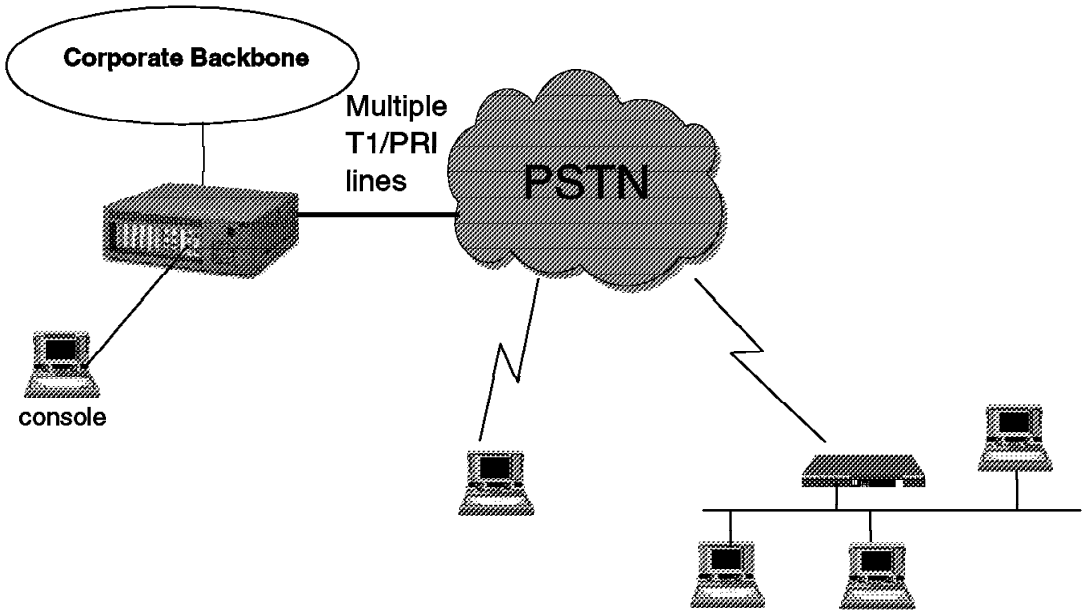
1. Select the **All Pools** radio button in the respective (Incoming or Outgoing) Pools area.
2. Select the pool you want to display.

3. Select the **Pool Members** radio button in the Phone Groups area.

To display all pools that contain a certain phone group:

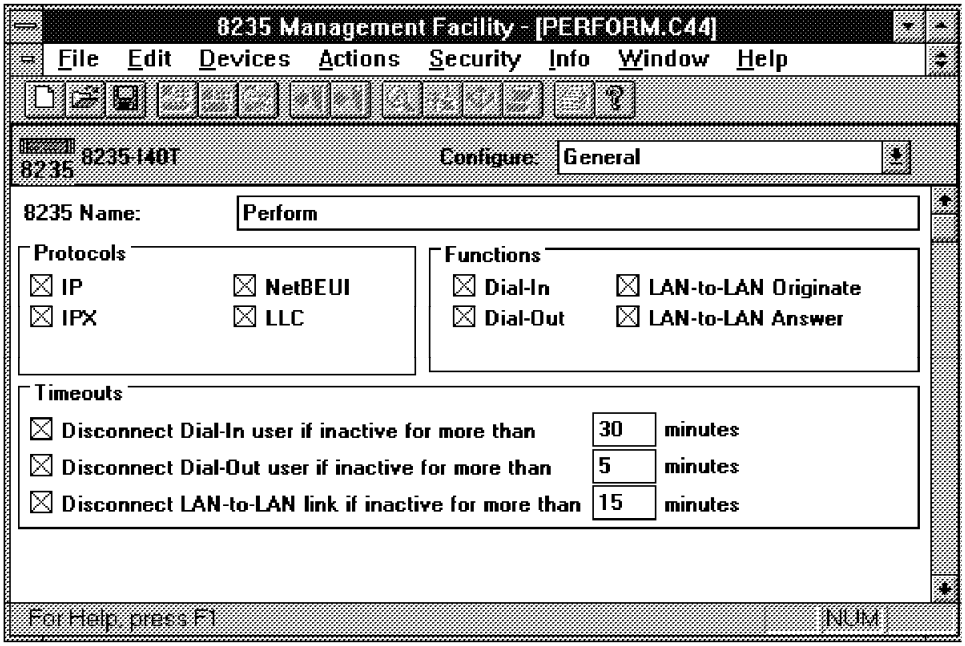
1. Select the **All Groups** radio button in the Phone Groups area.
2. Select the phone group for which you want to get this information.
3. Select the **Of Phone Groups** radio button in the respective Pools area.

5.4 Sample Scenario and Configuration of 8235-I40



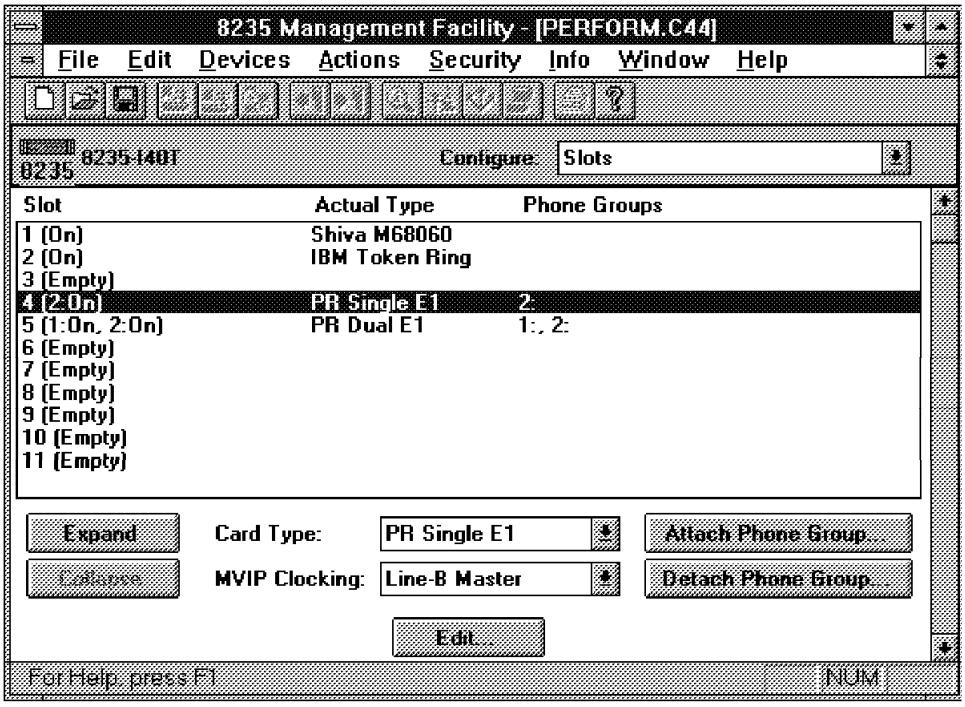
Note: The connection between the console and the 8235-I40 is a null modem.

5.4.1.1 Configuring General 8235-I40 Information



Note: Default values were changed.

5.4.1.2 Configuring Slot4 for E1 Card (Primary Rate)



Tips

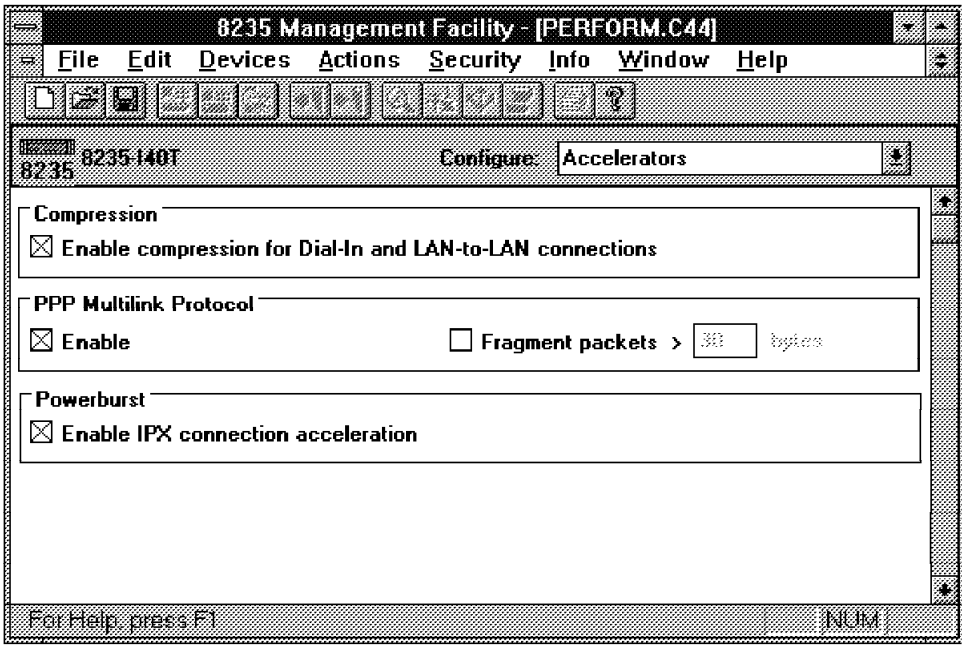
- Configure serial ports for CPU card.
- **Signaling**: Specifies how calls are brought up and taken down on a line. It is the protocol used between the switch and the WAN interface on how to handle a call.
- If the analog modem connections fail, review your choices for MVIP Clocking and LBO.

5.4.1.3 Sample CARDS.INI File

```
[PRI_ISA64]
453images=pr453.bsf
433images=pr433.bsf
images=pr453.bsf

[PRI_ISA48]
453images=pr453.bsf
433images=pr433.bsf
images=pr453.bsf

[PRI_ISA32]
453images=pr453.bsf
433images=pr433.bsf
images=pr453.bsf

[PRI_ISA24]
453images=pr453.bsf
433images=pr433.bsf
images=pr453.bsf

[SHIVA_DMC_V1]
453images=dm453.bsf;rc453.bsf;fl453.bsf
433images=dm433.bsf;rc433.bsf;fl433.bsf
images=dm453.bsf;rc453.bsf;fl453.bsf

[SHIVA_DUAL_T1]
453images=sw453.bsf
images=sw453.bsf

[SHIVA_DUAL_E1]
453images=sw453.bsf
images=sw453.bsf

[SHIVA_QUAD_T1]
453images=sq453.bsf
images=sq453.bsf
```

Note: This file is used to tell the Management Facility which driver files are sent to the 8235-I40 when **Set Configuration** is selected. If a patch file is released to upgrade the adapter card drivers, the filename will need to be manually edited here.

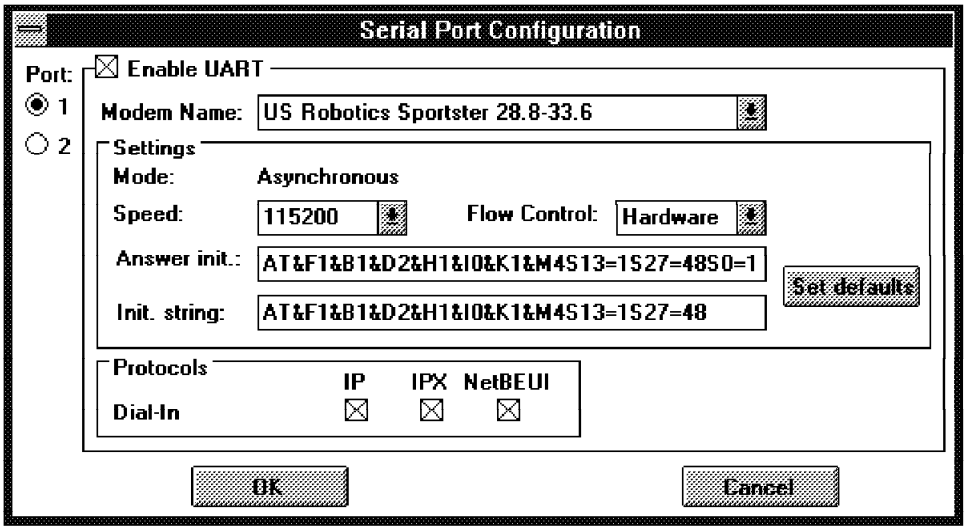
5.4.1.4 Configuring Accelerators



Note:

- Refer to Additional Configuration page for parameters.
- Must purchase a key for Powerburst accelerators to be enabled.

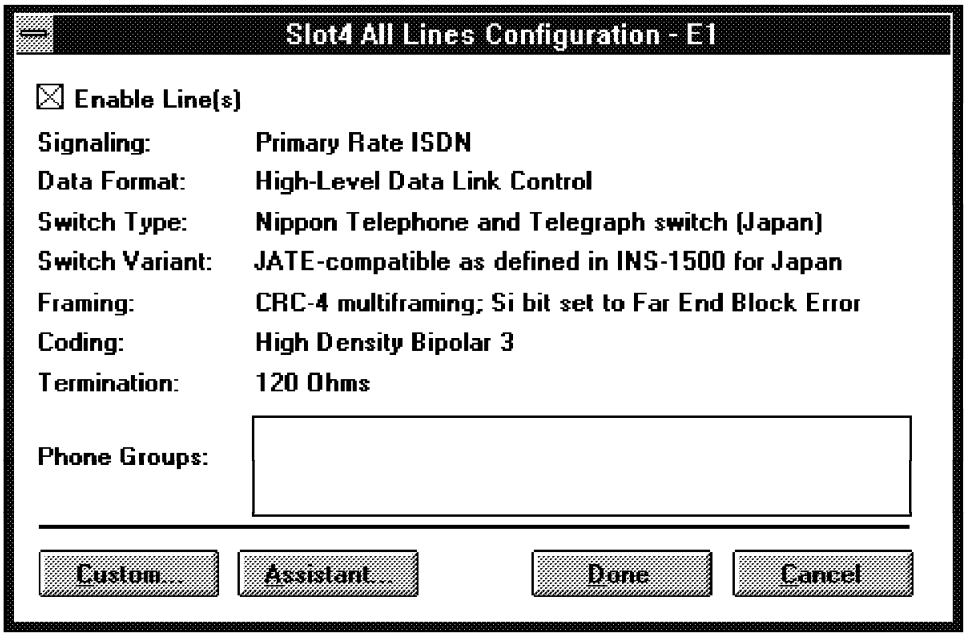
5.4.1.5 Enabling UART Port



Tips

- Through a null modem connected UART, you can monitor the boot process, view configuration, addressing, log messages, and available resources, and run diagnostics. Through a modem connection to the UART, you can view and edit the configuration, view the log, and see available resources. The difference lies in that the 8235-I40 must be up and running before a connection can be established over the modem.
- A complete list of modems may be found in the modems.ini file.

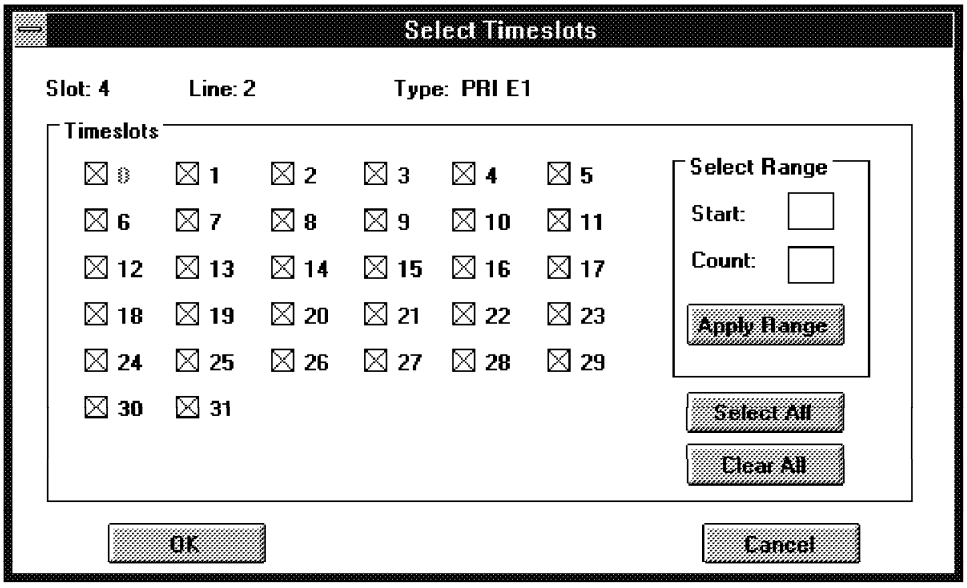
5.4.1.6 Slot4 All Lines Configuration



Tips

- Framing: Physical framing method used to format data on the line.
- Termination: Resistance in Ohms to terminate the line. (120 Ohms for twisted pair and 75 Ohms for coaxial.) This setting is only for E1 lines.

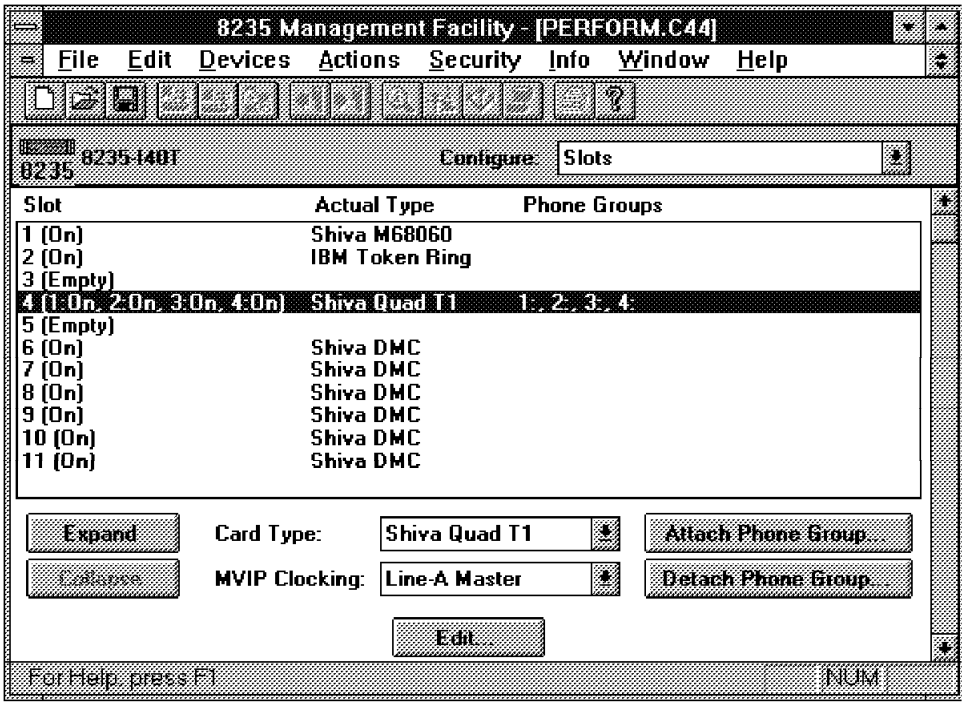
5.4.1.7 Slot4 Timeslots Configuration



Tip

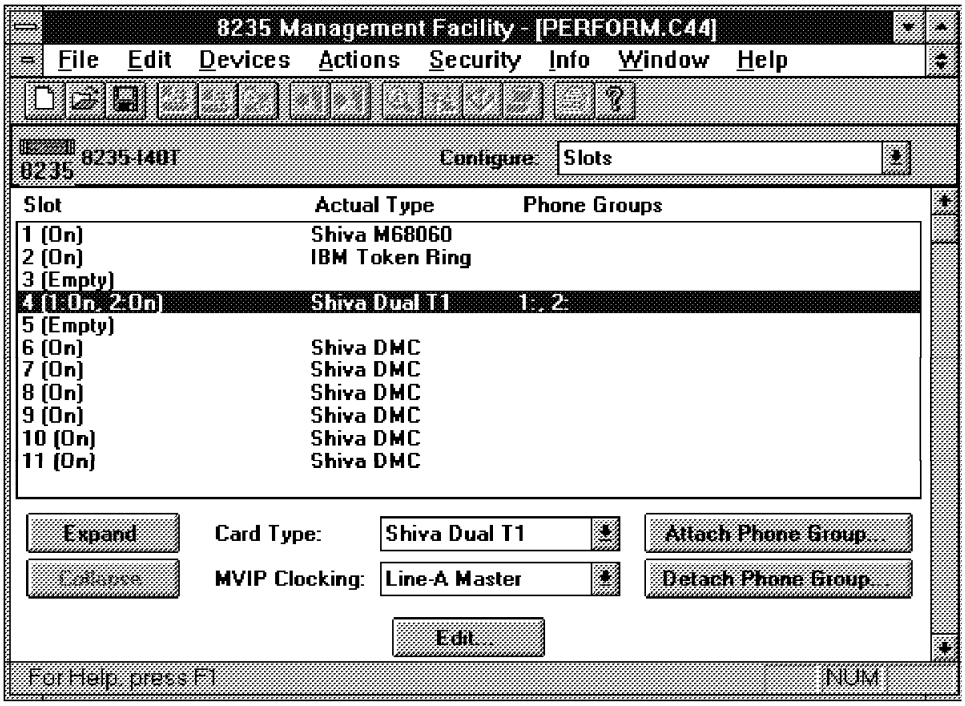
Timeslot 16 is reserved for synchronization, 30 for signaling.

5.4.2 Configuring Slot4 for T1 Quad Card

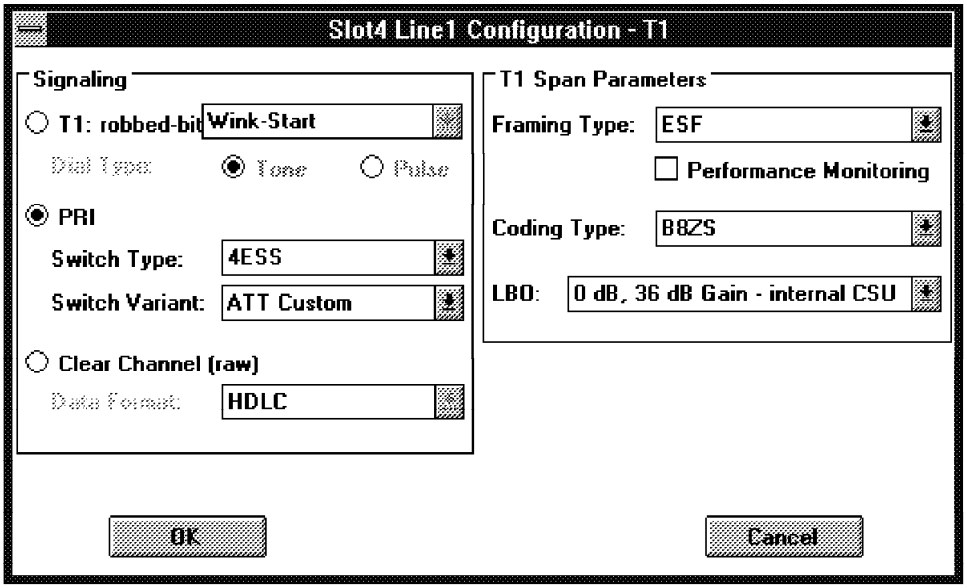


Note: This card is currently supported in North America. It is capable of supporting 96 simultaneous connections. However, only six DMCs for analog calls are supported, which equals 72 calls. Physically, seven DMCs may be inserted, for a capacity of 84 calls.

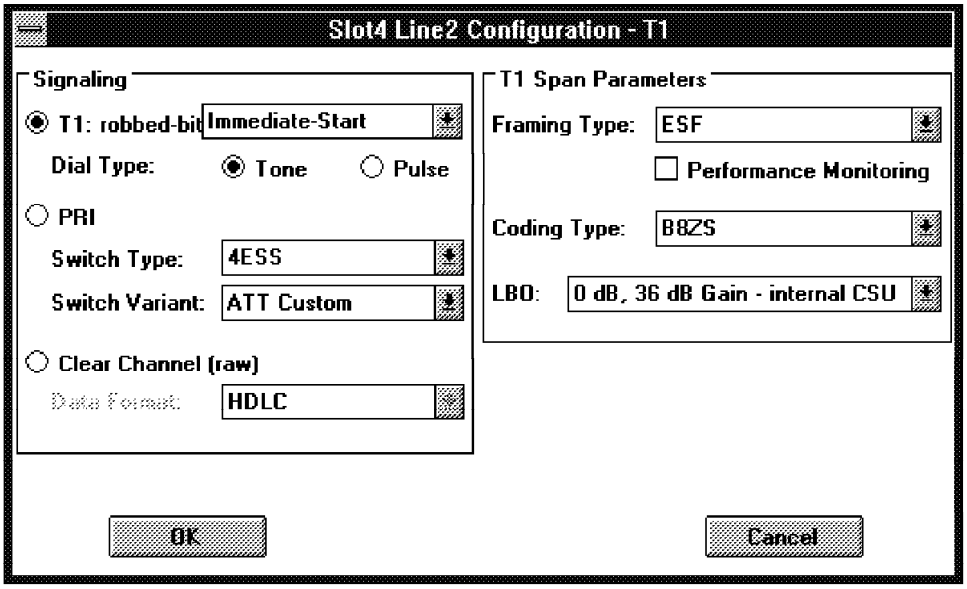
5.4.2.1 Configuring Slot4 for T1 Dual Card



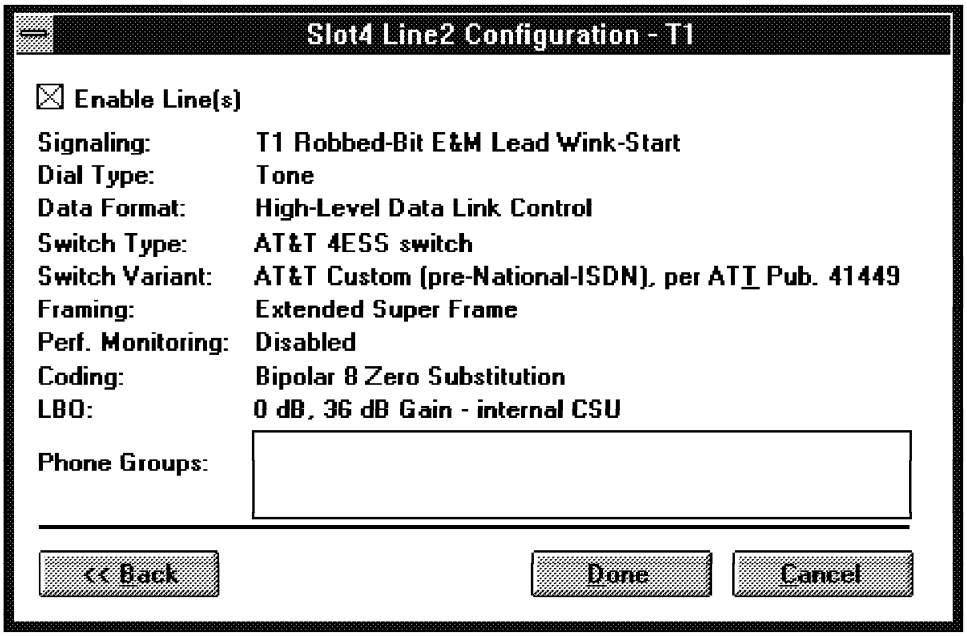
5.4.2.2 Enable Slot4 Line1 for Primary Rate Signaling



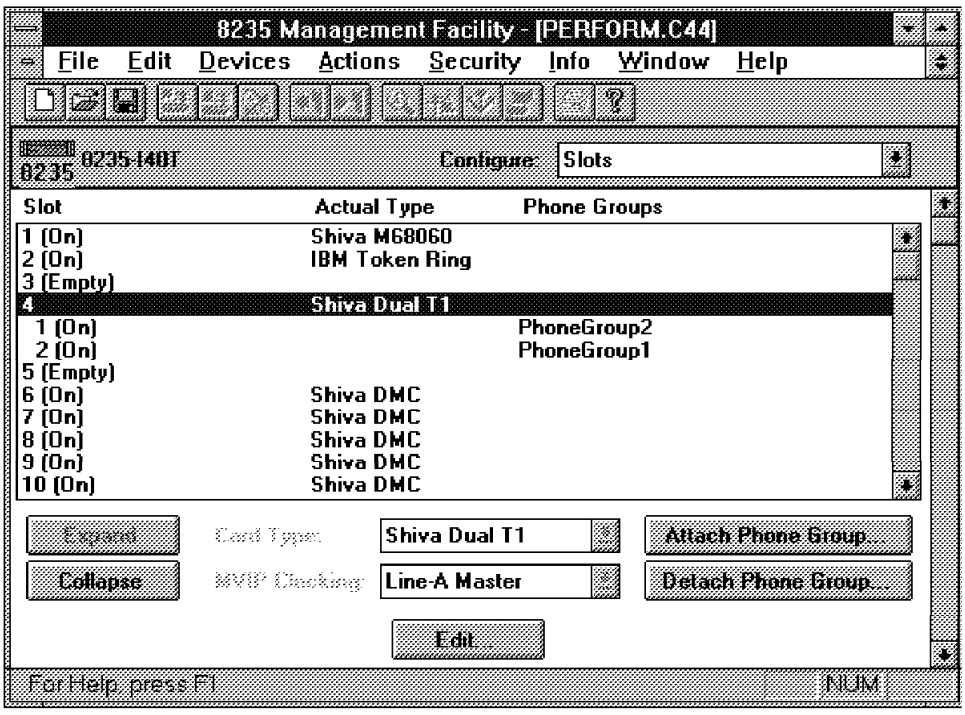
5.4.2.3 Enable Slot4 Line2 T1 Signaling



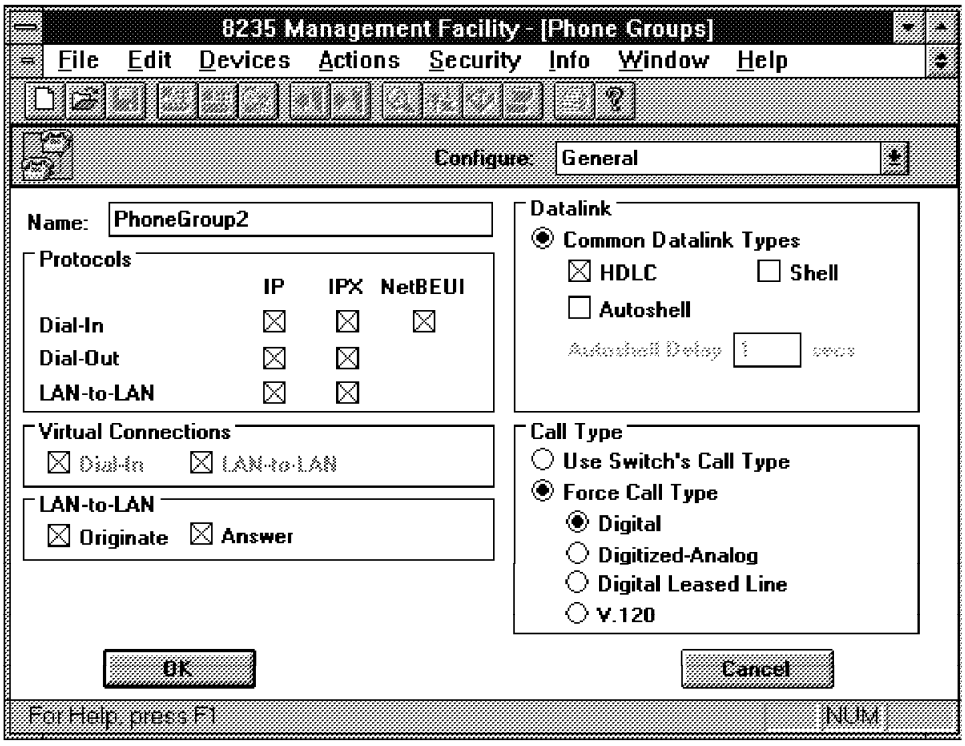
5.4.2.4 Enable Slot4 Line2 Signaling Summary Page



5.4.2.5 Slot4 Expanded - Attached PhoneGroups1 and 2



5.4.2.6 Configure PhoneGroup2 for Slot4 Line 1



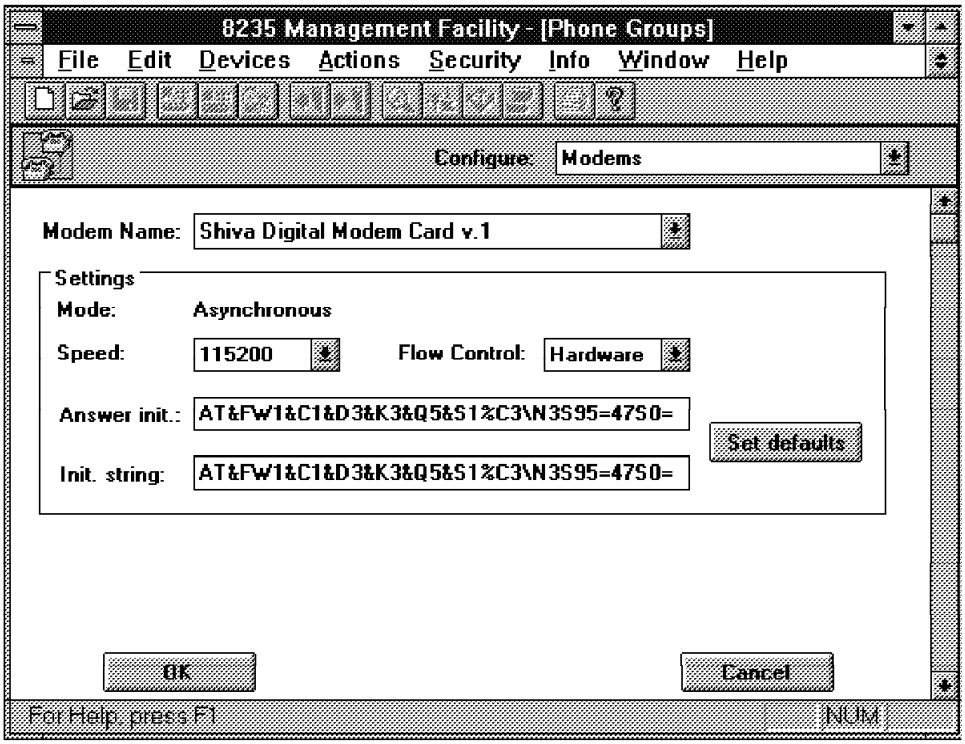
Note: Digital Leased Line should be selected for LAN-to-LAN trunk connections.

Note: AppleTalk is not shown because this configuration screen is from a token-ring device.

Tips

- Enable **Shell** for user access.
- Set MVIP Clocking if using digitized-analog or the switch's call type.
- ***Case Sensitivity***: When editing a configuration file using Shell or BootP, ensure that information entered into the Phone Group DataLink variable uses the correct case. If the following variables are not entered correctly, they will not be recognized by the 8235 Management Facility during the next Set Configuration: ARAv1, ARAv2, Shell, and HDLC.
- Show Stoppers (could not find parameter to enable the shell)
  - Shell Access
  - Force Call Type (could not rely on switch to discriminate)
- V.120 rate adaptation for Apple Remote Access (ARA) along with Force Call Type
- For both synchronous ISDN and V.120 connections simultaneously, the T1 or PRI line connecting to this slot must have one distinct telephone/directory number for each protocol. It should not be necessary to dedicate timeslots to the particular protocols.

5.4.2.7 Configuring Analog Modems (DMC) for PhoneGroup



Tips

Update DMC modems to 33.6 kbps

1. Update 8235 to 4.5.3
2. Go to shell and execute `DMC mupdate all`

   Note: Will update all modems not being used.

Testing DMCs:

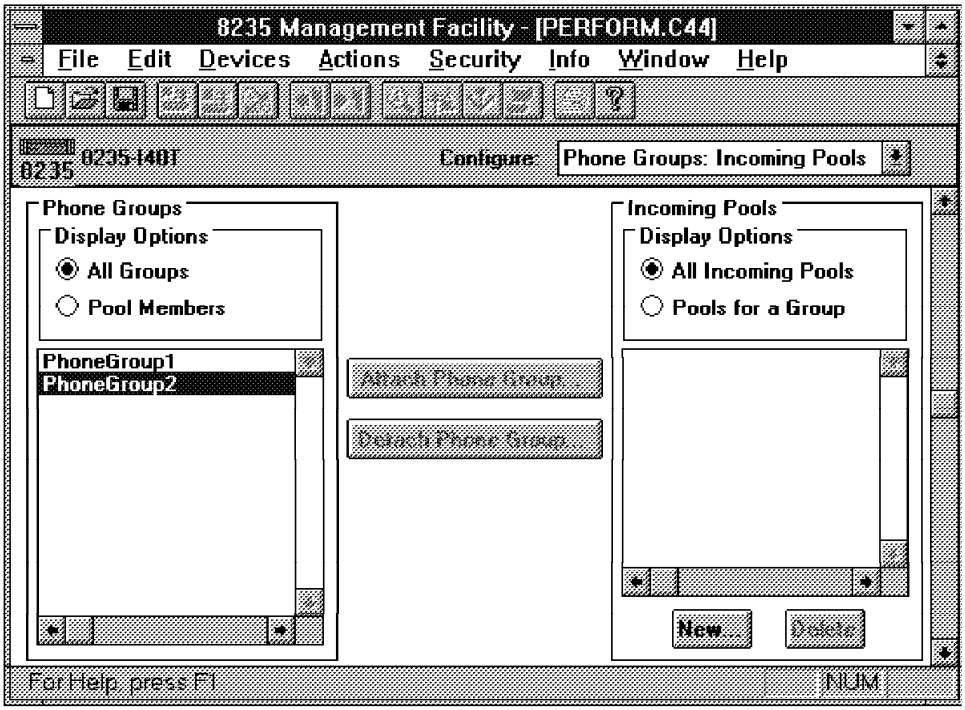
1. Update 8235 to 4.5.3
2. Go to shell and type `DMC Test_allcards`
3. Go to shell and type `DMC Test_1slot <slot number>`
4. Go to shell and type `DMC Test_modempair <slot> <modem1> <slot2> <modem2>`.

Note: The cards are based on Rockwell chips, shipping with V.34 code installed. Customers may need to perform a DMC update process after installing 4.5 firmware to upgrade their DMC cards from V.34 to V.34bis. To check the current code level on each modem, get the DMC info (through the Device Info), as shown in Figure 24 on page 50. Firmware Version 1.441 is V.34, Version 1.600 or higher is at least V.34bis.

The following is the DMCARDS.INI file:

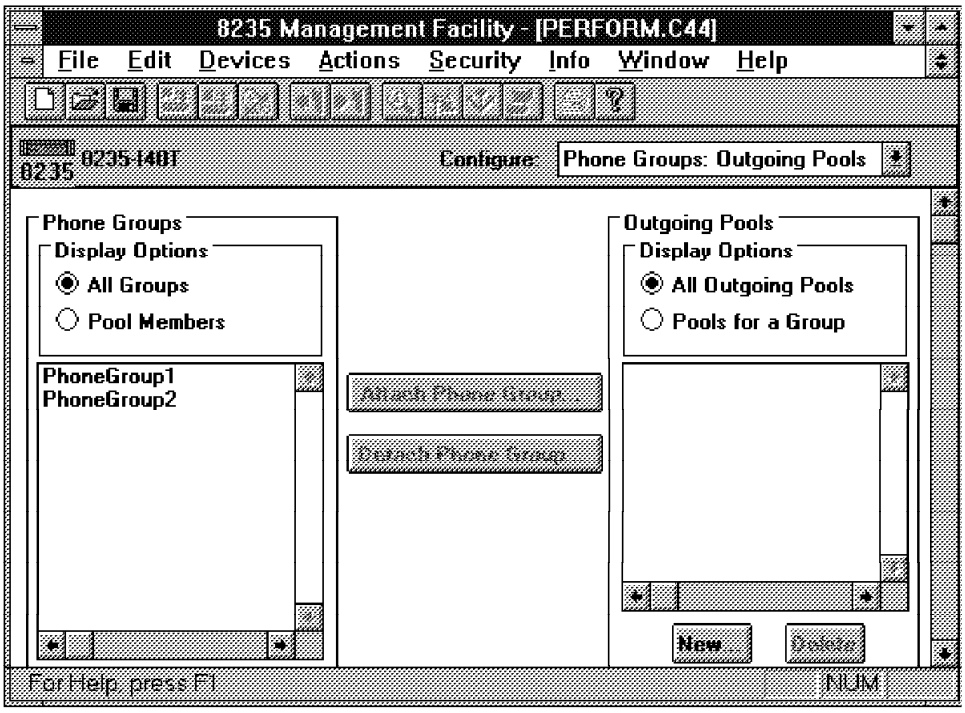
```
[Shiva Digital Modem Card v.1]
InitString=AT&FW1&C1&D3&K3&Q5&S1%C3\N3S95=47S0=0
AnswerInit=AT&FW1&C1&D3&K3&Q5&S1%C3\N3S95=47S0=1&W
BPSRate=115200
FlowControl=Hardware

[Shiva Digital Modem (ARA 1.0)]
InitString=AT&FW1&C1&D3&K3&Q0&S1S95=47S0=0
AnswerInit=AT&FW1&C1&D3&K3&Q0&S1S95=47S0=1&W
BPSRate=115200
FlowControl=Hardware

[<No Modems Selected>]
InitString=AT&FW1&C1&D3&K3&Q5&S1%C3\N3S95=47S0=0
AnswerInit=AT&FW1&C1&D3&K3&Q5&S1%C3\N3S95=47S0=1&W
BPSRate=115200
FlowControl=Hardware
```

5.4.2.8 Configure PhoneGroup2 Incoming Pools



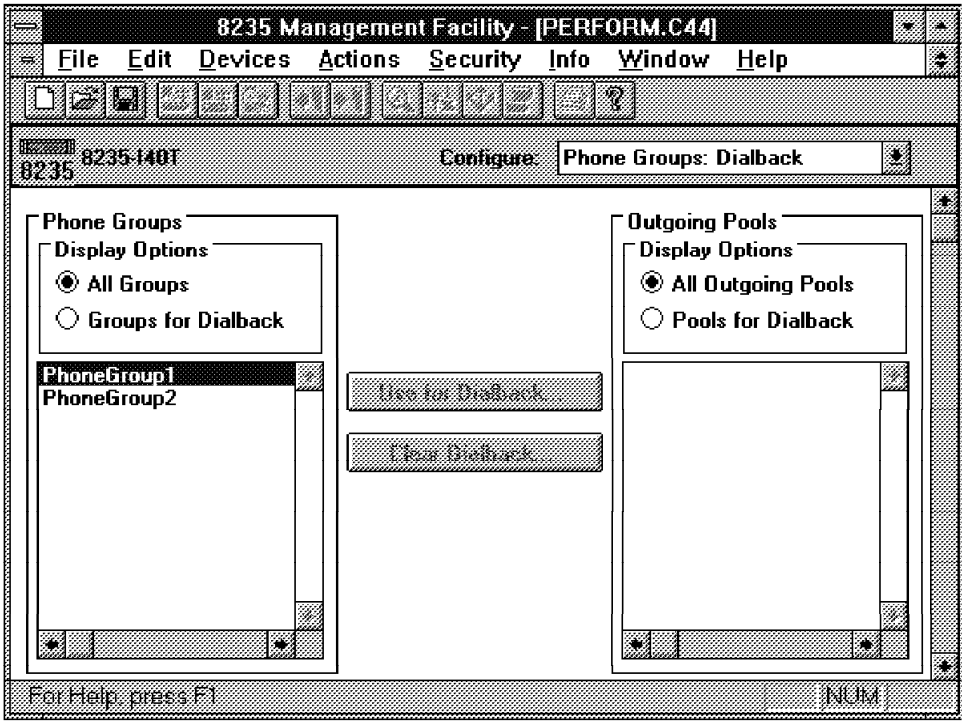
Note: To bind one or more phone groups for dial-in, create a new pool by clicking **New...** and enter a name. Select the pool name, the phone groups you wish to bind, and click **Attach Phone Group**.

5.4.2.9 Configure PhoneGroup2 Outgoing Pools



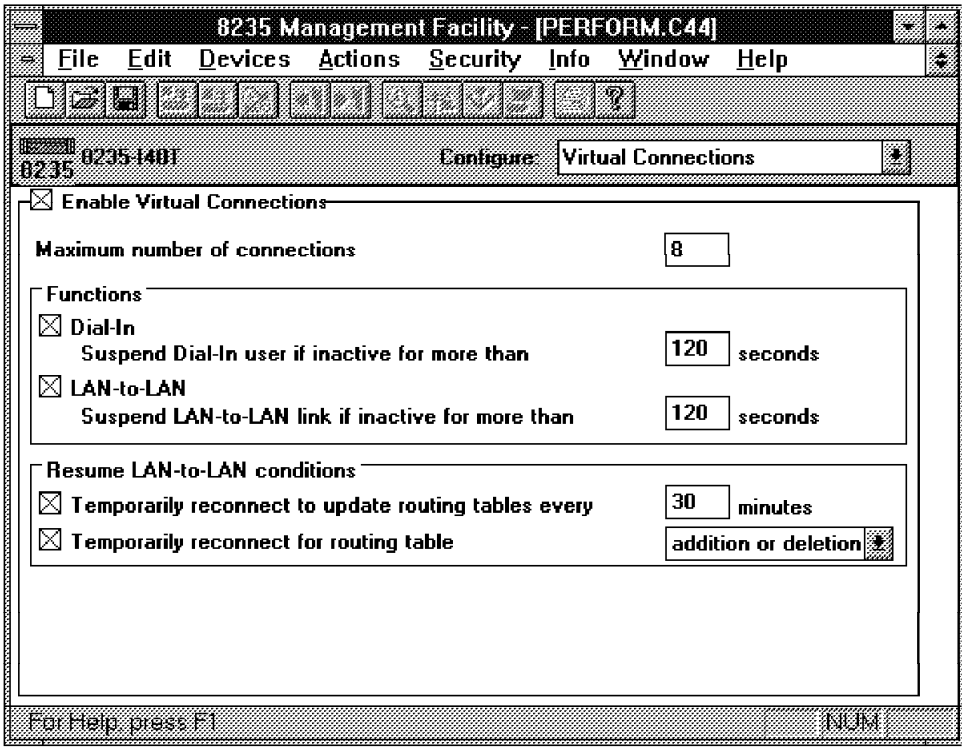
Note: To bind one or more phone groups for dial-out, create a new pool by clicking **New...** and enter a name. Select the pool name, the phone groups you wish to bind, and click **Attach Phone Group**.

5.4.2.10 Configure PhoneGroup1 (Dial-back)



Note: The outgoing pools will be listed here. Select the pool and associated phone groups to use for dial-back connections and click **Use For Dialback**.

5.4.2.11 Enabling Virtual Connections

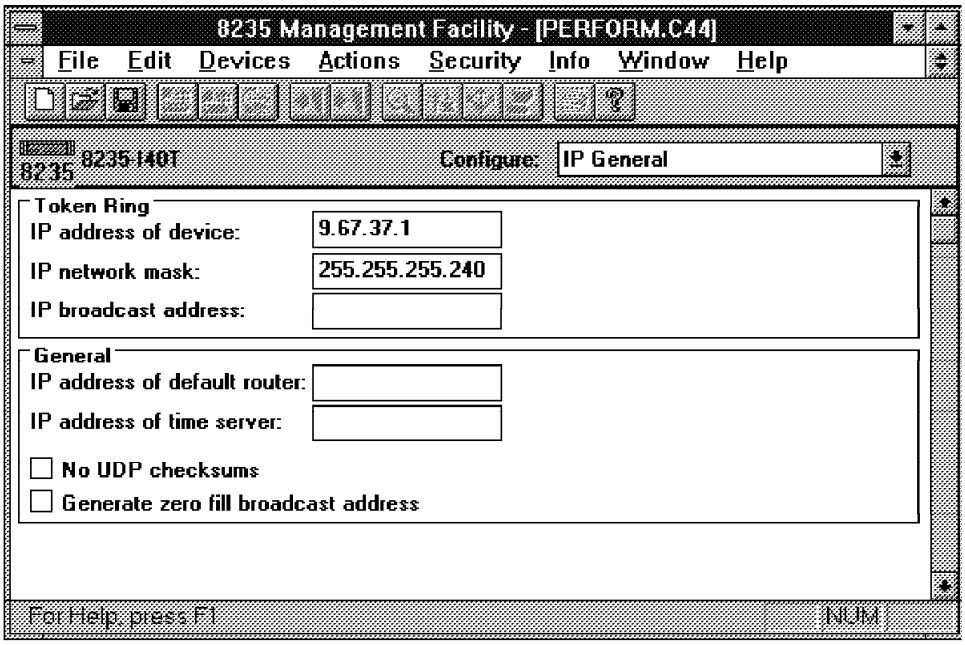


Note: Virtual Connections are used to save on connect time by physically disconnecting the link when no meaningful data travels across the link for a set timeout period.

Warning

If the maximum number of connections is exceeded through both active and virtual connections, then further connections cannot be established until a link becomes available. Make sure that the maximum number is at minimum the physical number of concurrent links possible. However, if this value is set too large, it is possible to have virtualized connections that cannot be reestablished because no slots are available. If this happens, the virtual connection will be lost and the user will have to manually reconnect.

5.4.2.12 Configuring IP General



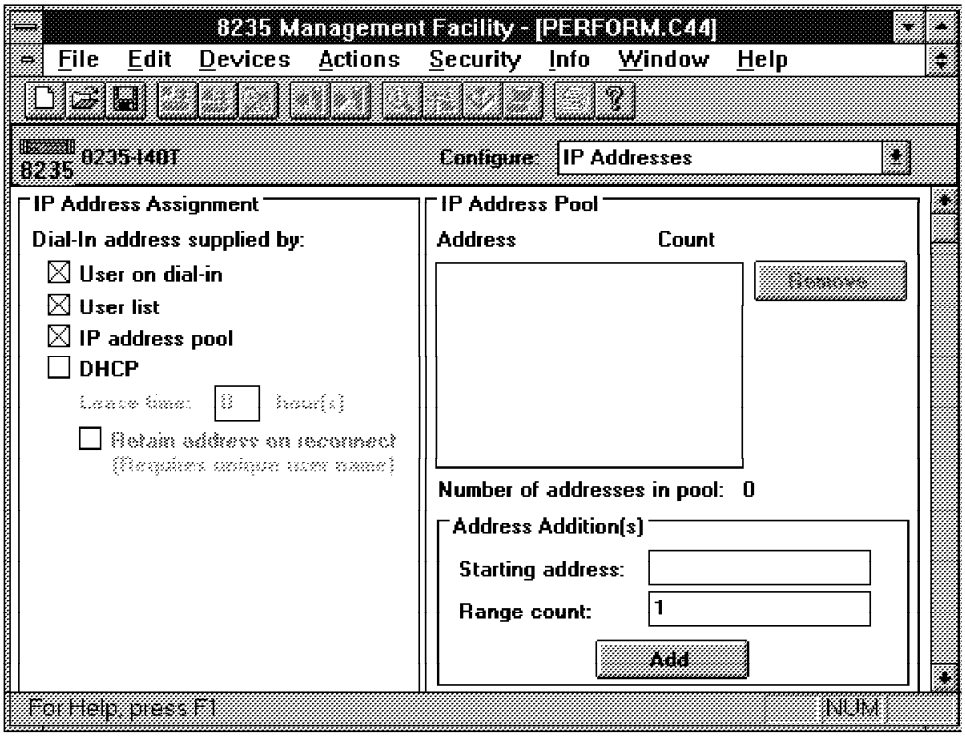
Tips

- To configure an 8235 without an IP address, use IPX or IP Auto download (configure sbootp.ini file, then pin reset the 8235) to give it an IP address.
- Address of Device = Host #
- Network mask = Subnet mask
- Broadcast address = transmits packets to be processed by host
- Address of default router = IP packets destined for remote IP hosts
- Generate zero fill broadcast address = default is all ones.

Possible causes of problems:

1. Don't define the subnet mask if not needed. The 8235-I40 derives an appropriate value if this is not configured.
2. You are using a wrong or duplicate IP address.
3. The router does not have 8235 address in ARP table.
4. The router may not have an updated SAP table.
5. The routing table is invalid because of misconfiguration or RIP broadcasts.

5.4.2.13 Configuring IP Addresses

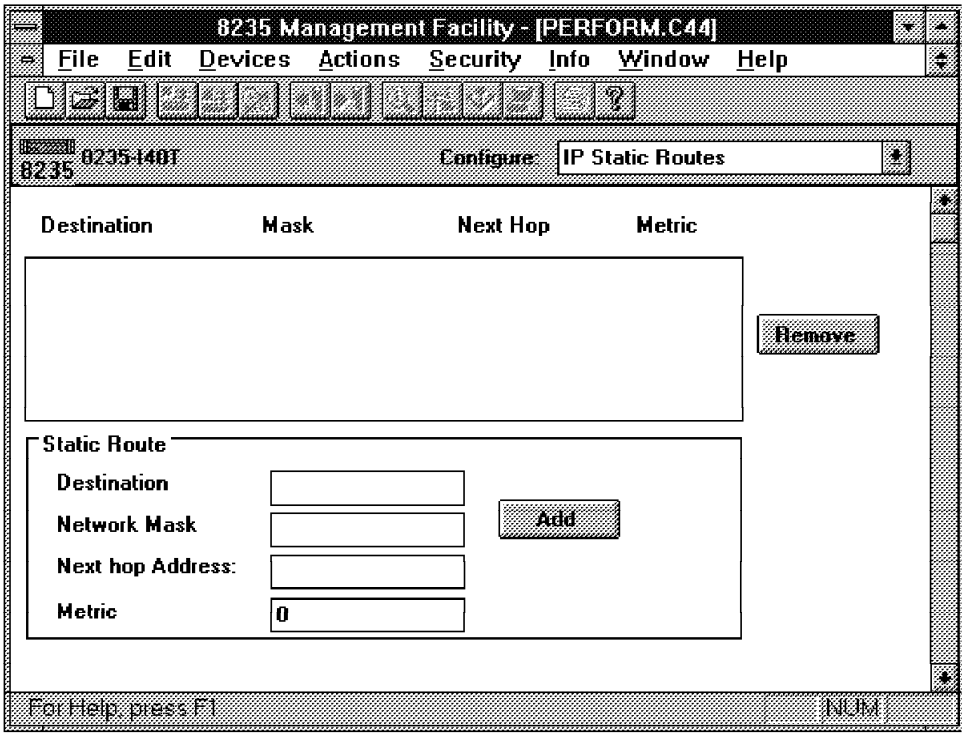


Tips

- DHCP = Not supported for LAN-to-LAN

  Usernames must be unique for **Retain address on reconnect** to be enabled. Otherwise, the 8235-I40 will not know which IP address belongs to which user when they reconnect.

5.4.2.14 Configuring IP Static Routes



Tips

- Destination = Address for static routing
- Network Mask = Significant bits of Destination address

  Example:

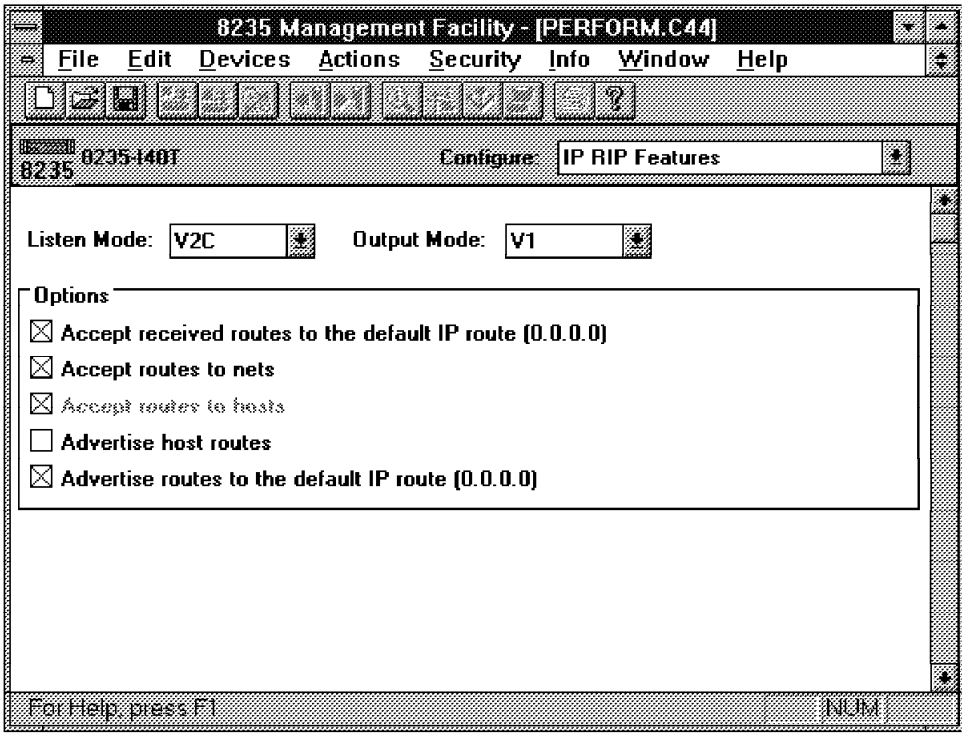
  Destination = 9.0.0.0 Netmask = 255.0.0.0

  All frames destined for addresses from 9.0.0.0 to 9.255.255.255 will be sent to the next hop address

  Destination = 9.0.0.0 Netmask = 255.255.255.0

  All frames destined for addresses from 9.0.0.0 to 9.0.0.255 will be sent to the next hop address
- Net hop Address = Address of router, must be on same local network or device
- Metric = Number of hops between device and destination

5.4.2.15 Configuring IP RIP Features



Tip

Determines how the 8235 shares routing table information with other routers.

- Mode Options:

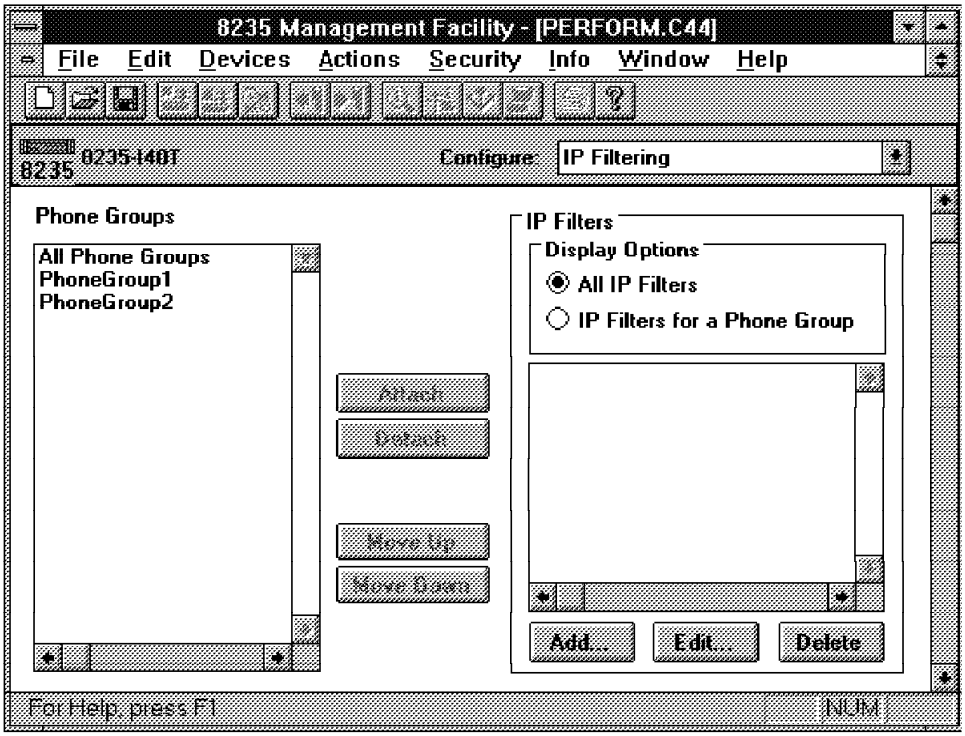
  None = Ignore All RIP broadcasts

  V1 = Do not include subnet

  V2C = 8235 listens for RIP V1 & V2 broadcast packets

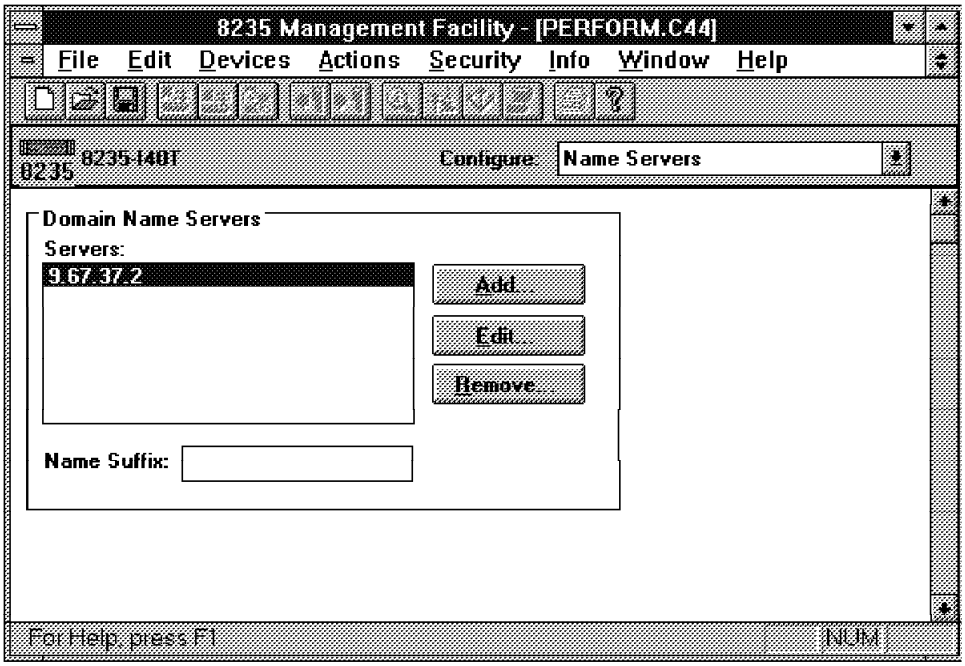
  V2 = Multicast packets includes subnet mask

5.4.2.16 Configuring IP Filtering



Note: See 5.4.3.4, “IP Filtering” on page 94 for more information on IP filtering.

5.4.2.17 Configuring IP Name Servers



Tip

These are DNS servers for the 8235-I40. They will be sent to the dial-in clients if needed during IP protocol negotiations.

5.4.2.18 IP Auto Download

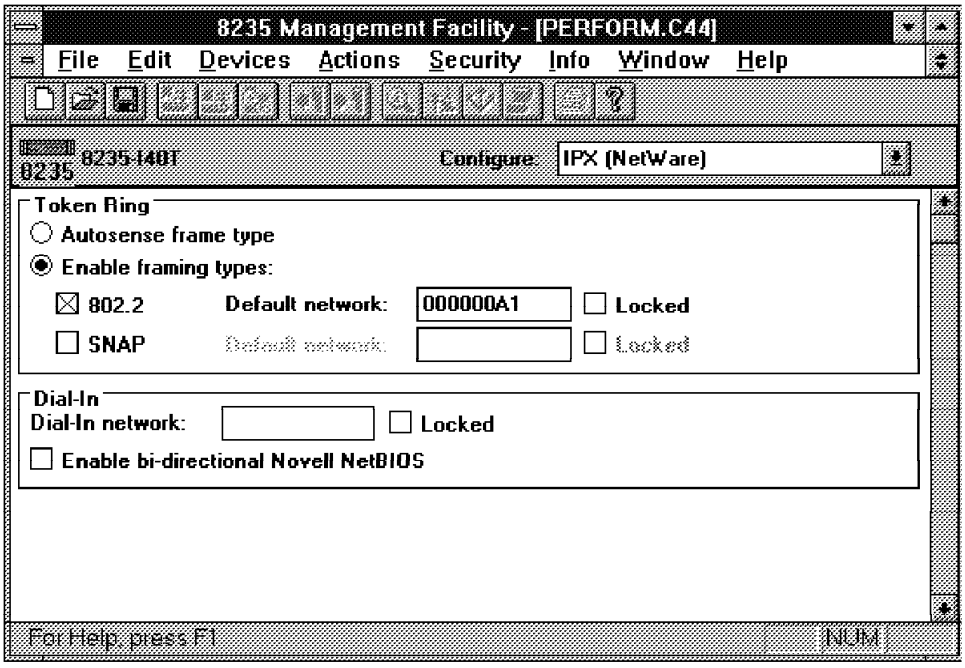
- Edit SBOOTP.INI[1]
- Start Management Facility: Select **Edit**, then **IP Auto Download**[2]
- Pin reset the 8235. See 4.4, “How to Pin Reset the 8235-I40” on page 37 for more information.

  Note: Windows 95 will need an AUTOEXEC.BAT file with path and set variables.

Tip

For 4.5, if the 8235 does not complete the microcode download change the .img file as noted in the Readme file.

5.4.2.19 Configuring IPX



Tips

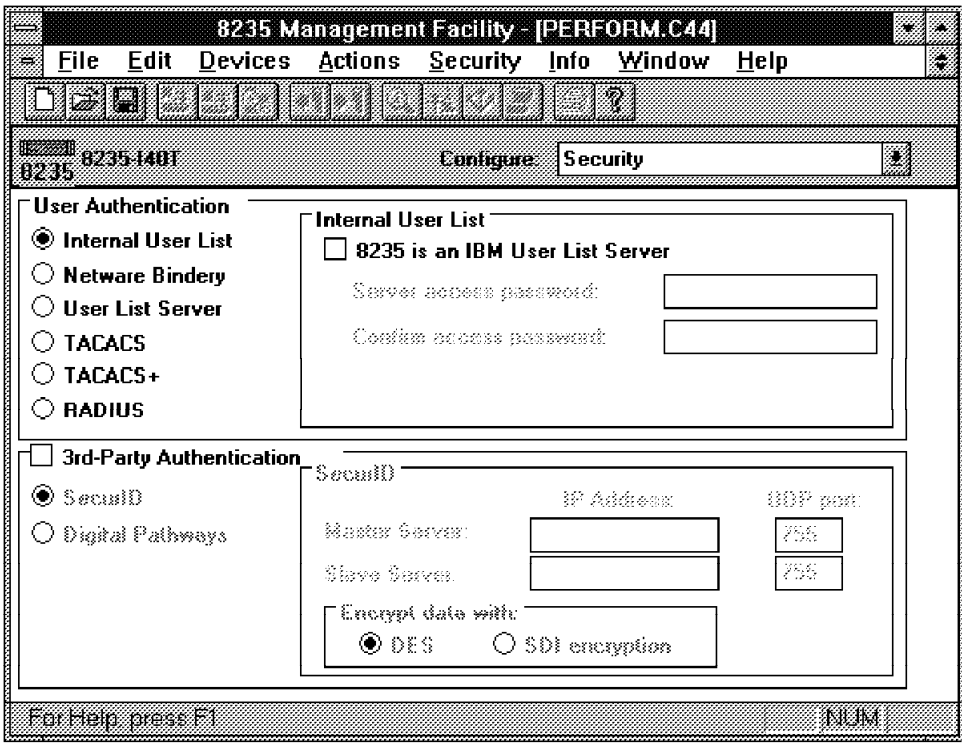
- Select frame type and lock in network number to reduce network traffic.
- Dial-In Network: Virtual IPX # between 8235 and devices.
- Use IPXODI.COM V2.11 instead of IPX.COM, LSL.COM 2.05, IPX compatible transport for WFW 3.11 and VLM 1.21 for 4.5 code.

---

[1] Open the 4.5 Readme file and change .img name

[2] Tip: http://www.networking.ibm.com/nes/nesibase/193.htm

5.4.2.20 Configuring the Third Party Security Page

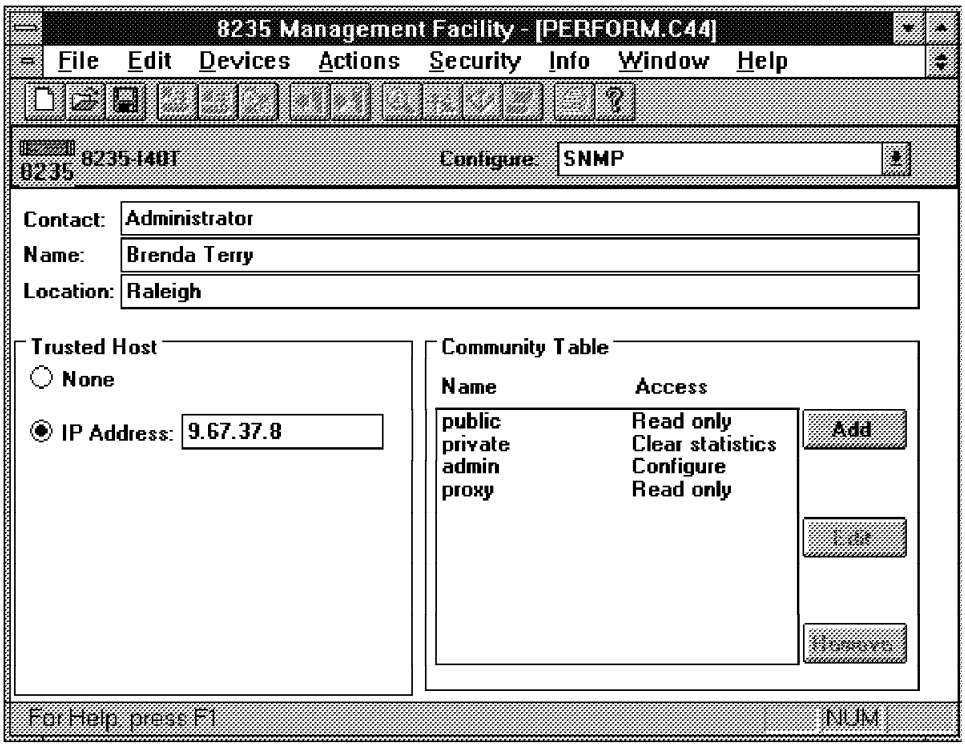


Attention

Do not Enable SecurID Authentication if you are using the external ACS box. If selected, you will be unable to use this function. It is is only to be enabled for the ACE Server.

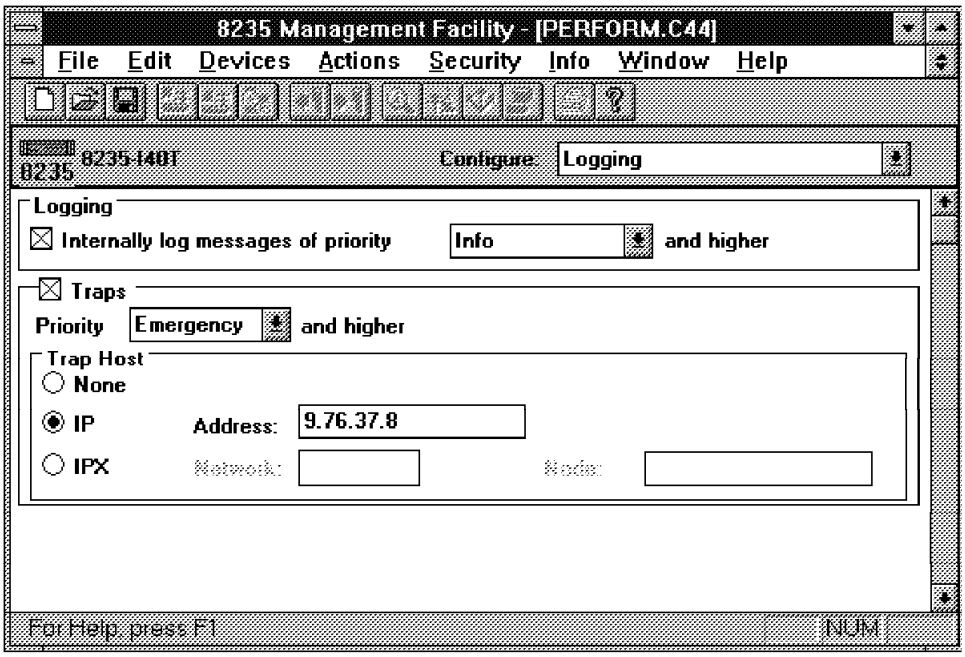
If using the external ACS device, you must speak to the administrator to determine how the ACS is configured for line speed and other functions. Note that these devices can only be used on the processor card UARTs.

5.4.2.21 Configuring SNMP



Note: MIB resides on the Management Facility. Correct steps to load the MIB and steps for BootP are included in the 4.0 Readme file.

5.4.2.22 Configuring Logging options



Tip

- Use Debug selectively; it produces 50% more traffic than Info.

5.4.2.23 Configuring Source Route Bridging Page

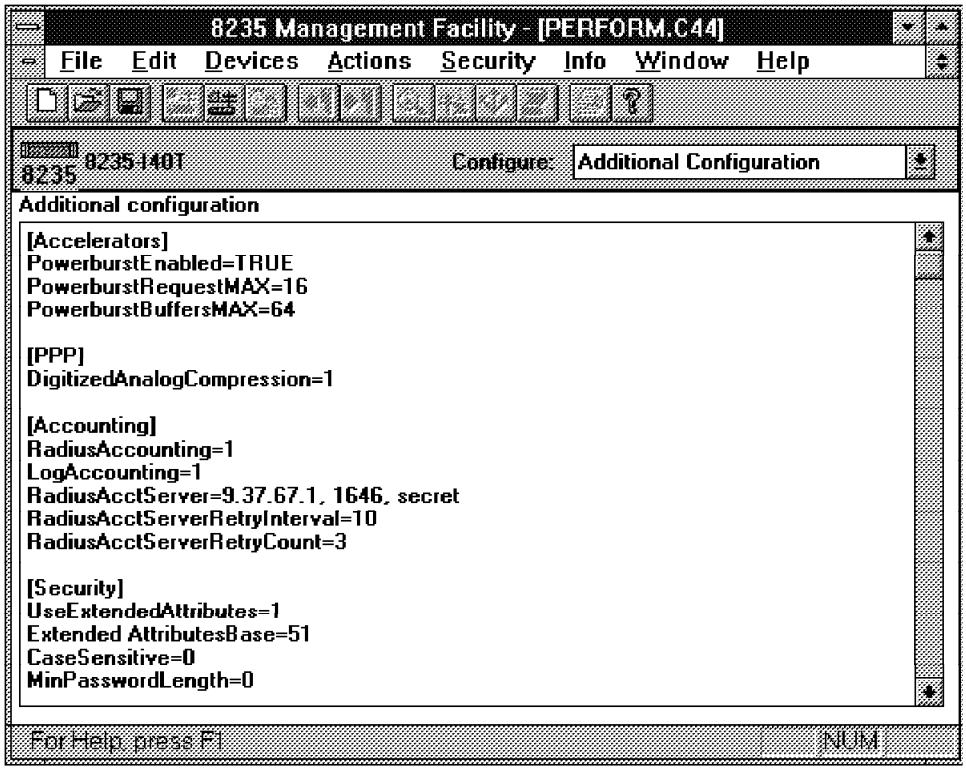
Source Route Bridging is used for the NetBEUI and LLC protocol traffic. The appropriate ring number for external and a virtual ring number for internal must be configured on this page. It is important that no ring numbers be duplicated on the network. This configuration page is not needed for Ethernet 8235 models.

If the clients can't reach the server, this configuration could be the problem:

```
RingA-->8209--RingB--8272 TRN Switch--RingC--8235 <--Client
                        ]
                        V
                  OS/2 LAN Server
```

The 8272 looks at both hubs as being on RingB with R2.33. The solution is to change 8235 to RingB.

5.4.3 Configuring Additional Configuration Page

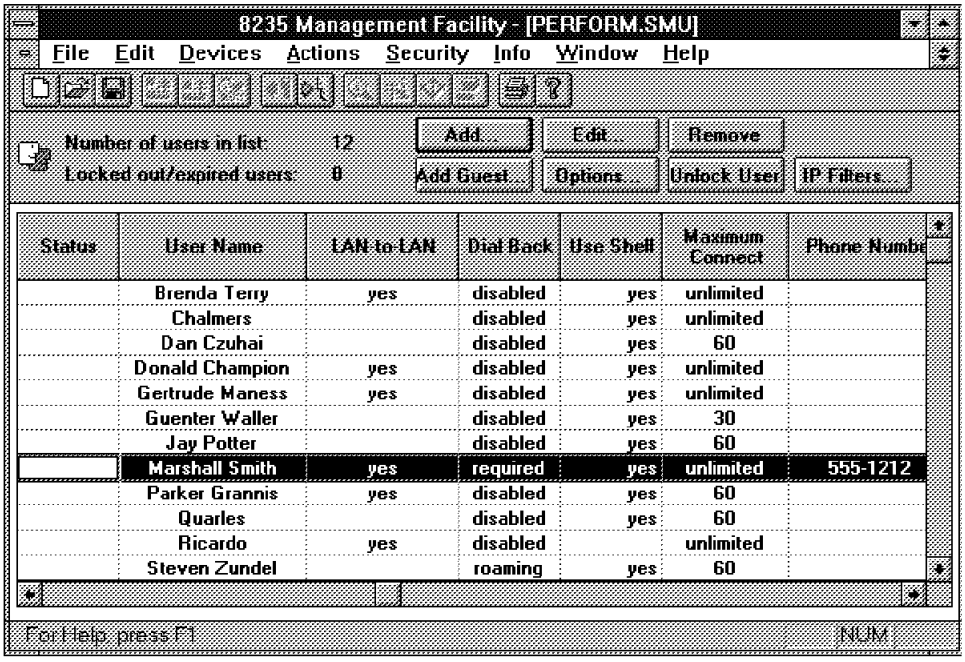


Note:

- These options may also be entered via the 8235 Operating Shell.
- This is also where you enter a Banner message.

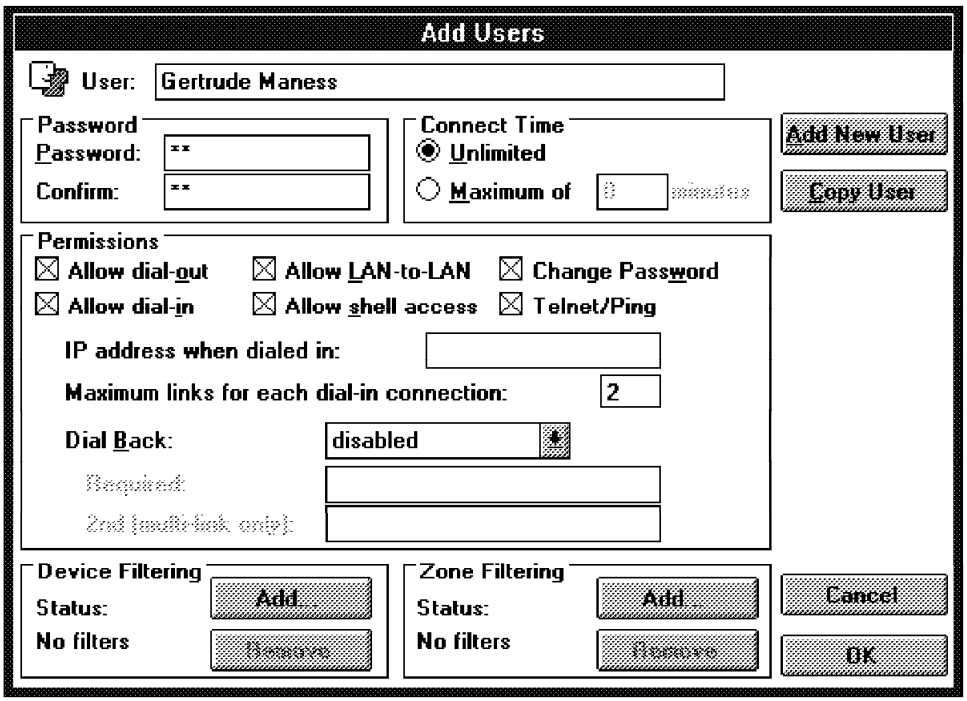
```
Banner="\n***********\n*WELCOME to Education and
       Training     *\n* Authorized Access Only !****\n
```

5.4.3.1 8235 User List

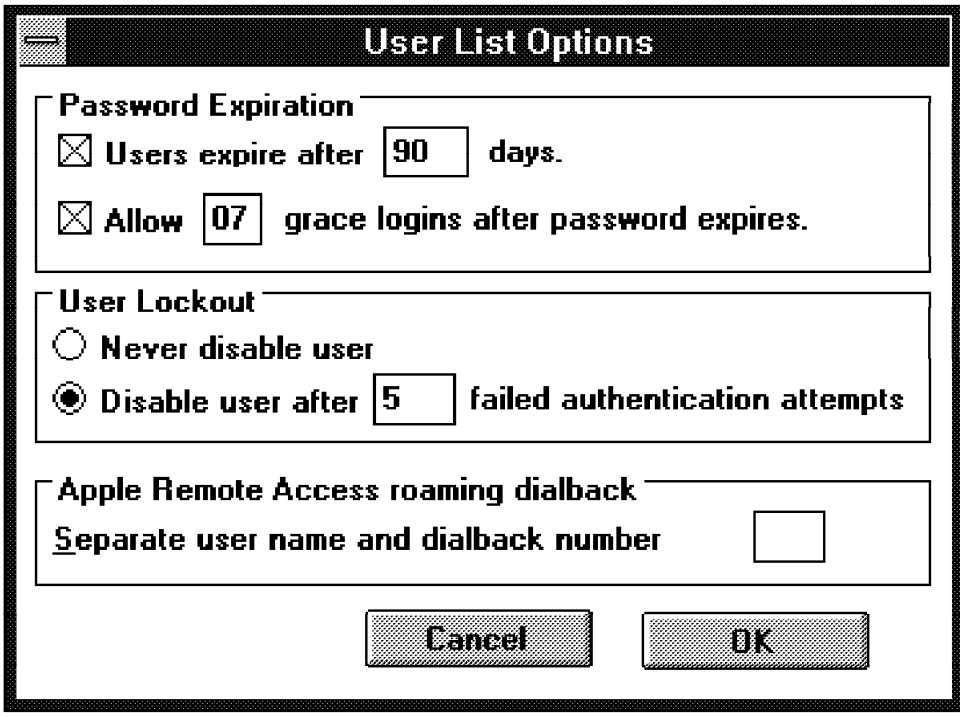


Note: The names in the panel above are those of the 8235 team that has used the 8235 extensively.

5.4.3.2 Add Users



5.4.3.3 User List Options



Note: Password expiration and grace logins are not recommended if users are dialing in without using the DIALs clients. Without the DIALs clients, it is much more difficult to change their password, and they will not see the warning message notifying them to change their password.

5.4.3.4 IP Filtering

To configure IP filtering, a filter must first be added. By default, all users have a Permit-In=Dst: all filter, which prevents any filtering from taking place. To add a filter:

1. Click **Add...** Figure 35 on page 95 appears.
2. Name the IP filter in the Name: box.
3. Configure to either permit or deny in:
   - A single host (access to a specific computer)
   - A mask of hosts (access to a subset of the network)
   - All machines
4. Click **OK**.
5. Select the filter in the right column and the appropriate users in the left column.
6. Click **Attach**.

For example, to configure the user **Marshall Smith** above with access to the entire network *except* for the 10.X.X.X network, the following steps would be taken:

1. Click **Add...**
2. Name this filter *No10Access*.
3. Select the **Deny In** radio button.
4. Select the **Address Mask** radio button.
5. Enter *10.0.0.0* in the Address: field.
6. Enter *255.0.0.0* in the Mask: field.
7. Click **OK**.
8. Select **No10Access** in the right column and **Marshall Smith** in the left column and click **Attach**.

Upon next login, this user is now prevented from accessing the 10.X.X.X subnet.

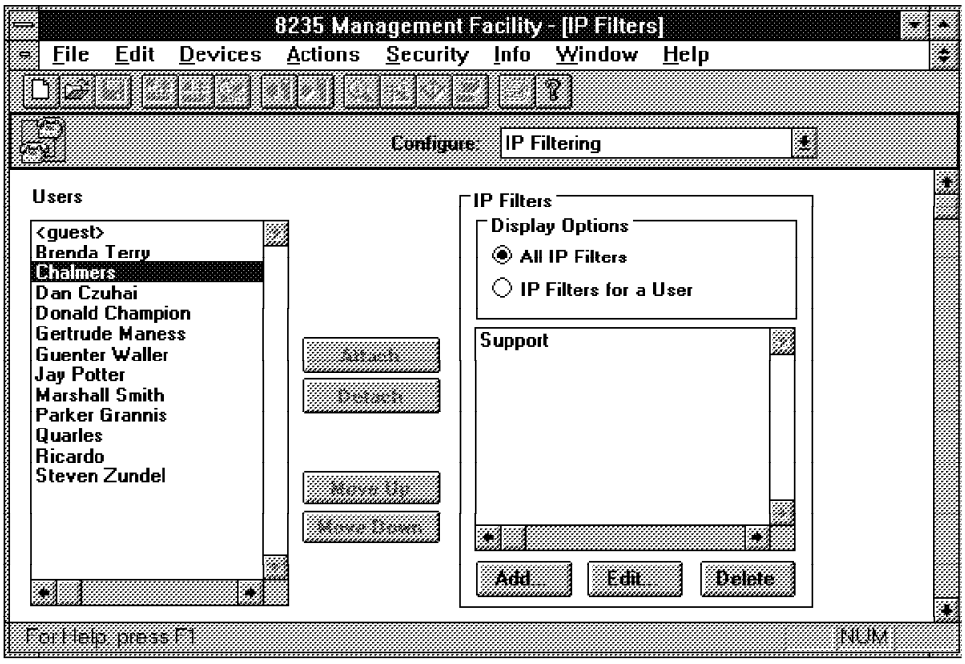


Figure 34. IP Filters Configuration Page

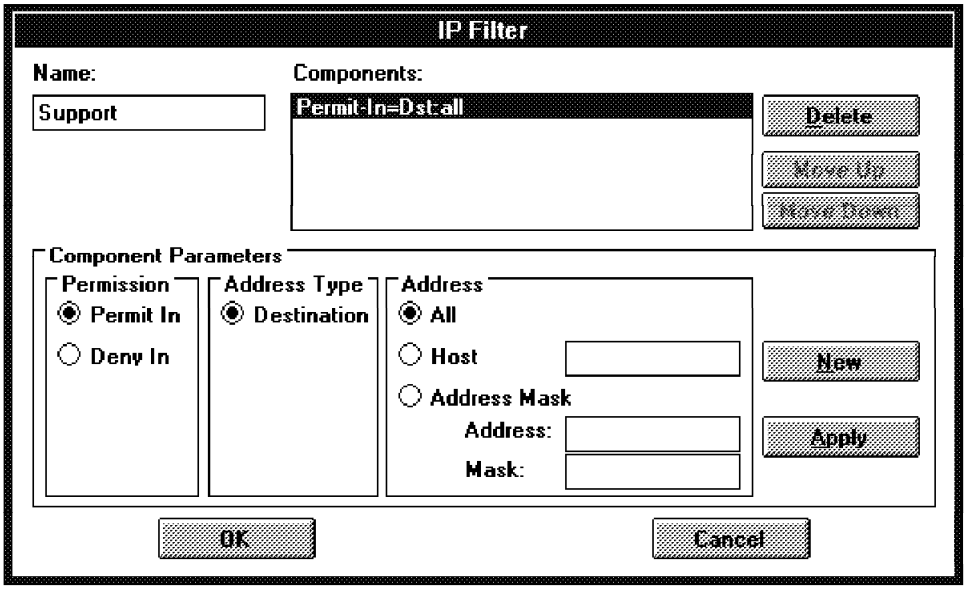


Figure 35. IP Filter Add Page

Note: This is the settings page for filters on a specific user or group.

Tip

To prevent remote users from configuring the devices, the IP filters can be used in conjunction with another setting.

1. Disable IPX dial-in for all incoming phone groups.
2. Create IP filters that Deny In the specific hosts used for the 8235-I40 devices.
3. Bind this IP filter to all users.

Now, even with the Management Facility, the users will be able to access the entire IP and NetBEUI/LLC network, but will not be able to directly reconfigure the devices.

Chapter 6. Description of the Dial-In Function

Dial-in is the core function of the 8235. This is the function for which the product was originally designed, and it is still the main application. It is designed to accommodate LAN application environments, configure them as if they were using a LAN adapter, but replace the driver that normally would interact with the LAN adapter with a driver that uses a modem or an external ISDN terminal adapter (via COM port) or an integrated ISDN card (via the drivers that come with it).

The 8235 is shipped with software packages providing this type of support for four different operating system environments:

- DOS
- Windows 3.X
- Windows 95
- OS/2

The software packages are called DIALs Clients. A DIALs Client basically consists of two parts:

- A device driver to replace or look like the LAN adapter driver
- A dialer to configure, establish, monitor and tear down the dial-in connection

This chapter describes how to install, configure and use the DIALs clients.

Other supported platforms for dial-in include:

- Windows 95 (with or without the IBM Security Pack for Windows 95)
- Windows NT (using RAS)
- UNIX platforms (using SLIP or PPP)
- ASCII terminal emulation packages (using the shell command Telnet)
- Asynchronous terminals (using the shell command Telnet)

These platforms do not provide the same set of functions as the DIALs Clients. This chapter contains some advice on how to use some of those platforms and describes some of the limitations.

6.1 Installation and Customization of DIALs Clients

Installing a DIALs Client is a simple task. On a command line (depending on your environment), invoke the setup utility. All you need to decide is the path where you want the files to be placed. The default directory name is `c:DIALS`. The only thing you may want to change is the drive.

Depending on the applications you want to run over the dial-in connection, you have two options regarding the device driver:

- The NDIS driver (Network Driver Interface Specification)

  This is the preferred interface in many environments, including IBM LAN Support Program, IBM MPTS, and Windows for Workgroups. The NDIS interface was specified by a group of manufacturers and is an industry standard. NDIS drivers are available with most LAN adapters. The DIALs

Client comes with the DIALNDIS driver. See Figure 36 on page 98 for an overview of the supported protocol stacks.

Important

Only the four protocols shown in Figure 36 are supported for dial-in. Each protocol must be enabled on the 8235 *and* on the DIALs client. Enabling it for the client takes place during installation. However, you can change your choice any time later.

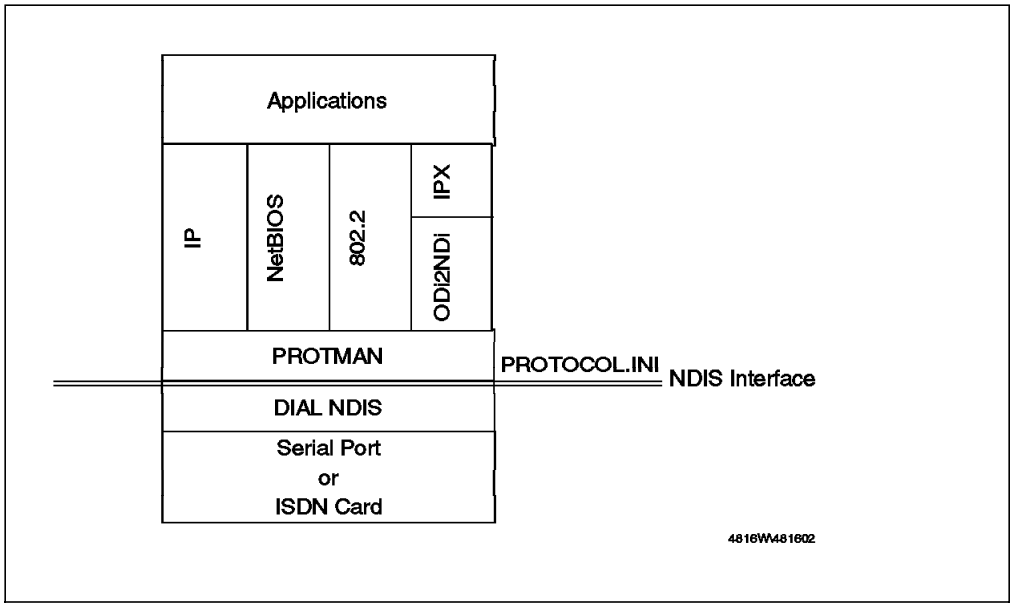


Figure 36. DIALs and the NDIS Interface

- The ODI driver (Open Data-Link Interface)

  This is usually the preferred interface to the LAN adapter in a NetWare environment. The ODI interface was specified by Novell. Many LAN adapters come with ODI drivers, including the DIALs Client. Figure 37 shows how an ODI environment is built. The protocol stacks above the ODI line remain unchanged when moving from a LAN adapter to a dial-in setup.

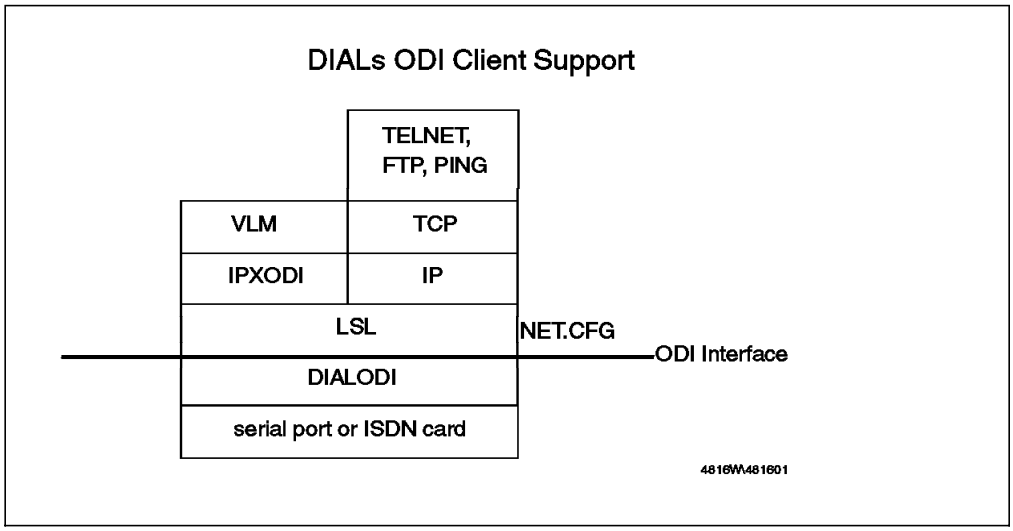


Figure 37. DIALs and the ODI Interface

6.1.1 Installation of the DOS DIALs Client

Use the setup utility and select the installation path (x:path). An initial setup will be determined; you will be asked about the COM port to be used, the modem and the protocols. If you are not sure at this point, reply with your best guess. You can change all this any time later when you have obtained the required information. At the end of the installation process, you will be directed to the user′s guide for further information. However, this guide does not exist anymore for Version 4.5, but has been replaced by the Online User′s Guide of the Windows version. For this reason you may want to install the Windows client on a selected system for reference purposes or to be able to print it from there (even if you will not use the Windows client).

The installation procedure will change the AUTOEXEC.BAT file, and, even if it is the DOS version, it will change the Windows control files SYSTEM.INI and WIN.INI. This allows the DOS drivers to be used in the Windows environment. Backups will be saved with the extension 000. These are the changes we observed:

- AUTOEXEC.BAT:
  - SET DIALS=xpath sets the system variable DIALS. This is used by the DIALs Client during execution to find its control files.
  - Add xpath to the PATH statement.
- SYSTEM.INI:
  - Add the virtual device driver DIAL.386.
- WIN.INI:
  - Link the file extension *.IR to the connectw application, which is the Windows version of the dialer.

Note that 4.0 is the first release to provide separate disks for the DOS version and the Windows version. Also note that Dial-In for DOS and DIALs Client for Windows cannot be active on the same workstation at the same time. If Dial-In for DOS is running when you attempt to run DIALs Client for Windows (or when the DIALs Client for Windows driver is loaded when Windows first starts up), an error message appears and you will not be able to dial in from Windows.

However, you can install both versions on the same system, but be aware that the DIALs Client for DOS and DIALs Client for Windows use the same name for some files (for example, the DIAL.386 file that is configured in the SYSTEM.INI file). Do not install both clients in the same directory.

Important

Some of the advanced functions available with the Windows and OS/2 versions are not supported by the DOS version. These include:

- Complete online manual
- Change of password by the user
- Support for ISDN cards, including MLP and virtual connections

Some of these issues apply to the Windows client in the same fashion.

Prompt for an Adapter Diskette: The DIALs Client comes with NDIS and ODI support; however, you cannot use the installation diskette as a driver diskette, because the files are compressed on this disk and must be expanded to be used. If you provide the DIALs Client diskette when asked for an adapter driver diskette by IBM LAN Support Program (LSP), for example, it will not be recognized.

Install the DIALs Client first, and provide the DIALS directory instead of the diskette as a path for the adapter driver diskette.

Command Line Parameters (DOS only): The command line parameters allow you to invoke most of the features from within a BAT file, so an automated procedure can be built for ease of use. However, if the user ID is password protected, there will be a prompt for the password. This cannot be automated.

Table 21. Command Line Parameters for CONNECT

Parameter(s)	Description
(none)	Load Connect program
/?	List Connect command options
@<filename>	Connect with a connection file
@<filename> /m	Connect with manual dialing
@<filename> /r	Connect with roaming dial-back
/d	Disconnect modem
/a	View asynchronous statistics
/e	View network error statistics
/ipx	View IPX networking statistics
/ip	View IP networking statistics
/netbeui	View NetBEUI statistics

LaunchGuard (DOS only): You can use LaunchGuard, a TSR program that helps you avoid loading programs from remote NetWare file servers. This is a performance issue if the size of these programs is such that loading them over the dial-up link can take several minutes. In such cases we recommend that you keep the executables local.

Note: LaunchGuard works only for the DOS version of the DIALs Client. If you are using Windows, loading the LaunchGuard utility does not help with your dial-in performance.

Also note that LaunchGuard works only to prevent starting executables from Novell NetWare file servers. Other files servers are not affected by using LaunchGuard.

To use LaunchGuard on your workstation:

1. Run GUARD.EXE from the DOS prompt, or from within a batch file, before you establish your dial-in connection.
2. For a list of command-line switches you can use to modify the behavior of LaunchGuard, see Table 22 on page 101.
3. Run the DOS CONNECT.EXE program and establish your remote dial-in connection.

4. Once you have run GUARD.EXE, any attempt to run a program off a remote file server results in a message appearing warning you that you are starting a remote application. The message tells you the name of the program you are about to run, its size, your dial-in speed (in bps), and an estimate of how long it will take to load the program.

   After displaying this information, the following question appears:

   `Do you want to execute this program? Y)es, N)o, D)isable LaunchGuard.`

   Press F1 for help at any time while the LaunchGuard message is displayed.

5. Press the first letter of the desired response.

   `Y` to close the LaunchGuard message and run the program from the remote server.

   `N` to close the LaunchGuard message and cancel loading the program on the remote server.

   `D` to close the LaunchGuard message and run the program from the remote server, disabling LaunchGuard in the process. You can re-enable LaunchGuard at any time by typing `GUARD /E` at any DOS prompt.

You can use any of the following command line switches to modify the behavior of LaunchGuard:

Table 22. LaunchGuard Command Line Switches

Parameter(s)	Description
/D	Disables LaunchGuard until you use the /E switch.
/E	Enables LaunchGuard if the /D switch has been used.
/H or /?	Lists all options available in LaunchGuard.
/M	Lets you specify how long a program should be expected to take to load before LaunchGuard pops up. By default, this is set to 0, so that LaunchGuard pops up for all programs. If you want LaunchGuard to pop-up for programs that take two or more minutes to load, enter `GUARD /M=2` at the DOS prompt. Valid entries are 0 through 9.
/N	Loads LaunchGuard without the online help. If the online help is included, LaunchGuard uses about 3.5 KB of RAM on your workstation; if you use this switch, LaunchGuard uses only 2.1 KB.
/U	Unloads LaunchGuard from your workstation memory as long as no other TSRs have been loaded since you first loaded LaunchGuard. If other TSRs have been loaded since you loaded LaunchGuard, you must unload them before you can unload LaunchGuard.

Memory Shortage for Port Setup or Connect: Because of the number of modems supported by Dial-In, you may run out of memory when opening the Port Setup window or when you click on the Connect button to dial in.

To avoid this problem, make a backup copy of the file MODEMS.INI, then open it in any text editor and remove modem entries you do not need. Be sure to make your changes to MODEMS.INI and not your backup copy.

6.1.2 Installation of the Windows DIALs Client

Select **Run** from the File menu and type a:setup.exe to start the installation.

Install or Remove: The setup utility allows you to either remove an old version or install a new one. However, removing an old version only works for Release 4.0 and above, and it does not remove a DOS 4.0 Version. It requires a DIALS.LOG file to exist. If this is not found, remove will fail.

Note: During the entire installation, there will be a Tips & Information window explaining what is happening. Do not enlarge this window; we could not find a way to make it smaller after this. If it is enlarged, you will not see the progress window anymore.

Before installing the DIALs Client, we recommend that you install the protocols you intend to use. The DIALs Client attempts to detect the installed protocols and recommends a setup based on its findings. For example, if it finds IPX as the only installed protocol, it recommends using the DIALODI driver. However, the installation program cannot detect all protocols. Even if the program states that no installed protocols have been detected, you may still continue the installation of the client, but configuration may have to be done manually.

The installation lets you select the installation path (x:path). It is advisable not to change the directory name from the default of DIALS.

Autodetect Communication Device: After copying the files, the port setup will follow. Try Autodetect to find the right COM port and modem type. In our case it did not work, although a modem supported by the modem list was attached. Not all modems listed in the modem list are supported for autodetect. If it does not work, provide the COM port and modem type yourself. If your modem is not listed, try default settings.

Connection Wizard during Setup: After building the IBM DIALs Program Group, the *Connection Wizard* will be invoked, a tool that helps you build a connection file step by step. However, it only takes care of the basic features; you may want to revisit your connection file settings afterwards. The required settings are user ID, phone number, and protocol selection. If you are not sure at this point, reply with your best guess. You can change all of the above and add more settings any time later when you have obtained the required information. At the end of the installation process, you will be offered the release notes. Select **Yes** and read them carefully. They contain last-minute information that is not available anywhere else.

System Files: The installation procedure will change AUTOEXEC.BAT, SYSTEM.INI and WIN.INI. Backups will be saved with the extension 000. In contrast to the DOS version, these backups are located in their respective directories, not in the DIALS directory. These are the changes we observed:

- AUTOEXEC.BAT:
  - SET DIALS=xpath sets the system variable DIALS. This is used by the DIALs Client during execution to find its control files.
  - Add xpath to the PATH statement.
- SYSTEM.INI:
  - Add the virtual device driver DIAL.386.
  - Powerburst drivers
  - Possible addition of ISDN drivers

- WIN.INI:
  - In the [extensions] section, link the file extension *.IR to the connectw application.
  - In the [programs] section, add connectw.exe.

Note that 4.0 is the first release to provide separate disks for the DOS version and the Windows version. See 6.1.1, “Installation of the DOS DIALs Client” on page 99 for details on this. With the Windows version, there is no dial-in outside of Windows. However, DOS applications can be used under the control of Windows, once the connection is made.

Memory

The DIALs Client for Windows 4.0 has introduced the concept of virtual device drivers (VxD) in order to save conventional memory. You will notice that DIALNDIS.EXE and DIALODI.EXE are substantially smaller (less than 10 KB each compared to nearly 40 KB in 3.5). The use of conventional memory is even less: 3 KB for DIALNDIS and 2 KB for DIALODI. This alone may be a good reason to use the Windows client for DOS applications.

6.1.2.1 Connection Wizard

If you have multiple connection configurations (different protocols to be used, different phone numbers, different modems, etc.) you may want to use several connection files and different icons to invoke these. The connection wizard allows you to create these, the same way as you have seen during the installation. There is only one additional step; this is the selection from a range of different icons and the option to place the icon in a selectable program group.

Figure 38. Connection Wizard

6.1.2.2 Support for Multiple Boot Configuration

In the DOS operating system, there is a feature providing a boot menu with multiple configurations to choose from. This is set up in the CONFIG.SYS and AUTOEXEC.BAT files. These files get conditional sections, and depending on the selection made at boot time, one particular section will be carried out, setting up the chosen environment.

This multiboot setup can be used to maintain different dial-in, local (LAN-attached) and stand-alone environments. This is of particular interest for users who work remotely from home or on the road as well as locally when they come back to their office. They can easily decide at boot time which setup is to be initialized.

Another use for this may be to easily move between different applications requiring different protocol stacks, if there are resource problems (such as memory constraints) that do not allow to load all the drivers simultaneously. If the applications in question do not have to be active at the same time, the solution is to swap environments by shutting down and rebooting a different setup.

The DIALs Client Setup recognizes a multiple boot configuration and modifies only the boot configuration you specify, including modifying all PATH statements, all SET DIALS statements, and all STARTNET.BAT files correctly.

Note: The multiboot feature can be used by the DOS client as well. However, the system files will have to be edited manually; the DOS setup does not recognize multiboot parameters.

6.1.2.3 Multiple Networks in Windows for Workgroups

If you are using the Windows for Workgroups NetBEUI protocol for networking and you use both a dial-in connection and a local network, as you might if you are using a laptop workstation both in the office and on the road, you can use the DIALs Client Network Setup dialog box to switch between the two networks. When you do this, DIALs Client changes the PROTOCOL.INI file in your Windows directory. This file determines how the different network protocols and network adapters you are using have been configured for Windows for Workgroups 3.11. No other files are changed by the Network Setup command.

To change the network driver used in Windows for Workgroups for network access, choose **Network Setup** from the Tools menu.

Note: If you are not running Windows for Workgroups or if the DIALs Client dial-in driver is the only network driver you have set up, this feature is not available, and Network Setup does not appear on the Tools menu. The Network Setup dialog box appears.

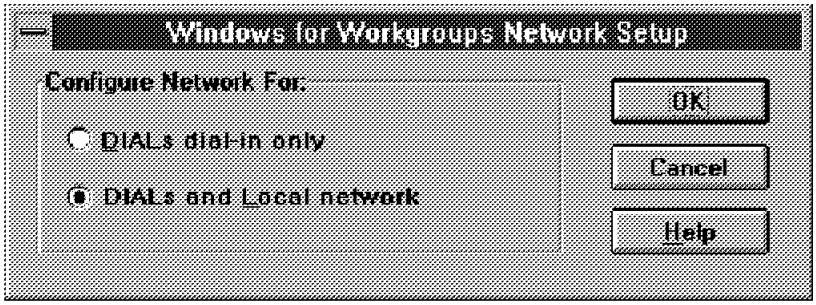


Figure 39. Windows for Workgroup Setup

Make your choice and click on **OK** when you have completed setting up the network. You have to reboot the workstation for the network changes to take effect.

6.1.2.4 Express Setup for Mass Deployment

Release 4.0 includes a new feature called Express Setup for network administrators. Express Setup lets the network administrator define a set of installation parameters that the DIALs Client Setup program uses by default for each user dialing into a site. For example, if all of the users of your site need to use the same dial-in telephone number, use the same modem for dialing in, and use the same networking protocols while they are dialed in, you can define all of those options to be set automatically when DIALs Client Setup installs the dial-in software on each user′s workstation.

Note: The Express Setup feature works best if all of your users have the same multiple boot configurations so you can have DIALs Client Setup modify the same configuration on each user′s workstation. For example, if your users all have a local and a remote boot configuration, you could tell DIALs Client Setup to modify the remote configuration automatically to load the DIALs Client drivers.

Some of the benefits of using Express Setup with DIALs Client include:

- Less user confusion. Users who do not know about networking protocols might not know whether to use IPX or IP, for example. With Express Setup, you can make that decision for your users and avoid confusion.
- Consistency of setup. When you use Express Setup, you can ensure that each user′s workstation is configured the same way for DIALs Client dial-in. If users have problems dialing in, you can support them more easily knowing how DIALs Client was originally set up.
- Avoid workload. The system administrator can avoid having to set up all of the user′s systems and, instead, distribute customized installation disks; for the above reasons, even untrained users will find it easy to do the installation. A set of simple instructions should cover most cases.

How Express Setup Works: When the Setup program runs, it looks on the root level of Diskette 1 for a file called EXPRESS.INI. If this file exists, the Setup program performs an Express Install, using the default values in EXPRESS.INI when they exist, and prompting the user for input when no default values have been provided.

To use Express Setup, you need to create a custom EXPRESS.INI file that provides the Setup program with default setup values specific to your users. Using any text editor, you can either create an EXPRESS.INI file from scratch, or you can modify the SAMPLE.INI file provided on Diskette 1.

The SAMPLE.INI file contains a complete set of Express Setup options, along with their explanations. To use this file, copy it to EXPRESS.INI, then open it with a text editor to modify the values of any lines you want to use.

Creating an EXPRESS.INI File: Follow the steps here to use the Express Setup feature of DIALs Client Setup.

1. Make a backup copy of the DIALs Client Setup diskettes.

   You can either make duplicate copies of Diskette 1 and Diskette 2, or you can create a network installation drive by copying the contents of Diskette 1 into its own directory and the contents of Diskette 2 into its own directory on a hard disk or shared network drive.

Note that the directories for Diskette 1 and Diskette 2 should be in the same directory; for example, you might have a directory called DIALS, and within that directory you might have DISK1 and DISK2.

2. Using any text editor, open the file on Diskette 1 called SAMPLE.INI. This file contains a commented list of all Express Setup options available.
3. Save this file in the same directory under a new name: EXPRESS.INI. The Express Setup feature looks only for the file called EXPRESS.INI to determine which options to provide and which to ask the user to enter.
4. Make changes to the values of any line you want Express Setup to use. Do not remove the semicolon from any of the lines of explanation present in EXPRESS.INI.
5. Save your changes and copy the file onto Disk 1 of the DIALs Client Setup diskettes (or into the Disk1 installation directory you have created for your users).

Notes

1. EXPRESS.INI is used for installation only. Removal must be accomplished manually. As a result, the Type of Setup dialog is considered an Install value, but it is not displayed.
2. Not all dialog boxes have corresponding parameters in this file. The existence of this file, when called EXPRESS.INI, indicates to SETUP that the default (OK or Continue) prompt should be accepted.
3. In order for installation via EXPRESS.INI to work smoothly, it is imperative that there be no deviations from the expected operation as set up by the administrator. If this file expects there to be certain Multiboot section names or modem names, for example, these should really be there. In most cases, if they are not, Express installation will either pause and await user intervention or fail.

Express Installation Options: This section summarizes the options you can specify in the EXPRESS.INI file for DIALs Client Setup to automatically set for the users. Much of this information is described briefly in the example Express Installation file included on Diskette 1 of the DIALs Client Setup diskettes (in the file SAMPLE.INI).

The basic structure of EXPRESS.INI files is shown here:

```
[SectionName]
ParameterName=value[,default]
```

If the entry is followed by ,default, the user will be asked to specify the value during the Setup process, but the value you enter here will be offered as a default entry.

For example, to specify the location in which DIALs Client Setup will automatically install DIALs Client without prompting the user, you might add this entry to your EXPRESS.INI file:

```
[Install]
Location=C:\DIALS
```

The following entry will prompt the user to specify a location in which to install DIALs Client but will suggest the path specified here:

```
[Install]
Location=C:\DIALS,default
```

Note: If any option described here is omitted from the EXPRESS.INI file, the user will be asked to supply that information during installation.

The following table only provides an overview of the parameters. For coding details refer to the SAMPLE.INI file and the README.TXT description.

Table 23. Express Installation Options

Option	Purpose
Location=	Indicates the hard drive and path in which to install the DIALs Client.
Modem=	Indicates the communication device that will be used for dial-in calls, and adds that device's information to the Modem Setup dialog box and as the default for any new connection files (.IR files).
Port=	Indicates the port to which the communication device specified in Modem is connected. Note that if the communications device specified by Modem= is a WinISDN-compatible ISDN card, the port you specify will be ignored; you must enter a value here, however, to prevent DIALs Client Setup from asking the user for a port number.
Multiboot=	If the user's computer is configured with multiple boot configurations (as specified in CONFIG.SYS and AUTOEXEC.BAT), this option specifies which configuration should load the DIALs Client software.
Boot=	Specifies whether the workstation is used for remote networking only, or for remote and local networking.
Description=	Indicates the value used by the Connection File Wizard to place in the Description field of the automatically generated connection file. This value is also used for the connection file's icon in the Program Manager.
DialInName=	Indicates the user's dial-in name.
PhoneNumber=	Indicates the telephone number of the 8235 the user will be calling.
Protocols=	Indicates the networking protocols that will be selected in the Connection File Options dialog boxes by default for use over the dial-in connections.
Autoconnect=	Determines whether to begin dialing in automatically whenever the connection file is opened in DIALS Client.
FileName=	The path and name in which to save the automatically created connection file. Replace the extension SR given in SAMPLE.INI by IR. This is an error in the sample file.
Reboot=	Specifies whether the user's workstation should restart automatically when express installation is complete.
ReadMe=	Indicates whether the user views the ReadMe file (README.TXT) after setup is complete.

6.1.3 Installation of the OS/2 DIALs Client

You can install DIALs/2 Version 4.5 on top of any previous DIALs/2 installation, including Version 4.5 itself. Before doing so, however, you should close all dial-in connections, and also close all DIALs/2 programs as well as any editor sessions that have DIALs/2 text files. Otherwise, the installation will not be able to complete.

If you are installing DIALs/2 Version 4.5 on top of an existing DIALs/2 installation, and if the DIALs/2 WaveRunner ISDN support is installed and active, then you must also shut down the DIALs/2 WaveRunner Helper. Follow the release notes in the README.TXT file on the installation diskette.

To install, enter `a:setup2` on an OS/2 command line. After copying the files you will be prompted for the port setup. Provide COM port and modem settings; you can change these any time later if you do not have the information at this point. Autodetect features have been added in Version 4.5.

This completes the first part of your installation. In case of an existing LAN environment, DIALs/2 setup will detect the LAN environment and attempt to add its driver information to it. For example, it will attempt to copy the DIALs/2 NDIS driver files (DIALNDIS.OS2 and DIALNDIS.NIF) to the MPTS/LAPS adapter driver directory (usually C:\IBMCOM\MACS), if that exists. However, you will not notice this during the installation.

For the second part, the configuration of your protocols, there are different possible ways, depending on your existing and planned environment:

1. You already have a LAN adapter installed and configured. You want to use it alternating with the dial-in connection.
   - After completion of the file copy you will receive a message that you should complete the installation by clicking on **Shuttle to REMOTE**. Doing so will change your system configuration in a way that you will be able to use dial-in connections after the next reboot, but you will no longer be able to use the LAN adapter. 6.1.3.2, “The Shuttle Concept” on page 111 provides more details on the Shuttle concept.
   - At any time you can select **Shuttle to LOCAL** to re-enable your original LAN adapter configuration. This will, in turn, disable your dial-in capabilities.
2. You already have a LAN adapter installed and configured. You want to use it concurrently with the dial-in connection.

   Note: This is only possible if the LAN-attached network and dial-in network have no path that connects them. Otherwise, you will lose your connectivity.

   - In order to preserve your LAN setup, do *not* use the Shuttle function. Instead, manually add a second adapter (the DIALs adapter) to the environment. Bind the required protocols to this adapter using LAPS (see Figure 40 on page 109). Select **Configure** and Figure 41 on page 110 appears. This is done after completion to install DIALs as a second adapter. In order to function properly over a dial-in connection, which is slower than a LAN connection, some parameter values need to be changed in the protocol drivers. These changes would be carried out by Shuttle automatically. Since you cannot use Shuttle in this case, you will have to apply the changes manually.

3. You do not have a LAN adapter. If you have not already installed MPTS/LAPS at some previous point, do so now.

   - Shuttle will not be possible. You will have to use LAPS to select the DIALs adapter and bind the required protocols to it. The parameter changes for the protocol drivers will also have to be applied manually.

     Note: In order to avoid manual editing of parameters for the protocol drivers (NetBIOS, 802.2) you may install a LAN adapter driver first, bind the required protocols to it, then install DIALs/2 and select **Shuttle to REMOTE**. Since you do not need the LAN adapter, you will never Shuttle back. However, this procedure has saved you the effort required to edit the parameters.

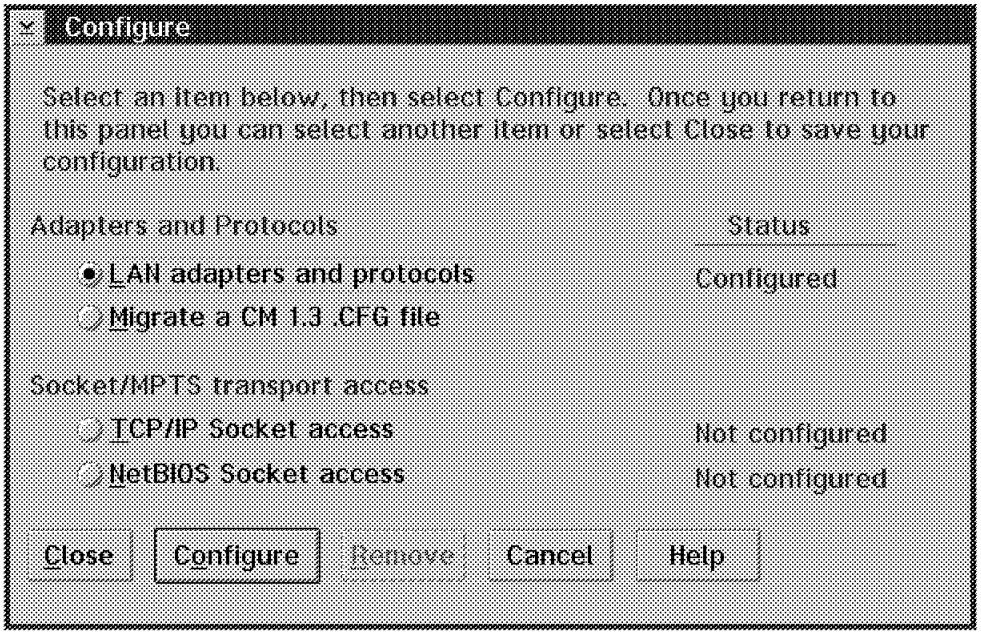


Figure 40. MPTS Invoking LAPS Configuration

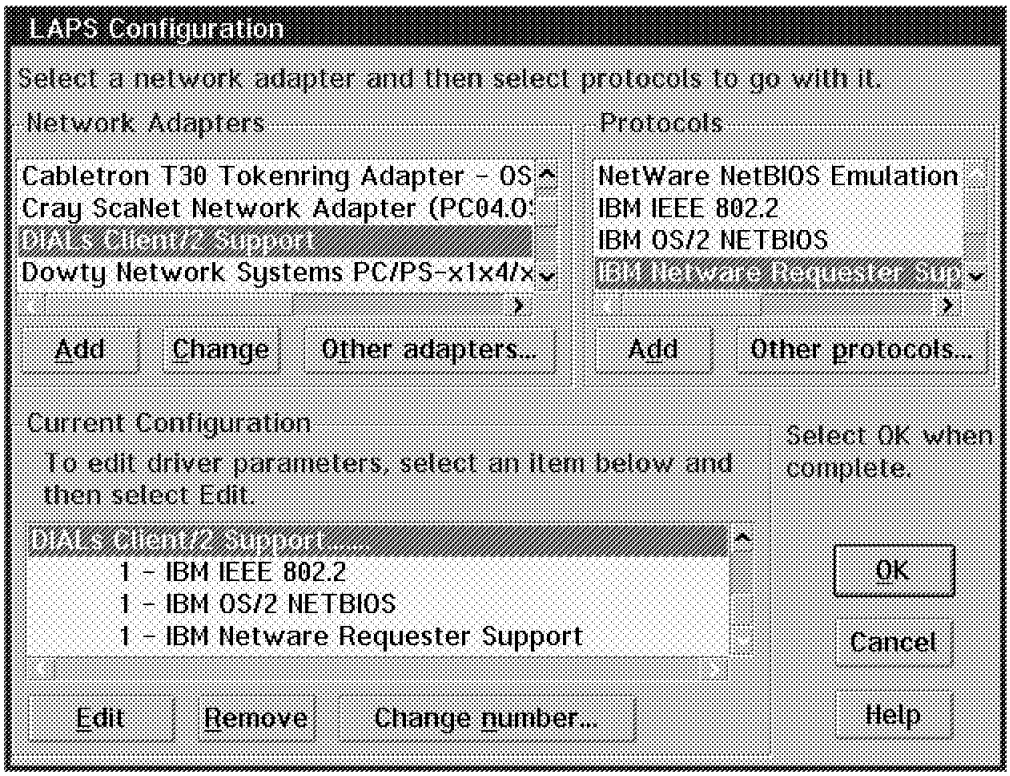


Figure 41. LAPS Configuration of DIALs As a Second Adapter (Adapter 1)

Manual Device Driver Installation: If the automatic copy of the DIALs drivers into the MPTS/LAPS directory (normally c:IBMCOMMACS) fails, you have to do it manually.

1. Invoke LAPS. If you have MPTS, invoke MPTS and enter LAPS from there. You will see the dialog box shown in Figure 42.

Figure 42. LAPS/MPTS - Manual Install of a Device Driver

2. Click on **Install**. An entry field for the location of the adapter file appears.
3. Change the path from A:\ to C:\DIALS (or the current installation directory).
4. Click on **OK** or press Enter. The Installation Complete message box appears.
5. Click on **Exit**. The DIALs/2 NDIS driver files are now installed. They still need to be configured.

6.1.3.1 ODI versus NDIS

You must configure either the DIALs Client/2 NDIS device driver or the DIALs Client/2 ODI device driver; they cannot operate concurrently. The following list will help you determine which driver you should configure:

- If you plan to use only NDIS applications with DIALs Client/2, you must configure the DIALs Client/2 NDIS device driver.
- If you plan to use only ODI applications with DIALs Client/2, you must configure the DIALs Client/2 ODI device driver.
- If you plan to use both NDIS and ODI applications with DIALs Client/2, you must configure the DIALs Client/2 NDIS device driver. (The NDIS device driver can be configured to support ODI applications. This is done by the ODI2NDI additional driver.)

If you are not sure what your applications are using, consider the following list of common applications:

- NDIS applications
  - IBM LAN Services
  - Communication Manager/2
  - Personal Communications
  - PC Support/2
  - TCP/IP for OS/2
- ODI applications
  - Novell NetWare
  - LAN Workplace

If your workstation is already configured for direct LAN attachment with NDIS device drivers, you can continue with the SHUTTLE/2 Program, as discussed in 6.1.3.2, “The Shuttle Concept.” Otherwise, you have to configure either the NDIS Device Driver (see Figure 36 on page 98) or the ODI Device Driver (see Figure 37 on page 98).

6.1.3.2 The Shuttle Concept

If you use the same workstation at work and on the road, it is necessary that you have two versions of your configuration files: one version for directly connecting to the LAN in the office, and one version for your remote connection from the road.

The configuration files that you need to save depend on the applications that you want to run on your workstation. For example, if you want to run CM/2 and LAN Requester, you need to save a copy of your CONFIG.SYS, STARTUP.CMD, and PROTOCOL.INI files for each environment. Other configurations might require a NET.CFG file.

One version would load the LAN adapter driver and associated protocol drivers, and the other version would load the DIALs Client/2 driver and associated protocol drivers.

To set up your workstation to use the SHUTTLE/2 program, you must be running a local configuration (in other words, directly attached to a LAN). The configuration must also use NDIS drivers, as ODI-only configurations are not supported at this time. Click on **Shuttle to Remote** to swap your startup files

(CONFIG.SYS, PROTOCOL.INI, and NET.CFG), if applicable, that you run for your local attachment with the startup files necessary to run remotely.

After you have run Shuttle to Remote, you need to shut down and restart your workstation. Your workstation is now configured to run remotely.

Note: The startup files are backed up to the Shuttle/2 directory and the working copies of the startup files are located in their respective directories with file extensions of LAN for local attachment and DIA for remote access.

Before you shut down your machine each day, think about the next place you plan to use it. If you plan to work in the office, for example, click on the **Shuttle to LAN** icon. This will configure your workstation for a local connection the next time you start up your workstation. Doing this each time before you shut down will reduce the amount of time you spend configuring your workstation.

6.1.3.3 Configuring DIALNDIS

LAN Adapter and Protocol Support (LAPS) is a part of NTS/2. It is shipped with most OS/2 LAN software (for example, Communications Manager, LAN Services, and TCP/IP). Using LAPS with OS/2 saves you time and effort. LAPS installs and loads network adapter and protocol device drivers for you. It supports both IBM and original equipment manufacturer (OEM) network adapter and protocol drivers that are in compliance with NDIS standards. LAPS supplies some network adapter and protocol drivers and supports the installation and configuration of other IBM and OEM network adapter and protocol drivers.

Multiprotocol Transport Services (MPTS) is the successor to NTS/2. Installation and configuration of adapter drivers is similar to LAPS; the configuration program supports configuration of socket access to networks in addition to the adapter/protocol driver configuration, which by itself is virtually identical to LAPS. This section describes how to configure the DIALs Client/2 NDIS (adapter) device driver and associated NDIS protocol drivers using MPTS or LAPS.

1. If you are using MPTS, proceed with step 2. If you are using LAPS, go to step 7.
2. Type MPTS at an OS/2 command prompt and then press Enter. If MPTS is not in your path statement, type C:\IBMCOM\MPTS at the command prompt.
3. Click on **OK** on the logo panel.
4. Select **Configure** from the MPTS main window.
5. Select the item **LAN adapters and protocols**.
6. Click on **Configure**. The LAPS Configuration window appears. Go to step 11.
7. Type LAPS at an OS/2 command prompt and then press Enter. If LAPS is not in your path statement, type C:\IBMCOM\LAPS at the command prompt.
8. Select **Configure** from the LAPS main window.
9. Select **Configure LAN Transports** as the configuration option.
10. Click on **Continue**. The Configure Workstation window appears.
11. See Figure 43 on page 114. From the Network Adapters list, select **DIALs Client/2 Support**.
12. Click on **Add** unless this selection is already in the Current Configuration list.
13. In the Protocols list, select the appropriate protocols for your configuration. Double-click on the name or click once on the name and click on **Add**.

Note: For ODI application support, you must add the protocol named IBM NetWare Requester Support. This will install the above-mentioned ODI2NDI driver.

14. Depending on which protocols you are using, you now can configure the specifics for 802.2, NetBIOS, and ODI. You can also configure a locally administered address (LAA) for the DIALs Client. This is described in 6.1.3.4, “Configuring Protocol Drivers for DIALs (LAPS/MPTS).”
15. If you are using MPTS, proceed with step 16. If you are using LAPS, go to step 21.
16. Select **OK**. The Configure window appears.
17. Select **Close**. The MPTS main window appears.
18. Select **Exit**. The CONFIG.SYS Updates window appears.
19. Select **Exit**.
20. Click on **OK**. The message Exiting MPTS appears. Go to step 24.
21. Select **OK**. The CONFIG.SYS Updates window appears.
22. Select **Continue**.
23. Click on **OK**. The message Exiting LAPS appears.
24. Click on **Exit**.
25. Shut down OS/2 and restart your PC.

6.1.3.4 Configuring Protocol Drivers for DIALs (LAPS/MPTS)

While in the LAPS configuration window, you can configure the drivers that you have added to the DIALs device driver by double-clicking on them or by selecting **Edit** while they are selected. There are a number of recommended changes, mostly due to the lower speed of a dial-in connection as opposed to a LAN connection.

Changes for 802.2: To change the timeout values in 802.2 to reflect the slower communications speed of a dial-in asynchronous line, do the following:

1. Edit IBM IEEE 802.2.
2. Page down to edit Group 1 Response Timer - T1 and Group 2 Response Timer - T1. They have default values of:

   ```
   Group 1 Response Timer - T1     15
   Group 2 Response Timer - T1     25
   ```

   Increase these values to:

   ```
   Group 1 Response Timer - T1     200
   Group 2 Response Timer - T1     250
   ```

3. Select **OK** to save the configuration changes.

Changes for NetBIOS: To change the timeout values in NetBIOS to reflect the slower communications speed of a dial-in asynchronous line, do the following:

1. Edit IBM OS/2 NetBIOS.
2. Page down to edit Inactivity Timer - TI, Response Timer - T1, and Acknowledgment Timer - T2. They have default values of:

```
Inactivity Timer - TI          30000
Response Timer - T1              500
Acknowledgment Timer - T2        200
```

Increase these values to:

```
Inactivity Timer - TI          60000
Response Timer - T1            10000
Acknowledgment Timer - T2       2000
```

3. Change the Adaptive Windowing Interval value from 1000 to 0.

Changes for IBM NetWare Requester Support (ODI2NDI): By default, the DIALs Client/2 NDIS device driver emulates an Ethernet LAN driver. IBM NetWare Requester Support must be configured to use the Ethernet frame types supported by the DIALs Client/2 NDIS device driver.

1. Edit IBM NetWare Requester Support.
2. Edit the frame header support parameters so that ETHERNET_802.3 frame header support and ETHERNET_II frame header support are set to YES, and all others are set to NO.

Changes for DIALs Client/2 Support (DIALNDIS): There are two parameters you can change:

- The Locally Administered MAC Address (LAA)

  This is used in many networks instead of the burnt-in MAC address (UAA - Universally Administered Address). Using LAA allows easier replacement of network adapters without having to reconfigure gateways. Obtain a valid LAA from your network administrator. Choosing an invalid LAA or one that is being used by another PC causes failures on the network.

- The token-ring frame size

  Enabling this feature allows applications to use a maximum frame size of 4096 when dialed into a token-ring attached 8235. Otherwise, the DIALs driver will use Ethernet-size (1514 byte maximum). This feature will not work with the token-ring I40 model.

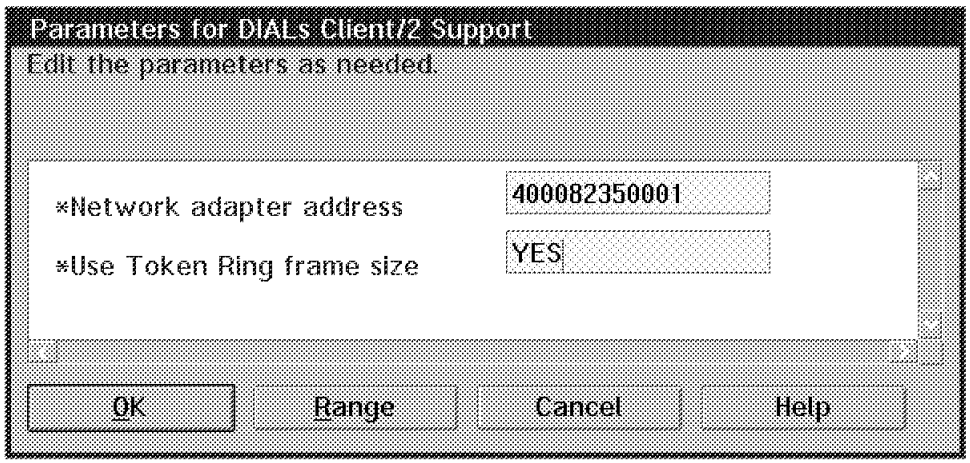


Figure 43. LAPS/MPTS - DIALNDIS Parameters

1. Edit DIALs Client/2 Support.
2. Enter your LAA in the Network adapter address field.

3. Enter YES in the Use Token Ring frame size field.

6.1.3.5 Configuring DIALODI

DIALODI.OS2 is a device driver that provides an ODI link driver interface for ODI protocol drivers. It is particularly useful for configurations in which only ODI network applications (such as the OS/2 NetWare Requester) are being used.

To set up DIALODI to work with OS/2 NetWare Requester if you have not yet installed the OS/2 NetWare Requester:

1. Begin installation of the OS/2 NetWare Requester.
2. When the installation program asks which installation option you would like, specify the installation option that updates CONFIG.SYS in addition to copying the files.
3. When the installation program asks you for the name of an ODI LAN driver, type in the name DIALODI.OS2.
4. When the program asks you which driver files to copy, specify that only the default driver DIALODI.OS2 should be copied. You will then be prompted to insert a driver diskette. Insert the DIALs Client/2 diskette and select **OK**.
5. Complete the remainder of the installation.

   Create a NET.CFG file in the NetWare Requester directory, which contains the following statement:

   ```
   LINK DRIVER DIALODI
   ```

To set up DIALODI to work with OS/2 NetWare Requester if you have already installed OS/2 NetWare Requester:

1. If you have a configuration that is using NDIS device drivers, you should back up your CONFIG.SYS and PROTOCOL.INI files, and then use LAPS to remove all adapter and protocol drivers from those files. (With an ODI-only configuration, you will not be able to run any NDIS applications.)
2. Edit CONFIG.SYS.
   a. In the NetWare Requester section, immediately after the statement DEVICE=C:NETWARELSL.SYS, insert the statement DEVICE=C:DIALSDIALODI.OS2.
   b. Remove the following two statements:

      ```
      DEVICE=C:IBMCOMPROTMAN.OS2
      RUN=C:\IBMCOM\NETBIND.EXE
      ```

3. Edit your NET.CFG file (or create one in the NetWare Requester directory if it doesn't exist) so that it contains the following statement:

   ```
   LINK DRIVER DIALODI
   ```

   If NET.CFG contains the statement LINK DRIVER ODI2NDI, comment it out by inserting a semicolon at the beginning of the statement line; if you later decide to run NDIS and ODI concurrently, you can then comment the DIALODI statement and uncomment the ODI2NDI statement.

6.1.3.6 Command Line Version of CONNECT

CONNECTC is the command line version of Connect/2. It provides a command line interface for connection and disconnection. The most powerful capability this gives you is the ability to connect and disconnect from within OS/2 batch files (*.CMD) or programs (*.EXE) created for automation of tasks that require dial-in to a LAN, such as uploading or downloading a set of files to or from a file server on the LAN.

Note: CONNECTC supports virtual connections, ISDN digital connections, channel aggregation (Multilink Protocol), and PPP data compression. It does not support third-party security, changing your password, connection time limit warning, server-generated alert messages, or the display of statistics.

To connect, type `CONNECTC @<filename>` where `<filename>` is the name of a connection file. (If you omit the standard `IR` extension, it is assumed to be part of the filename.)

You must use the Connect/2 desktop application (CONNECT2.EXE) to create connection files. If the user name specified in the connection file has a password associated with it on the 8235 server to which you are dialing in, or if the user name is not known by the server, CONNECTC will prompt you for the correct user name and password (as CONNECT2 does). (This means that for fully automated dial-in, you can only use a user name that has no password, unless you have version 4.5, which supports a password to be inserted on the command line.)

To disconnect, type `CONNECTC /d`.

6.1.3.7 Concurrent Connections

The DIALs Client/2 NDIS device driver (DIALNDIS.EXE) can be configured to run concurrently with a LAN adapter provided that the adapter is not attached to the same LAN to which the 8235 you are dialing into is attached. The two LANs should not be directly connected; that is, there should not be a path (made up of bridges, routers, or gateways) between the two LANs. Furthermore, you should not configure any network application capable of forwarding traffic among multiple LANs (such as IBM TCP/IP for OS/2) to forward traffic between the LAN attached through the 8235 and the directly attached LAN. For example, you cannot configure IBM TCP/IP to route IP traffic between the two LANs.

6.2 Other Clients

For all other supported platforms there is no full support of all functions that a DIALs Client provides. Usually there is a component in the basic operating system that is capable of dialing into an 8235 and supporting one or several protocols. The preferred method for this is the Point-to-Point Protocol (PPP). Advanced features of DIALs clients (such as password change, banner message display, and call-back) are not supported in such an environment.

6.2.1 Windows 95

The only other operating system with a specific 8235 dial-in support is currently Windows 95. With 8235 Release 4.0 IBM has introduced the 8235 Security Pack for Windows 95, an extension of the built-in Dial-Up Networking support. Without this extension, the Dial-Up Networking function only has the basic dial-in capability.

6.2.1.1 Basic Windows 95

Dial-Up Networking can be found in the My Computer folder on the Windows 95 desktop. To configure a new dial-up connection, click on **Make New Connection** and follow the required steps. You have to provide the following:

- A name for the connection
- A port and modem setup
- A phone number to be dialed, including your country

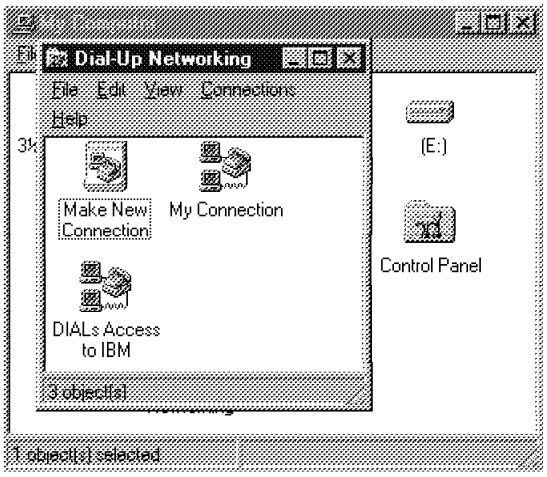


Figure 44. Windows 95 - Dial-Up Networking

Once you have completed this, a new icon will be created as shown in Figure 44. Clicking on it with the right mouse button will bring up a menu; from this menu select **Properties**. This will bring up a configuration dialog box that allows you to change the setup parameters that you provided during creation. Select **Server Type** and you get another configuration page that has three areas:

- Type of Dial-Up Server (drop-down menu) with three options:
  - NRN:NetWare Connect
  - PPP:Windows 95, Windows NT 3.5, Internet (this is apparently the default, and this is what you must select for the 8235)
  - Windows for Workgroups and Windows NT 3.1
- Advanced Options with three check boxes:
  - Log on to network
  - Enable software compression
  - Require encrypted password
- Allowed network protocols with three check boxes:
  - NetBEUI
  - IPX/SPX compatible
  - TCP/IP

  Next to TCP/IP you will find the button **TCP/IP Settings...**. If you click on it, you get another dialog box. This box allows you to set an IP address and name server addresses or decide to have them assigned dynamically by the dial-in server.

Before you try to make your first connection, make sure that the protocols you intend to use are properly bound to your Dial-Up adapter and the applications are bound to the protocols. In order to do this, select **Control Panel** in the My Computer folder and click on **Network**. You will get a window similar to the one shown in Figure 45, which will allow you to check all bindings for the Dial-Up adapter.

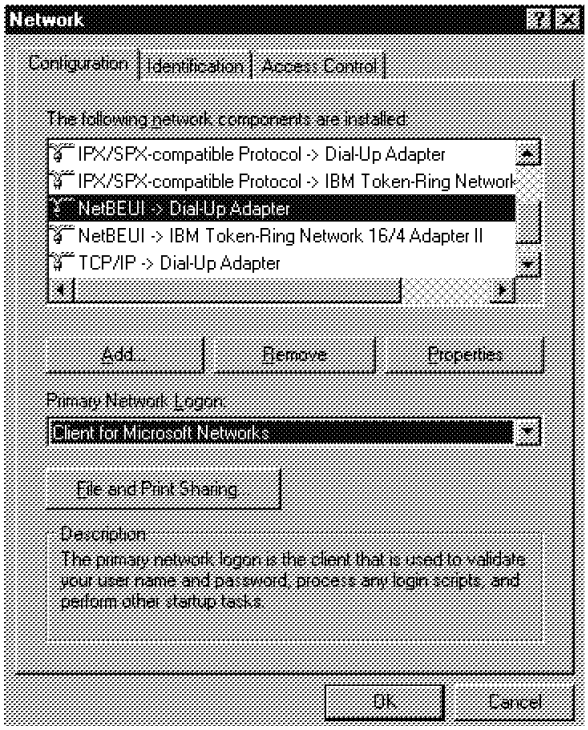


Figure 45. Windows 95 - Bindings

When you are satisfied with the results, click on the icon that you have created in the Dial-Up Networking folder, and you will get the Connect To window as shown in Figure 46. This is where you provide your 8235 user ID, password, and phone number to be dialed.

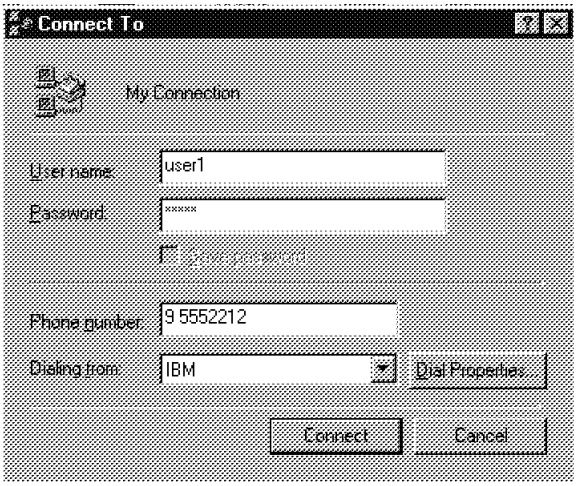


Figure 46. Windows 95 - Dialing

Click on **Connect** to start dialing. When the modems connect, your user ID and password will be validated. You will not be able to receive a banner message, but you will get connected and you will be able to use your applications and protocols as configured. The duration of the connection and (on request) server type and enabled protocols are displayed (see Figure 47).

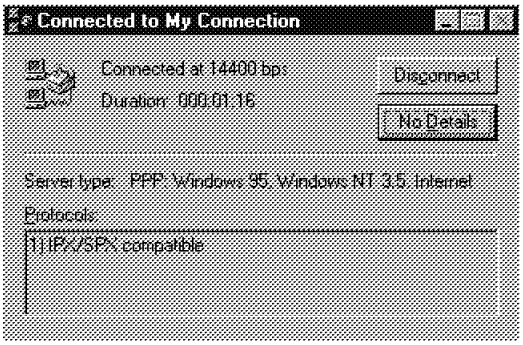


Figure 47. Windows 95 - Connected

6.2.1.2 Windows 95 Security Pack

Using Dial-Up Networking as it ships from Microsoft, users can dial directly into an 8235 (for which they have dial-in privileges) but cannot take advantage of advanced features specific to the 8235. Using the 8235 Security Pack for Windows 95, users of 8235s can take advantage of these dial-in features not available to other Dial-Up Networking users.

The following features are supported by the Security Pack:

- Roaming dial-back (fixed dial-back is supported without the Security Pack)
- Changing the dial-in password
- Advanced security dialog boxes
- Display of warning message if password has expired (Grace Login message)
- Display of banner message and server generated alerts

6.2.1.3 Installing the Security Pack

Follow these instructions to install the 8235 Security Pack. You will be asked to restart Windows after completing the installation.

1. Expand the self-extracting 8235 Security Pack archive into any temporary directory, or insert a diskette containing the expanded 8235 Security Pack files.
2. Open **Control Panel**, and start **Add/Remove Programs**.
3. Click on the **Windows Setup** tab.
4. Click on **Have Disk**.
5. Locate the directory or disk that contains the 8235 Security Pack installation files, and then click **OK**.
6. Select the check box next to IBM Security Pack for Windows 95 (so that it contains a check mark, see Figure 48 on page 120), and then click on **Install**.

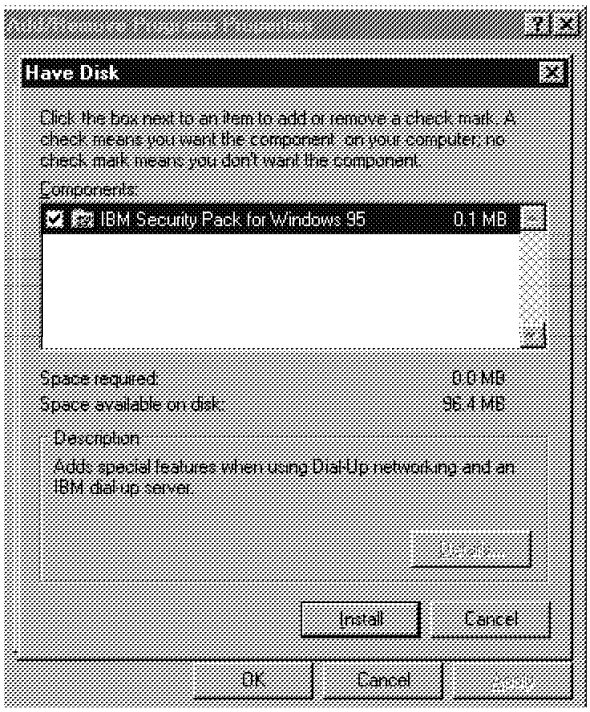


Figure 48. Windows 95 - Security Pack Install

7. You will find the IBM Security Pack for Windows 95 in the list of components that show a checkmark, indicating that they are installed (Figure 49).

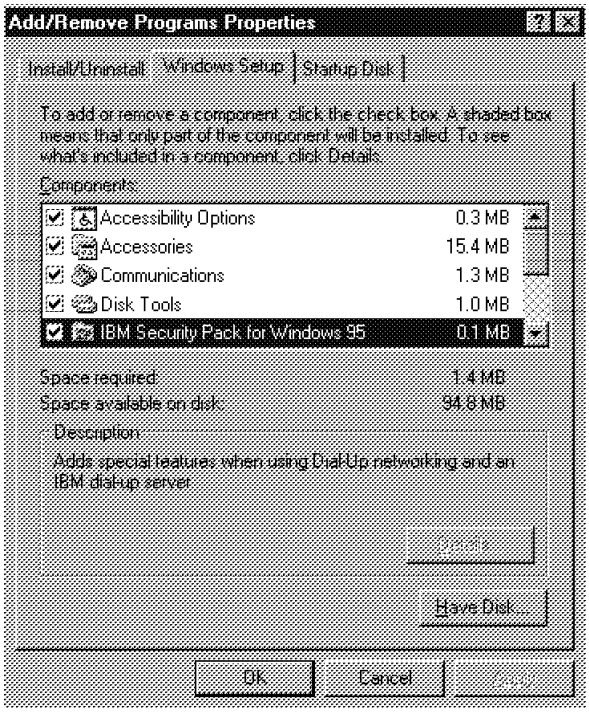


Figure 49. Windows 95 - Security Pack Install Complete

8. Click on **OK** to close the Add/Remove Programs dialog box and finish the installation.

9. When the dialog box appears suggesting that you need to restart the workstation, restart Windows 95 by clicking on **Yes**.

Now you have access to the five additional features mentioned above. The additional messages and the advanced security dialog will be invoked as appropriate without further action required. You will not notice any change unless these boxes appear. The change password feature, however, and the dial-back feature, have a visible effect and will only be carried out if you invoke them.

6.2.1.4 Setting Up a Roaming Dial-Back Number for a Connection

To set up roaming dial-back for a Dial-Up Networking connection to an 8235:

1. Set up your dial-in connection as described in 6.2.1, “Windows 95” on page 116.
2. When you have set up the dial-in connection, click on the **Start** menu, and then choose the **Programs** submenu, then the **Accessories** submenu, and then the **Roaming Dialback Tool** (see Figure 50).
3. In the Connections list, select the dial-in connection for which you want to set up roaming dial-back.
4. In the Phone Number field, enter the telephone number to which your modem is connected.
5. Click on **Apply** to save your changes to this dial-in connection.
6. Repeat steps 1 through 5 for any other connections for which you want to use roaming dial-back.
7. Click on **OK** when you have finished entering roaming dial-back information.

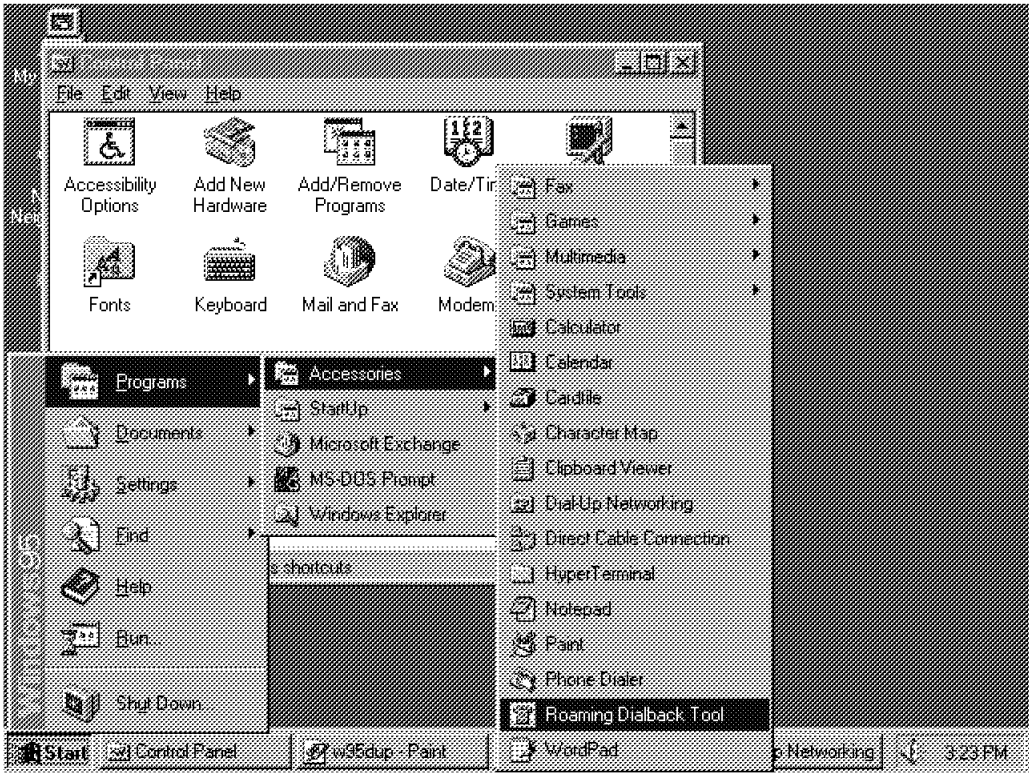


Figure 50. Windows 95 - Roaming Dial Back Tool

Now, every time when you start a connection for which you have set up roaming dial-back, the dial-back will be carried out without any further action required. When you no longer want to be dialed back, follow the same steps and clear the phone number field.

Notes:

1. Enter the telephone number for your modem in the correct format for dialing a telephone number from the remote site (such as adding a 9 to use an outside line, a 1 for long-distance calls, or other access number; non-US users will require a different format).

   For example, if your modem was connected to (800) 555-1234, you might enter 9,1-800-555-1234 as the dial-back number if the telephone system at the 8235′s site requires a 9 before outside calls.

2. You must be dialing into an 8235 to use roaming dial-back. If you set up a roaming dial-back number for connections to remote access servers other than an 8235, it will be ignored.

3. If the remote network administrator has set up a fixed dial-back number for your dial-in account (so the 8235 will call you back at only the specified number for added security), the roaming dial-back number you set up here is ignored.

6.2.1.5 Changing Your Dial-In Password

8235s with Version 3.5 and higher firmware and software installed support the ability to change your login password while you are connected to the remote network.

Note: This feature must be enabled for your dial-in user ID by the 8235 administrator. However, there is no way to tell whether you have Change Password privileges until you follow these instructions; after you follow these steps, a message appears indicating either that the password was changed successfully, or that you did not have privileges to change your password.

Whenever you dial into the 8235 with the Security Pack installed, a Change Password for <YourName> icon appears automatically in the Windows 95 task bar (see Figure 51 on page 123). Follow these instructions to change your password while you are dialed in:

1. Click on **Change Password for <YourName>** in the Windows 95 task bar.
2. Enter your current dial-in password in the Current Password field.
3. Enter your new dial-in password in the New Password field, using up to 16 characters.
4. Enter your new dial-in password again (exactly as you did in step 3) in the Confirm New Password field.
5. Click on **OK** to send your new password to the 8235.

The new password takes effect the next time you dial into this 8235.

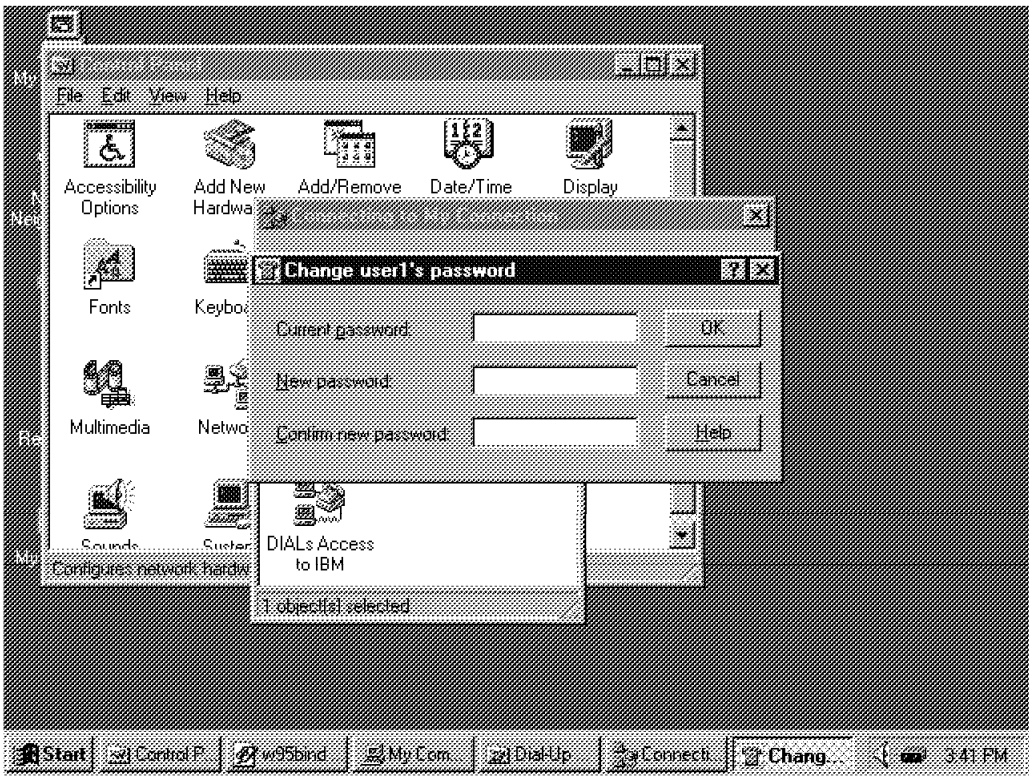


Figure 51. Windows 95 - Change Password

6.2.1.6 Using the Additional Dialog Box Features

The 8235 additional dialog box features are:

Advanced Security Dialog: If you are dialing into an 8235 with Version 4.0 or higher firmware and software installed that is configured with a third-party security device (such as a SecurID system from Security Dynamics), the 8235 Security Pack will display the Advanced Security dialog box, in which you can enter your third-party security information.

When you dial into an 8235, Windows 95 sends the user name and password you specified for the Dial-Up Networking connection. Once you have connected successfully to the remote access server, the third-party security device (if one exists) prevents you from communicating with the remote network until you have entered authentication information for it as well. Follow the instructions on-screen to satisfy the third-party security server's requirement. This may involve additional components such as SecurID cards or SecureNet Key token devices.

Note: If you are having problems with the dialog boxes not appearing, upgrade to version 1.37 or higher of the Security Pack for Windows 95.

Grace Login Message: Refer to 10.2.1.1, "Global Settings" on page 221 for a discussion of the concept of grace login to allow network access for a configurable number of times even though the password has expired, in order to allow the user to change the password.

Banner Message: Refer to “Sending a Message at Login (Banner)” on page 230 for a discussion of the banner message feature of the 8235 to send a welcome message to every user dialing into the network. The 8235 can be configured such that only users capable of displaying banner messages are allowed in. If this is the case, Windows 95 users without the Security Pack will not get access to the 8235, because their system is not capable of displaying the banner message.

6.2.1.7 Uninstalling the Security Pack

You can remove the 8235 Security Pack at any time by following these steps. You will be asked to restart Windows after removing the 8235 Security Pack.

1. Open the **Add/Remove Programs** control panel as for installation.
2. Click on the **Windows Setup** tab.
3. Deselect the check box next to 8235 Security Tune-Up Pack (so that the checkmark disappears).
4. Click on **OK** to close the Add/Remove Programs window.

After you have removed the Security Pack, you can reactivate it at any time by following the instructions in 6.2.1.3, “Installing the Security Pack” on page 119.

6.2.2 Windows NT

There is currently no special support in Windows NT for the 8235. Windows NT uses the PPP interface to dial in. The following document provided by the IBM 8235 development group describes how to use Windows NT to dial into the 8235.

An 8235 to be used with Windows NT must be at minimum Release level 3.5. Do not attempt to use the Windows DIALs Client because you will get a `dial.386 Not Loaded` message when you try to run the client. Use the Remote Access Service that comes with NT.

Supported and Unsupported Features:

- NT Domains are not supported as user validation mechanisms. Users may, however, authenticate via any one of several other validation mechanisms and then log into an NT domain as if locally attached.
- NetBEUI is now supported with Windows NT. However, Security Pack 4 is required for NT 3.51 in order to properly negotiate the NetBEUI protocol.
- Dynamic IP addressing is supported with Version 3.5 microcode.
- Management Facility is not supported and is not planned to be supported.

Client Configuration Steps: If you have already installed the Remote Access Service Client, then the following may be different, but you make the configuration you will be using to dial into the 8235 similar to the following. These instructions are for NT 3.51; NT 4.0 should be similar.

First the Remote Access Service needs to be installed. (Your configuration should resemble the following one, regardless of whether you are doing it for the first time or modifying an existing one):

1. In the Control Panel, double-click on **Network**.
2. Choose **Add Software**.

3. Make sure the Remote Access Service is selected in the next window that pops up. (At this point it is a good idea, if not a requirement, to have the CD for Windows NT 3.5 in the CD-ROM drive.)
4. Select **Continue**.
5. When the window for the path of the install files is displayed, make sure it is correct. Then click on **Continue**.
6. When the next window pops up, select the COM Port you are using for your modem; then click on **OK**.
7. You may have it detect your modem, but it will take a minute or two. Not all modems will be able to autodetect; be sure to select the correct COM port.
8. On the Configure Port page, make sure the correct modem is selected in this window. If your modem is not in the list, then see below on how to add a modem entry and begin the whole process again.
9. We highly recommend that you select **Dial Out Only** on this page as other options may not allow you to dial.
10. Next comes the Protocol Configuration by selecting **Network**. It is best to leave all of the protocols enabled, so that you can add and remove the protocols you are going to use in the Remote Access Program itself.
11. Click on **Continue** in the Remote Access Setup window.
12. Then comes the Bindings by clicking on **Bindings**. You bind the protocols you are going to use to the MS PPP driver. This could be called Remote Access WAN Wrapper.
13. Click on **Networks**, if it will allow you to click on it, and put the Microsoft Windows Network before the NetWare Network. This will only occur if you have installed the NetWare client (on the server package, it is called NetWare Gateway Services).
14. Click on **OK** in the Network Settings page and allow the machine to reboot itself.

Next comes the RAS Phone Book Entry. (Your configuration should resemble the following one, regardless of whether you are doing it for the first time or modifying an existing one.)

1. Open the **Remote Access Program** group.
2. Double-click on the **Remote Access** icon.
3. Once it comes up, it will then prompt you to fill in some information. You fill in the Entry Name, Phone Number, and Description lines just as you would the DIALs Client.
4. If the dial-in name is different from the workstation name, then it is required that the Authenticate Using Current Name and Password box be unchecked or disabled.
5. Click on the **Modem Settings** button and configure the settings on a per site basis. You should have enabled Hardware Flow Control, Error Control, and Modem Compression. The modem speed should be set to the maximum that the modem supports. Then click on **OK**.
6. The X.25 and ISDN settings should be set accordingly to your specific hardware. Once you finish with those settings, click on **OK**.

7. Click on the **Network** icon. The protocols are selected on a per site basis, and PPP should be selected for best performance.
8. IP and IPX protocols should be selected as they are needed. NetBEUI is not supported and should not be selected. (It all depends on your situation as to whether you need to run IPX, IP or both.)
9. If you are using IP, then you will need to click on **IP Settings** to set those options.

   Select the Server Assigned IP Address if you are going to allow the 8235 to give the client its IP address. (This requires an IP on the port or in the user list for the login name.)

   Select the Required Specific IP Address if you are specifying a specific address on the client and a valid IP address needs to be given to the client. (This requires that the 8235 be set to allow the client IP address; a different address needs to be set here if you are also connected to a LAN using IP.)
10. The Request LCP Extensions check box enables newer PPP features. If you are having persistent problems, then clear this box. (This box has the Time Remaining and Requesting Callback features that most users are not going to need, especially if these features cause problems.)
11. The SLIP setting is tested and supported but is not recommended as it is slower and requires more configuration steps that could go wrong. (You will only have IP with this setup anyway).
12. Once you have all these settings in place, then click on **OK**.
13. Click on **Security Settings**. Then set the option of Accept Any Authentication Including Clear Text. Other settings will not allow you to go through the 8235. Third-party security devices or authentication devices are supported and should be selected if you are using any. Select the After Dialing option of Terminal so you will be given a prompt after the modems connect; this is so you can log in through your security device.

To add a modem entry if your modem is not listed:

1. Make a backup copy of the modem.inf.
2. Copy one of the sections already in the file and put the copy at the end.
3. Change the section name to the name of the modem.
4. Make modifications according to the modem′s documentation (you can also get help from our document on Modem Initialization requirements).
5. If all else fails, then call the modem′s manufacturer.

Troubleshooting: **Problem:** Unable to access any Novell servers and make an IPX connection.

Possible solution: The NetWare Client needs to be loaded as a protocol in the Network Control Panel (on the server package it is called NetWare Gateway Services).

Problem: An error pops up when you try to connect to the 8235, which says there is an advanced option not set properly.

Possible solution: Click on the **Network** icon in the Control Panel icon group and click on **Network** to move the Microsoft Network above the NetWare Network. (This is only a problem if you plan to use IPX/SPX in this configuration.)

Troubleshooting tools: There are two log files that can be generated, but they have to be enabled.

1. This one is more for the general PPP type of logging. Go into the registry. Go into the section of HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP and set logging to 1. This will produce a file called \WINNT35\SYSTEM32\PPP.LOG and for more information see the Windows NT manual and online help.
2. This one is more for the modem connection problems. Go into the registry. Go into the section of HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters and set the logging to 1. This will produce a file called \WINNT35\SYSTEM32\DEVICE.LOG. For more information, see the Windows NT manual and online help.

6.3 Connection File and Advanced Client Setup

The DIALs Connect application manages the configuration of modems, phone numbers, passwords, and other items that establish the connection between the remote PC, the 8235, and the LAN. DIALs Connect needs to be active only while connecting and disconnecting. However, it can remain loaded during the connection to provide information about the status of the call, traffic statistics, modem configuration, alert messages, and more.

A separate connection file needs to be created for every remote network you want to access. The connection file contains all of the information the DIALs Client needs to connect to the remote network. When you create a connection file for dialing into a remote network, you should save the connection file and use it each time you want to connect to that particular network. Connection files have the file extension IR. To create a connection file, use the function **Make Icon** in the File menu. The icon will be associated with the connection file that is active while you create it.

Prior to running the DIALs connect application to create a connection file, the following information should have been obtained:

- The telephone number to dial
- A valid user name and, if required, a password (strongly recommended)
- The network protocols such as IPX, IP, NetBEUI/LLC, which are required to make the connection.

6.3.1 Creating a Dial-In Connection File Using Connect

This section describes how to create and save a connection file. It applies to all platforms supported by DIALs Clients; however, some of the features do not apply to all of them. This will be noted when it applies.

See Figure 144 on page 217 and Figure 166 on page 243.

The contents of the Connect window are also saved in the connection file. An example can be viewed in Figure 164 on page 242.

1. Start Connect in your specific environment. The Connect window appears.

   Note: If you receive the message Dial-in driver not loaded. (for DOS), DIAL.386 driver not loaded. (for Windows 3.X) or DIAL.OS2 driver not

loaded. (for OS/2) you cannot connect to a remote network, but you can still create and save a connection file.

2. Enter a description of this connection file (for example, Salesnet) in the Description box. This field is optional and can be up to 63 characters long. The Windows version, however, will let you type in as much as you want, and will cut off the string after 63 characters.

3. Enter your dial-in user ID (for example, Sarah Woods; spaces are allowed) in the Name box. Dial-in user names are not case-sensitive and can be up to 32 characters long.

   Your dial-in user name is specific to the 8235 you are calling; it does not necessarily match your user name for using other services on the remote network such as your file server or E-mail ID.

4. If your user ID has a password, enter it in the Password box. Passwords may or may not be case-sensitive and are displayed as asterisks (*) when you type them. Alternatively, enter the password when prompted for it during the connection process. For security reasons, passwords are not saved to the connection file; so, you do not need to enter a password if you are not making a connection now.

5. Enter the telephone number of the network you are calling in the Phone Number field. Enter the number exactly as you would dial it manually, using up to 63 characters (including commas, hyphens and other special characters). Use commas if you need to add a pause (usually 1 to 2 seconds for each comma you use, but this varies with your modem). Hyphens are optional. This allows you to enter long-distance prefixes and telephone company charge codes.

   Note: Do not include any modem dial commands, such as ATDT, in the Phone Number field. Keep in mind that many modems cannot handle more than 36 characters for dialing, so that if the DIALs Client reports an error while dialing, this might be the cause.

6. Click on **Options** to set up the desired networking protocols and other features you want to use for this connection. The Connection File Options dialog box appears.

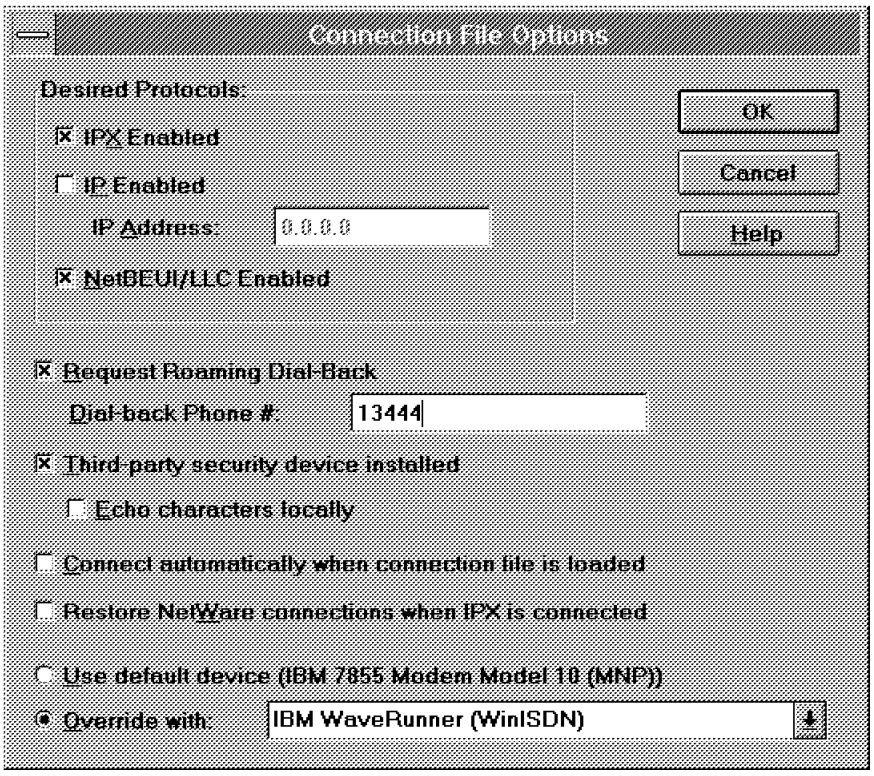


Figure 52. Connection File Options (Windows)

7. Enable the network protocols you want to use when connected. You can enable any combination of IPX, IP, NetBEUI/LLC by selecting the check box next to each protocol. However, you will be able to use a selected protocol only if the remote server also supports that protocol. To disable a selected protocol, reselect its check box.

   Attention

   As opposed to the 8235 configuration, you cannot enable NetBEUI and LLC individually for the client. This has an important consequence: If the 8235 is to support clients using NetBEUI/LLC, NetBEUI *must* be enabled, even if the client will only use LLC 802.2 for this application (for example 3270 emulation). If it is not enabled, protocol negotiation will fail.

   On the other hand, LLC only needs to be enabled on the 8235 if a client actually wants to use it for an application. If the application is LAN Requester using NetBIOS, no LLC is required on the 8235.

   Note: When using the IP protocol, filling in the IP Address field means working with a static IP address. From the 8235′s point of view, this corresponds to the first method: User on dial-in. The address specified here must match the one configured in the IP protocol stack if the IP stack does not support dynamic updates.

   If a dynamic IP address assignment is to be used, this field must be left at its default value 0.0.0.0. In this case, the IP address will be obtained over the dial-in connection from the 8235. There are two methods as to how this can be supported, depending on the protocol stack in use:

   - The DIALs Client dynamically updates the IP address in use by overriding the preconfigured value. This method requires you to use an

IP stack that is recognized and explicitly supported by the DIALs client. Currently (Release 4.5), this support exists for the following IP stacks:

- TCP/IP for OS/2 with DIALs/2
- Windows 95 TCP/IP
- Novell LAN Workplace
- PC/TCP
- A few others with limitations

  Note: The Online Software Configuration Notes of DIALs for Windows provides the full details.

- The IP stack uses either BOOTP or RARP to obtain its IP address from the 8235. This is only possible when a dial-in connection exists. Since most IP stacks will send the BOOTP or RARP request when they are loaded, this implies that they must not be loaded before the connection is established.

8. If your User ID is set up on the 8235 to support roaming dial-back, select the Request Roaming Dial-Back check box.
9. If you selected this check box, enter a phone number in the Dial-back Phone Number field. Be sure that this is a valid telephone number for the telephone system used by the 8235. Prefix numbers may be required for the 8235 to access an outside line (if it is attached to a PBX). However, these can either be defined here or in the Dial prefix field of the Port Configuration of the 8235. The latter is the recommended way to do it.

   Roaming Dial-Back lets you tell the 8235 to call your modem back at a telephone number that you specify so you can reverse the charges for the telephone call. This feature must be enabled for the user ID. The user can decide case by case for each dial-in session to request a call-back or not.
10. (Not available for DOS) Select the **Connect Automatically when Connection File is Loaded** check box to set up this connection automatically whenever this connection file is opened. If you do not enable this option, you must click on **Connect** to make a connection after you open the connection file.

    Note: If you select this check box, you must create an icon for this connection file for the DIALs Client to connect automatically.
11. The Third-Party Security Device Installed option tells the DIALs Client to open a third-party security terminal window for communication with a security server that is configured on the 8235.
12. The Echo characters locally option tells the DIALs Client to display characters on the screen as you type them. Select this check box only if you also selected the Third-Party Security Device Installed check box and the modem you are using does not echo keystrokes. (If it does, you will get each character echoed twice.)
13. (Available for Windows only) The Restore NetWare connections when IPX is connected option tells DIALs for Windows to automatically log on to Novell NetWare servers as soon as the dial-in connection is established.
14. (Not available for DOS) The Use default device radio button tell the DIALs Client to use the communications device that is currently set as a default in your port setup. This will change whenever you modify the port setup, even if the Connection file itself is not changed. This is the only option for releases before 4.0.

The radio button **Override with** allows you to select one of multiple communication devices that were pre-configured during port setup (see also 6.3.2, “Modem Configuration and Port Setup” on page 131) and select one of them via the connection file. This feature overcomes the former limitation that a connection file could not store any information about the communication device.

15. Select **OK** to return to the Connect box. Select either **Save** or **Save As** from the File menu to save your connection file.
16. The Save Client Connection File window appears. Save your connection files in the installation directory. Do not change this.
17. Enter the name of the file in the File Name box. Do not enter a file extension. The file extension .IR is automatically appended to the file name.
18. Select **Save** to save the dial-in connection file.

6.3.2 Modem Configuration and Port Setup

For the benefit of mobile users, the port and modem setup has been made more flexible in Release 4.0 and above. It now supports multiple dial-in configurations, including multiple communication devices (or multiple configurations of the same device).

When you select **Port Setup...** from the Tools menu, you will get the Port Setup window (Figure 53), which holds the current default settings. These will be selected if the Connection File selects the default device or if you are not using a connection file. An initial setting for this window is created during installation. If you have previously enhanced the modem setup by adding other devices, the Modem drop-down list will contain these devices.

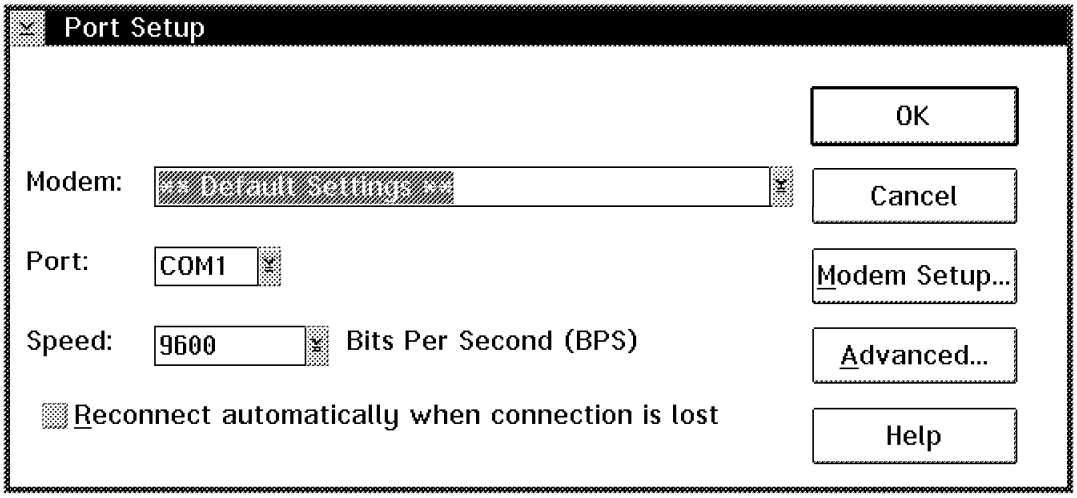


Figure 53. Modify Client Port and Modem Defaults

Click on **Modem Setup...** if you want to add or remove modems to your list of installed devices. You will get the Modem Setup window (Figure 54 on page 132). The Available Devices list holds all modem and communication adapter definitions that are stored in the MODEMS.INI file that is copied to your DIALS directory during install, along with all definitions that you may have added. The latter are stored in the MODEMS2.INI file, which is created the first time you create or modify a modem entry. The **Install** button allows you to add more devices to the Installed Devices list. The **Remove** button reverses this.

Note: The **Detect...** button for modem autodetection does not work in the OS/2 client at level 4.0.2. This has been fixed in 4.5.

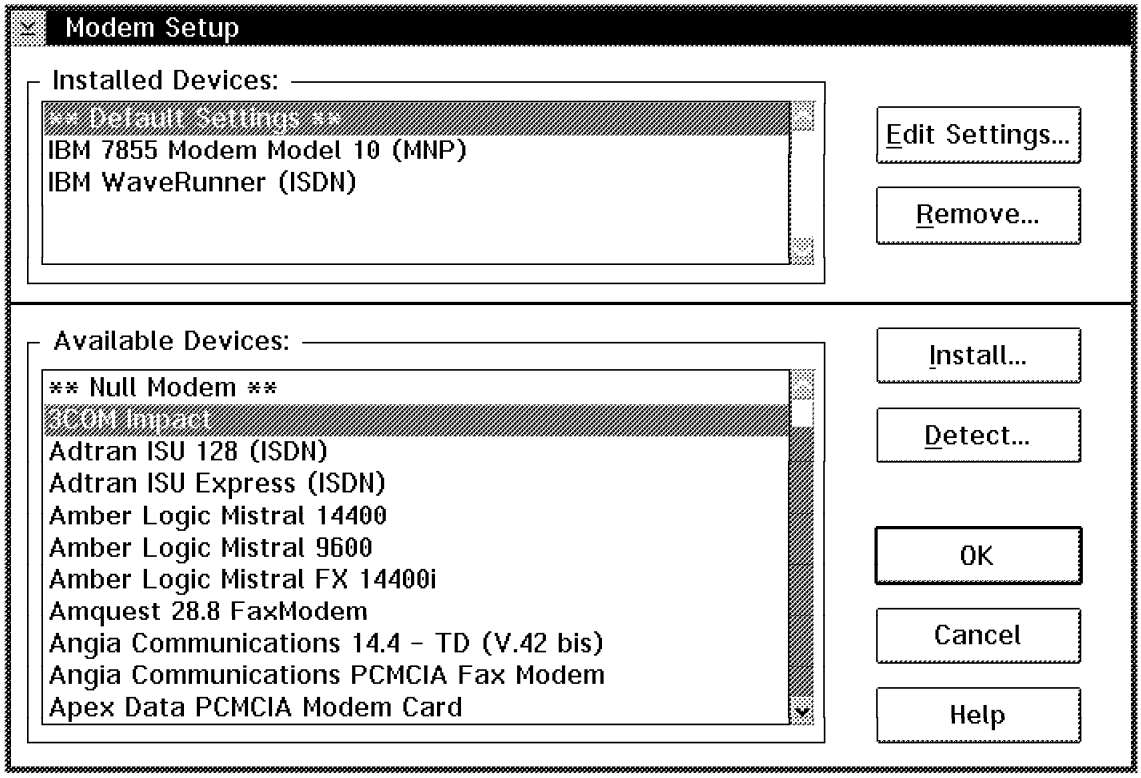


Figure 54. Install or Remove Communication Devices

You can only modify the devices in the Installed Devices list. Use the **Edit Settings** button. You will get the Edit Modem Configuration window (see Figure 55 on page 133). This is where you actually change modem strings, the maximum port speed and the flow control method.

The Initialize string is used to dial in; the Answer Init string is used for call-back when re-initializing the modem after hang-up. For ISDN cards, as shown in this example, there is only an ATZ reset command; this may depend on the card, however. We strongly recommend that you use Flow Control Hardware if the modem in use supports this method (also referred to as RTS/CTS). This will reduce the risk of overrun errors.

When you change the Modem Name, you will create a new entry; otherwise, you replace the existing one.

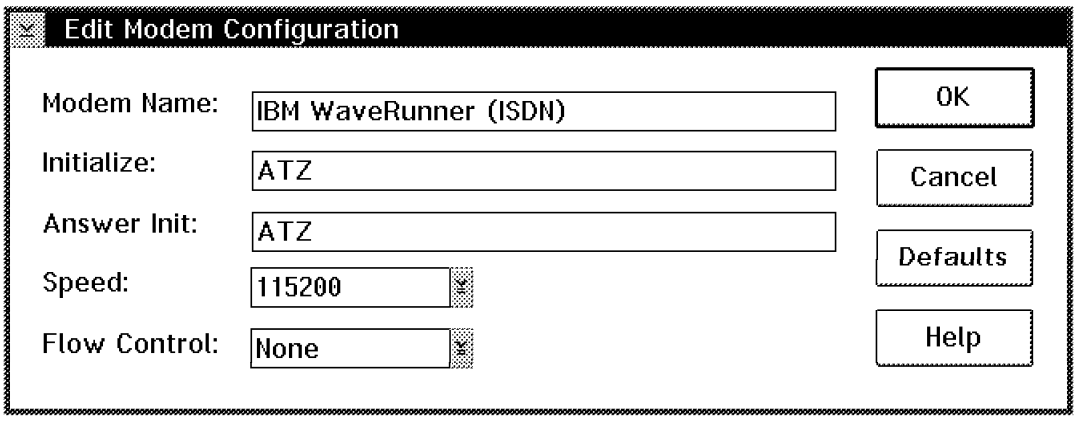


Figure 55. Edit a Modem Setup

There is one other place for setup parameters that apply to the current default port setup. Consequently, it is accessed from the Port Setup window, by selecting the **Advanced...** button. Depending on whether this device is an external device connected to a COM port (see Figure 56) or an integrated ISDN adapter card (see Figure 57 on page 134), you will get a different dialog window with different parameters.

Note: PPP compression and virtual connections are available for both analog and ISDN connections.

PPP compression is a software compression method used between the DIALs Client and the 8235. It was mainly implemented to support communication devices that do not provide compression of their own. Today, most of the standard modems have built-in compression, either MNP5 or V.42 bis. The modem Init string configured for a modem should activate this function. Whether the dial-in connection will actually use modem compression depends on the negotiation between the two modems. PPP compression can be useful even for modems, as it uses a different algorithm to increase throughput.

The situation with ISDN adapters is different, however. There is no standardized compression method. Some adapters do not provide any compression at all; others use a proprietary method that only works between two adapters of the same make. PPP compression will significantly improve the throughput in these cases. The compression rate depends on the type of data; it will be low if the data has been compressed before (using file compression, for example) or if it is binary. The best results can be observed for ASCII text data; the compression ratio may range between 2:1 and 8:1.

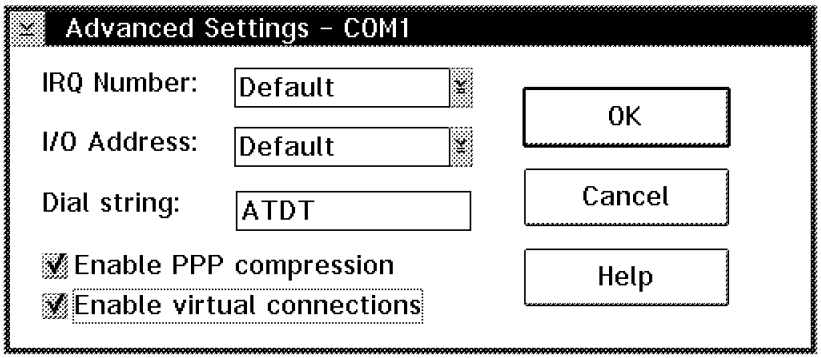


Figure 56. Advanced Modem Settings

Only in rare cases will you have to modify the defaults for IRQ and I/O addresses. The Dial String should either be ATDT (tone dialing) or ATDP (pulse dialing) depending on the type of network or PBX to which the client workstation is connected.

Attention

Changes to the dial string are the main reason for frequent use of this window. Mobile users may have to use tone dialing in one location (for example, the office, equipped with a PBX) and pulse dialing in another location (for example, at home). Many countries still have public telephone networks that require pulse dialing.

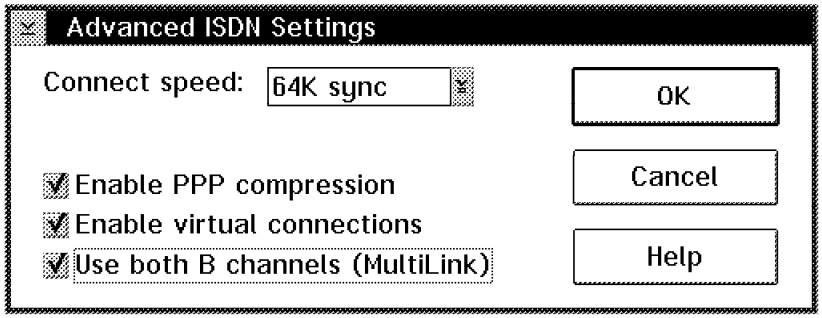


Figure 57. Advanced ISDN Settings

For ISDN, the option to select between 64 kbps, 56 kbps, and 56k Data Over Voice (DOV) applies mainly to the US. All other countries use 64 kbps only. The 56k DOV technology is used to get near ISDN throughput for the cost of a voice call, which some telephone operators tariff at a lower rate.

Note

This is the place where the client specifies that a multilink connection, combining two ISDN B-channels, is to be used. However, this must be enabled on the 8235 in order to make it work properly. If, during dial-in, the second B-channel cannot be established, the connection will fall back to a one-B-channel connection.

6.3.3 ISDN and Advanced Client Setup

The DIALs Client has a number of features designed to take advantage of high-speed connections, such as those you can establish using ISDN. ISDN has several significant advantages over the use of analog modems:

- Fast connection establishment: one to three seconds
- Higher data rate: 64 kbps minimum, further increase possible through
  - Channel aggregation
  - Data compression
- Digital end-to-end, hence more reliable

For example, a V.34 modem is capable of connection speeds of up to 28.8 kbps (without data compression). If your workstation has an ISDN terminal adapter (TA) and you have a working ISDN line, you can call an 8235 with an ISDN

connection at speeds of up to 64 kbps. If you are using the IBM WaveRunner Digital Modem, you can connect to an 8235 containing an ISDN BRI module at speeds of up to 128 kbps.

The DIALs Client offers the following additional features when you are connecting by way of ISDN lines:

- Virtual connections
- Multilink protocol (MLP) connections using two ISDN B-channels.

  The DIALs Client supports MLP only if you are dialing into a remote network using an ISDN adapter.

For both features, the answering 8235 must be configured to accept that feature on dial-in connections.

Configuring the DIALs Client for ISDN: You should have installed the ISDN card and software required to operate it before installing the DIALs Client (or before activating the ISDN card in the Port configuration).

When the adapter card setup is completed, it is very simple to enable its use for DIALs. It is as easy as installing another modem as seen in 6.3.2, “Modem Configuration and Port Setup” on page 131. The only difference is the fact that port and port speed are disabled because they do not have any meaning (see Figure 58).

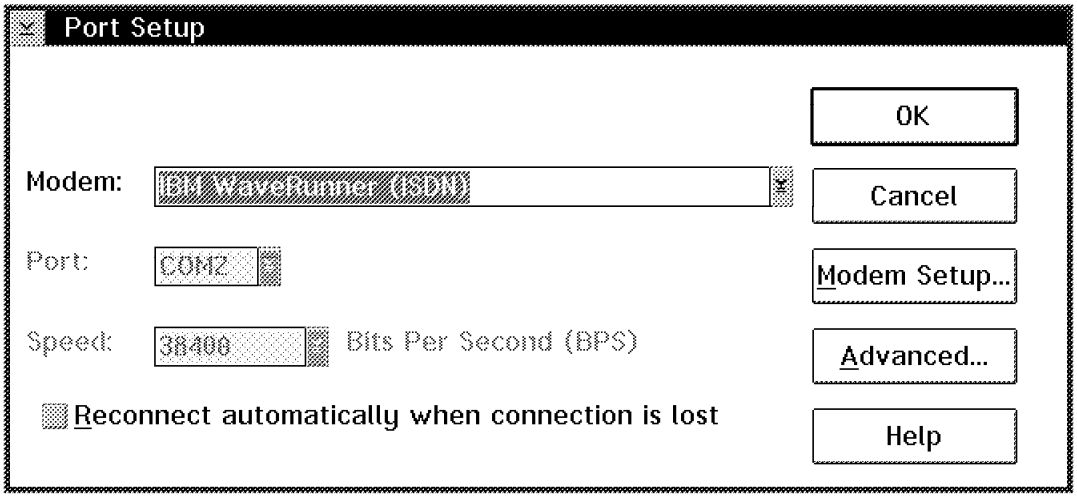


Figure 58. DIALs for OS/2 ISDN Port Setup

Everything else will be taken care of by the DIALs Client. This includes activating the required drivers that come with the DIALs Client to support the ISDN cards in cooperation with the drivers provided by the card itself. No drivers need to be set up directly by the user. A reboot (or a restart of Windows) is required, however, in order to load the required drivers.

A few considerations regarding the different DIALs Client platforms are necessary, however.

- There is no ISDN internal card support for DOS.
- The DIALs Client for Windows uses the WinISDN interface to access the card drivers.

Note that in case of the IBM WaveRunner card, there are additional modules (ISDN port monitor) that do not exist for the other supported cards. The following cards are supported:

- IBM WaveRunner ISA/MCA
- IBM WaveRunner PCMCIA
- ISDN*tek Cyberspace Card
- Synaptel Syncard PC

- The DIALs Client for OS/2 currently supports only the IBM WaveRunner card by providing dedicated drivers. Note that the WaveRunner Helper, unlike the other drivers, is not installed in a system configuration file such as CONFIG.SYS, AUTOEXEC.BAT or WIN.INI. It is loaded via STARTUP.CMD; the entry is added to that file by DIALs Connect when the ISDN card is installed. When the WaveRunner Helper is started, it checks for the presence of DIAL.OS2 (either DIALNDIS or DIALODI) and terminates itself if this is not found.

  Note: When the STARTUP.CMD is in REXX syntax, the Start command added to it by DIALs will violate the syntax. In this case, either change it to meet the REXX syntax requirements or consider creating an icon and placing it into the OS/2 Startup folder.

6.3.3.1 Virtual Connections

Virtual connections (VC) minimize connect-time costs by physically disconnecting the circuit when there is no meaningful traffic. In addition, the VC offer increased ease of use and management because connections need to be made only once. Thereafter, VCs come up when required and are suspended during periods of inactivity.

Virtual connections are enabled on the Advanced Settings dialog box (see Figure 56 on page 133 or Figure 57 on page 134) by selecting the appropriate check box. The selection is stored in the DIALS.INI file. The remote 8235 must be configured to support VC also; otherwise, a VC will not be established.

Note: NetBEUI/LLC must be disabled on the client if a VC is to be used. It is not supported with VC. See Figure 59. This does not apply to the 8235; it may support either NetBEUI or LLC for other clients (with non-virtual connections) while VC are enabled.

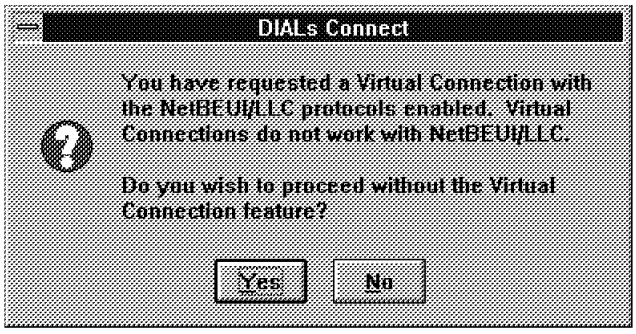


Figure 59. Virtual Connections and NetBEUI/LLC

Once a VC has been established, the suspend timer is started and the data traffic is monitored on both sides of the connection. When the timer reaches

zero, the connection is suspended by terminating the call, starting the spoofing mechanism and monitoring all transmit data. Depending on the data being considered as meaningful or not, they will either be ignored, spoofed locally or they will cause the connection to be resumed and brought back to the *up* state. A new connection will be dialed. This can only be done from the client side; the 8235 will never reestablish a dial-in VC.

While the connection is up, each data packet sent in any direction will reset the suspend time to its initial value. The Virtual Connections statistics page provides a collection of data related to the behavior of the connection. It can be used to verify whether the purpose of a VC (saving on connection charges) is achieved.

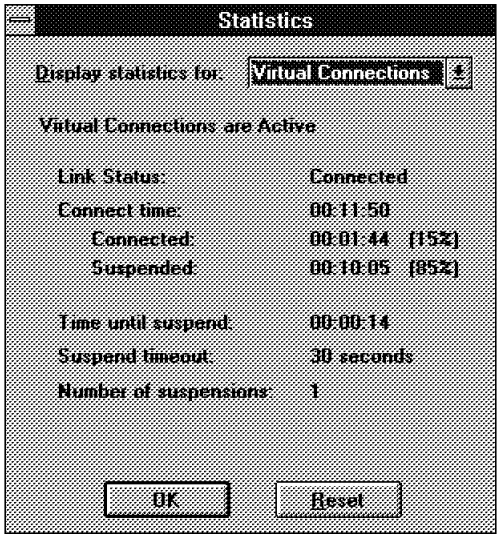


Figure 60. Virtual Connections Statistics

Application Notes: For virtual connections to operate correctly, disable any automatic update features in all applications that send or receive network data through a dial-in virtual connection.

Lotus Notes: To use Lotus Notes over a virtual dial-in connection, disable the automatic updating feature. In Notes, choose **Setup, Mail** from the Tools menu. The Mail Setup dialog box appears. Disable the Check for New Mail check box. Click on **OK** to save your changes and close the Mail Setup dialog box. (If this feature is selected, Notes will check for mail regularly, forcing the DIALs Client to reestablish the virtual connection each time.)

6.3.3.2 Multilink Connections

The DIALs Client for OS/2 and Windows provides support for high-performance channel aggregation using the industry-standard Multilink PPP Protocol (MLP). This feature allows dial-in connections to use multiple ISDN lines in a single connection session, providing increased bandwidth and performance.

Using the DIALs Client and an ISDN connection through your workstation, you can connect to an 8235 using up to two B channels on an ISDN BRI module. You can use MLP over direct, fixed, or roaming dial-back multilink sessions. To use MLP over a dial-in connection, you must:

1. Enable the **MLP** check box in the Advanced ISDN Settings dialog box.
2. Use a supported integrated ISDN card.

3. The 8235 must be configured to allow MLP connections.
4. Of course, the 8235 must be connected to an ISDN line through one or more ISDN BRI modules or external terminal adapters (TAs).

If all of these conditions are met, the DIALs Client establishes an MLP connection automatically when you dial in.

In the DIALS.INI control file, in the [Multilink] section, there are additional parameters that control the operation of MLP connections. Normally it will not be required to modify these parameters; the defaults will yield satisfactory results.

The Multilink statistics page provides a collection of data related to the behavior of the MLP connection. It can be used at any time to verify that the connection is up and actually uses two channels.

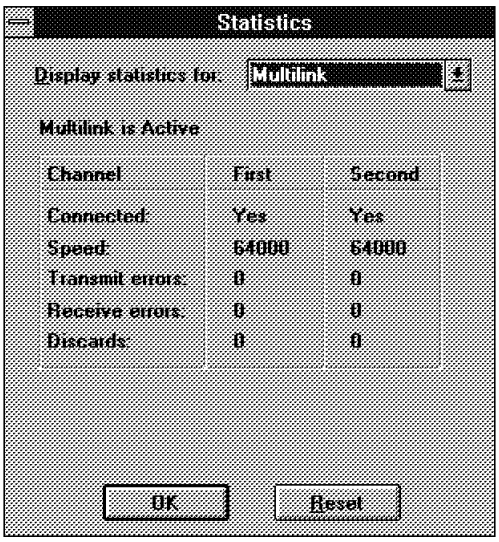


Figure 61. Multilink Statistics

If, for some reason, the second B-channel cannot be established, the connection will not automatically fail, but instead, will fall back to one channel.

6.3.3.3 Some Thoughts on Tariff Management

Both VC and MLP are attempts to optimize connection charges while maintaining maximum throughput. However, these methods may not be sufficient given the complexity of telephone charges in some cases. Phone charges normally depend on the duration of the connection. In some cases, a basic fee is charged for connection establishment, so that the first charge unit is more expensive than the remaining ones. In some countries, even unsuccessful attempts to connect are charged, provided the call was delivered.

Virtual connections cannot cope with all these variations; this brief discussion is supposed to cover a more common situation. Assume a three-dimensional tariff structure like this:

Table 24. A Sample Phone Tariff Structure

Time of day	Mo-Fr				Weekend			
	local	region	long-1	long-2	local	region	long-1	long-2
22-6								
6-9								
9-12								
12-18								
18-22								

In order to save on charges (rather than increase your charges), the suspend timer of a VC must be adjusted to the length of a tariff charge unit. Consequently, the optimal value for this timer varies with time of the day and with the day of the week. In addition, if the user is mobile and accesses the 8235 from different tariff zones, another dimension of variations comes into effect.

The timer value is stored in the DIALS.INI file. This file is unique, so the user must manually edit this file every time a different timer value is needed. In order to reduce this effort to a minimum, a standard timer value should be chosen that covers most of the cases in a reasonably good way. This value should not be less than the smallest charge unit in use at any time.

6.3.4 Statistics of a Dial-In Connection

At any time (even if no connection is active) the Connect application can be used to display statistics pages. They provide counters and status information regarding various aspects of the dial-in connection:

- Port: status, port used, speeds, serial chip hardware, errors, time values
- Errors: receive and transmit errors
- IP: status, receive and transmit statistics, IP address of client and host (8235)
- IPX: status, receive and transmit statistics, IPX net address and node address of client
- NetBEUI: status, receive and transmit statistics, NetBIOS name, and node address (the statistics apply to both NetBIOS and LLC)
- Compression: status, separate statistics for transmit and receive regarding achieved compression rate
- Virtual Connections: status, current status, cumulated times and current timer values, number of suspensions
- Multilink: status, separate statistics for each channel

These statistics can be viewed for troubleshooting and tuning purposes.

6.3.5 Logging a Dial-In Connection

A new function with Version 4.0 is the DIALs Client Logger (PPPLOG.EXE), available for Windows 3.x, Windows 95 and OS/2. In the case of a persistent problem using DIALs Client, it provides the option to log technical details of the dial-in connection, such as the state of data compression, data frames transmitted and received, and so on. This may be requested by IBM technical support.

In most cases, you should start the DIALs Client Logger before you run the DIALs Client, to ensure a complete record of what happens as you establish your dial-in connection. To use the DIALs Client Logger:

1. Get a command line, type `C:\DIALS\PPPLOG.EXE` and press Enter. If you installed the DIALs Client in a directory other than C:\DIALS, enter that path instead. When the DIALs Client Logger first opens, a dialog box appears, which allows you to select options.

   Note: You can create an icon for the logger if you need it frequently. This is not provided by default because users generally do not need to use this feature.

   Note: In Windows 95, right click on the icon in the taskbar tray, and select logger instead of the execution step noted previously.

2. In the Log Filters section, select the check box next to the information you want to log.
3. If you want the DIALs Client Logger to display the log information on-screen (in its own window) during your dial-in connection, select the **Display Log events on screen** check box in the Output Options section.
4. If you want the DIALs Client Logger to save the log information as an ASCII text file during your dial-in connection, select the **Save log events to disk** check box in the Output Options section. If you select this check box, you must also enter a name for the path and file in which you want to save the log information. For example, you might enter `C:\PPPLOG.TXT` to save the information root directory of your C drive.
5. When you have selected the options you need, click on **OK** to begin logging the dial-in connection. No activity will be logged until the DIALs Client Connect program is running and you start to establish a dial-in connection.

You can pause activity logging temporarily while you browse the log, copy information, and resume.

Note that once you start logging information, you can close the DIALs Client Logger program while logging continues in the background. When a dialog box appears asking whether you want to disable logging while the log application is not running, click on **No** to continue collecting log information.

Note: This stores incoming messages into a buffer to be read by the logger at a later execution point. This does not continue to append the incoming log messages to the file, if the log is being saved to disk. If this buffer fills before it is read, the oldest message will be deleted to make room for new messages.

Note: For the best results, you should always set up the DIALs Client Logger to save the log to an ASCII text file in addition to (or instead of) displaying the information on-screen. If your workstation screen is not wide enough to display all of the columns of information collected by the Logger, the Logger truncates the information that can not be displayed. However, all log information that the Logger collects is saved to the ASCII text file you specify, regardless of how much information can be displayed on-screen.

When you view the log information on-screen or in a text file, it looks similar to the following example:

```
 1 - 16777.247   Rx:   32 bytes    Channel: 0  NetBEUI
 2 - 16777.247   NetBEUI  Rx       NetBIOS   NR=79  NS=18
 3 - 16777.247   NetBEUI  Tx       RR       NR=19
 4 - 16777.247   Tx:   18 bytes    Channel: 0  NetBEUI
 5 - 16775.184   Rx:   43 bytes    Channel: 0  NetBEUI
 6 - 16775.184   NetBEUI  Rx       NetBIOS                        Add
 7 - 16774.872   Rx:   31 bytes    Channel: 0  NetBEUI
 8 - 16774.872   NetBEUI  Rx       NetBIOS                        Add
 9 - 16772.747   Rx:    8 bytes    Channel: 0  LCP       Echo-Request
10 - 16772.747   PPP Event          LCP       Event: RXR         Stat
11 - 16772.747   Tx:    8 bytes    Channel: 0  LCP         Echo-Reply
12 - 16771.716   Rx:  185 bytes    Channel: 0  NetBEUI
```

Note: The numbers listed in the second column indicate the time the event occurred in the number of milliseconds either since you first started logging or since you last selected **Clear Log** from the Edit menu. This means that the number will be negative if the event occurred before you started logging or cleared the log, and positive if it occurred after that point.

6.4 Performance Considerations

Many of the performance aspects relate to a specific protocol or application. They will be discussed in that context. However, some issues are more general. These are presented in this section.

OS/2 Autostart: During startup, the OS/2 desktop restarts applications that were previously running. For network applications, this can cause delays because a dial-in connection to a remote network has not been made.

To disable this feature of the OS/2 desktop, change the AUTOSTART= statement in the CONFIG.SYS file to:

```
AUTOSTART=TASKLIST,FOLDERS
```

Programs that need to be started during the OS/2 startup can be added to the STARTUP.CMD file after the statement:

```
C:\DIALS\CONNECT2.EXE
```

Keep things local: When you run an application program (.EXE) file from a disk, your workstation has to read it into memory (RAM) to run it. If the program is on a remote file server, this process can be very slow due to the much lower speed of a dial-in connection as compared to a LAN connection.

For the best performance over a dial-in connection, you should load application programs from the hard disk of your workstation rather than from a remote network server.

Follow this procedure to prevent accidental running of application programs from a remote network server:

1. Make sure that all of the necessary files for an application are on your local hard disk. Many programs need more than just an EXE or COM file to run. They also need dynamic link library files (DLL), online help files (HLP), and so on. If you are not sure whether you have all of the files you need on your hard disk, use the original program disks to reinstall them on your local hard disk.

2. Make sure that any batch files, program information files (.PIF), and menu front-ends on your local hard disk are set up to run applications on your local disk, not on the hard disk of the server.
3. Make sure that your PATH= statement does not include any network drives.

Modem Performance: Another key to optimizing the performance of your system is to have an understanding of how the computer communicates with the modem. Most V.34bis modems support speeds of up to 115.2 kbps. 115.2 kbps represents a combination of the physical speed between modems of 33.6 kbps and the ability of most modems to compress data at the ratio of 4 to 1. This means that although the modems talk to each other at 33.6 kbps, they talk to the PC at 115.2 kbps.

Not all combinations of PC hardware and software can operate as fast as the modems. Attempting to run a system faster than the PC configuration can slow performance significantly, as data packets can be lost and have to be retransmitted. This means that your system might run more slowly when configured for 57.6 kbps than it does configured for 19.2 kbps. This is compared with LANs, which run at 4 Mbps or higher. The speed difference on a typical file transfer is about 1000 to 1.

Along with the speed of the modem itself, there are three other factors that determine how fast a data rate a system can sustain:

1. The speed of the PC
2. Whether or not the serial port hardware buffers data
3. The operating system and memory management software on the PC

The way these three interact determines performance.

The modem receives data from the line one character at a time and passes it to the serial port. If the serial port supports buffering, it will wait until it has received several characters (usually 16) and then tell the DIALs Client that there is information to be read into the PC memory. The system software (operating system or memory manager) determines how long the serial port has to wait before it can ask the DIALs software to read its data.

A buffered serial port is faster. Buffering allows the serial port to ask the DIALs software to read data 16 times less often. For example, the buffered port reads data once for every 16 characters of data instead of reading every character.

Memory managers slow performance because they might make the serial port wait longer before passing data to the DIALs software. When the DIALs software waits so long that the modem and serial ports cannot store the data, serial port overruns result.

A faster PC processor improves performance because memory managers and operating systems do not have to make the serial port wait as long before transferring data.

Consequently, all four factors, modem speed, serial port type, PC processor speed, and system software, determine the speed at which you can operate your modem without causing lost packets and degraded performance.

The DIALs Client/2 software provides statistics regarding packet loss (serial port overruns, for example) that help determine the best configurations. On most

PCs, a chirping sound is emitted from the PC speaker when the serial port is experiencing overruns. The modem speed should be decreased until these overruns become less frequent.

The DIALs asynchronous statistics provide information about the serial port type. A 16550 UART type indicates that your serial port is buffered, whereas a 16450 indicates that it is not.

6.5 Other Types of Connections

The main purpose of the 8235 is to support dial-in connections for single users and other 8235s. These are generally based on analog (modem-based) phone connections or digital ISDN B-channel connections. However, there are other constellations that are also supported:

- Permanent connections
- Packet switched (X.25) connections via PAD

The special considerations that apply to these types of connections are briefly discussed here.

6.5.1 Direct Attach, Leased Lines

Leased lines and directly attached devices (via null modem cable) have the same characteristics from the 8235′s point of view: the connection is always supposed to be up, there is no modem and no dialing process. This is reflected by a single parameter in the MODEMS.INI modem data base: `Direct=Yes`. There is a default entry covering both cases: `[** Null Modem **]`. The port speed in this case should be the same as the line speed; flow control should not be used.

An important case when this would be used is direct attachment to a serial port for out-band management when, for some reason, in-band connectivity is not working. The most common settings for a serial port are 8-bit data, no parity, one stop bit, and 9600 bps. Set your terminal or terminal emulation accordingly, unless you have changed a port and know its current port speed.

6.5.2 X.25 via PAD

The 8235 allows dial-in capability over many connection types. In place of a modem, almost any RS-232 device can be used. This means the connection can be made, for example, through a modem using standard analog phone lines, an X.25 PAD, a PBX, a security device, a cellular modem, or a DSU/CSU with analog output, over a digital line. This section focuses on a particular type of digital service, packet-switched networks, commonly referred to as X.25.

6.5.2.1 Packet-Switched Digital Networks

Packet switching, in contrast to circuit switching, refers to the method by which data is routed across a network. Packet switching is advantageous in applications that do not continually stream data, but are short and bursty, such as electronic mail. Packet-switched networks are commonly referred to by the specification X.25, which specifies the interface between a host system and a packet-switched network. Data characters are bundled into maximum-size packets, addressed and routed across the network on a hold-and-forward basis. The X.25 specification covers packet format, methods of establishing a circuit, multiplexing, flow and error control, and sequencing. Depending on the service provider, this network allows access to multiple sites within the same provider′s

area, as well as connection to national and international packet carriers. In determining whether packet switching is appropriate for your needs, you should determine the type and amount of data being transmitted, the number of sites, and the cost. Further information on X.25, packet switching, and digital networks can be provided by your telecommunications provider.

6.5.2.2 Ordering the Digital Interface

Your local telephone company should have information about X.25 and other digital services. The actual service name will vary by carrier, and multiple variations of packet-switched networks may be available in your area. When selecting an X.25 PAD or any communication device to be used with an 8235, be sure that it supports an RS-232 DTE interface and either in-band AT commands or manual dial. For more information on Packet Switching or other digital data services, contact your phone company.

6.5.2.3 8235 Solution

A number of X.25 PAD, Switched 56 DSU, and ISDN service unit vendors offer connections to the phone company's digital services while providing the option of an RS-232 DTE interface to connect to the 8235.

6.5.2.4 Dial-In Client Configuration with DIALs Client

If the digital device supports the Hayes AT command set, you may use command strings (add a MODEMS.INI entry) to control the device. If the unit doesn't support the AT command set, but allows manual dial, the user runs the DIALs Client with the /m option for manual connection, dials the digital unit and, once connected, selects **Continue** to connect to the network.

The DIALs Client normally uses short retry timeouts (1.5 seconds) during PPP negotiation. For slow connections such as X.25 PADs, these timeouts are too short, and the connection cannot be negotiated. The following lines should be added to the DIALS.INI file and to the connection file (file with the .IR extension) to extend these timeouts to four seconds:

```
[Options]
LongTimeouts=Yes
```

6.5.2.5 Apple Remote Access (ARA)

When using a Macintosh with Apple Computer's Apple Remote Access (ARA) software to dial into an 8235, a Connection Control Language (CCL) script is used to communicate between the software and the modem. CCL scripts may be modified to accommodate connections other than the *standard* dial-in connection. For example, a CCL script may be modified to deal with a Mac directly connected to an 8235, or it could be made to deal with the negotiation through the X.25 network.

6.5.2.6 Configuration of the 8235

The following parameters should be changed to configure the 8235 for an X.25 PAD. These parameters can be added in the Additional Configuration page in the Management Facility or directly through the command shell.

X.25 PADs use an internal buffering transmission scheme designed for ASCII terminals. This scheme slows down PPP packet transmission, sometimes to the point where a PPP connection will fail to negotiate a connection due to timeouts. Three new configuration options, two for 8235 and one for the DIALs software,

have been created to ease this situation. The two options for the 8235 require a restart to take effect.

PPPRestartTimer: This parameter sets the amount of time PPP will wait for responses during negotiation. The default is 2 seconds. For X.25 networks (or any high-latency network that PPP must traverse), this parameter should be increased. Ideally, it should be slightly longer than the actual round-trip packet delay on the network. If it is too long, PPP negotiation may take a long time from an end-user perspective. IBM recommends a setting no higher than 5 seconds. To affect all serial ports, the parameter is entered in this manner:

```
[Serial*]
PPPRestartTimer=4
```

Individual serial ports can be configured by specifying the port number during configuration:

```
[Serial3]
PPPRestartTimer=4
```

Note: The PPPRestartTimer parameter requires the use of the `LongTimeouts` parameter for the dial-in client.

X.25 PAD: This optimization increases throughput, particularly during request-response style interactions (for example, NETX sessions). When turned on (default is off), the 8235 assumes that it is connected to an X.25 PAD configured to use CR as a packet terminator. In other words, the 8235 assumes that when the PAD receives a carriage return, it will immediately assemble the packet from all the data in its buffer and send it out. The 8235 inserts a CR at the end of each PPP packet, and ensures that CR never appears within a packet. Thus, the PAD will send out each PPP packet whenever it is complete, instead of waiting for the rest of its buffer to fill.

```
[Serial*]
X25PAD=1
```

Individual serial ports can be configured by specifying the port number during configuration:

```
[Serial3]
X25PAD=1
```

Note: This parameter is ignored if the line is configured for synch operation.

6.5.3 Manual Mode

Manual mode is supported by all the DIALs Clients (DOS, Windows, OS/2). It can be used for troubleshooting purposes or for limited out-band shell access if no terminal emulation package is available. The Connect application is started, but it is not used for automatic dialing. Instead, the user gets an interactive terminal window (as with the third-party security feature) and types in the modem commands manually. Once the modems connect, the user can either carry on manually by logging in to the command shell, or select the **Continue** function to start PPP negotiation and get a *normal* dial-in session on an 8235. Manual mode is invoked as follows:

- Type `connect /m` (for DOS).
- Press Alt+M when the Connect window is active (for Windows).
- Press Ctrl+M when the Connect window is active (for OS/2).

To terminate manual mode you have two options:

- Continue with the PPP negotiation and get a DIALs connection (F10 for DOS, select **Continue** for OS/2 and Windows).
- Cancel and break the modem connection (F9 for DOS, **Cancel** for OS/2 and Windows).

Chapter 7. Dial-In Application Environments

This chapter gives examples of the dial-in feature of the 8235, considering the different network applications over each operating system and protocol supported.

Figure 62 shows you the topology of the connection. The remote workstation is installed with the DIALs Client software and it remotely connects to the 8235 through a telephone line.

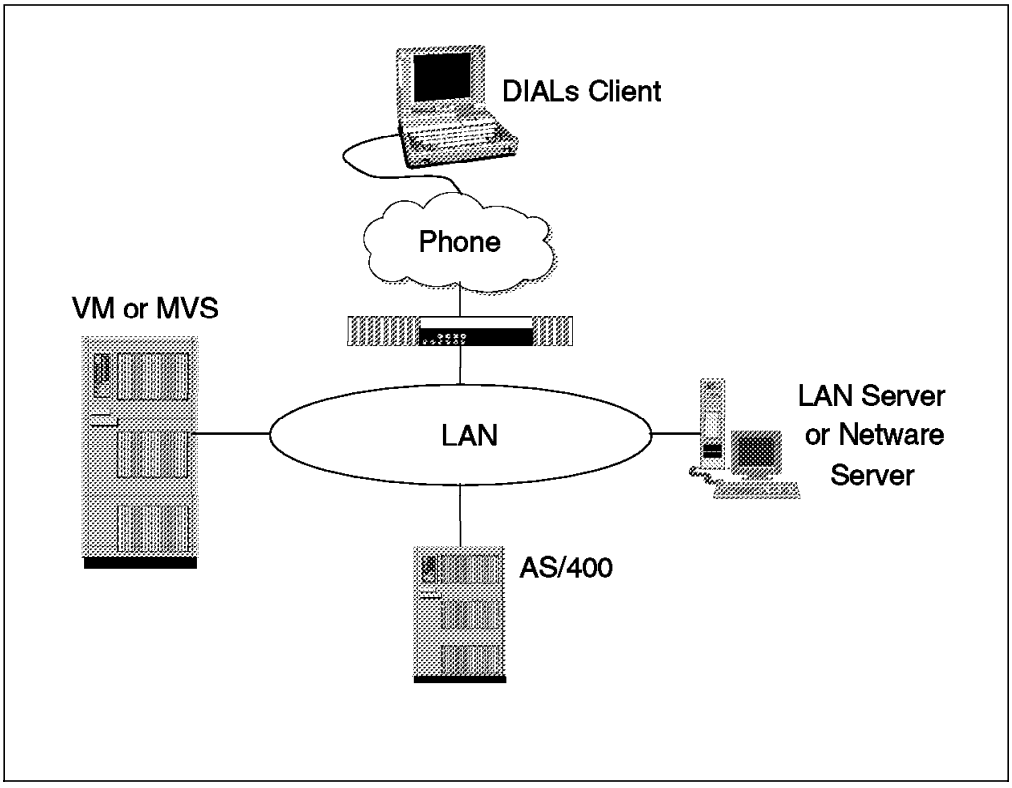


Figure 62. Dial-In Connection Topology

7.1 OS/2 Environment

All the procedures described in 6.1.3, “Installation of the OS/2 DIALs Client” on page 108 should have already been done before attempting to follow any of the examples in this chapter.

7.1.1 Communication Manager/2

We recommend that Communication Manager/2 runs at a modem speed of 9.6 Kbps or higher to avoid problems that might occur with logons or session establishment.

The parameter requirements are:

- Change the Send Window Count and Receive Window Count values for the Data Link Control (DLC) from 4 to 1.
- Change the I-frame size to 1500 or less.

- Set the required change parameters described in 6.1.3, “Installation of the OS/2 DIALs Client” on page 108.

The following control files is defined for this configuration:

```
SET AUTOSTART=TASKLIST,FOLDERS
         .
         .
         .
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
         .
         .
         .
RUN=C:\IBMCOM\PROTOCOL\NETBIND.EXE
RUN=C:\IBMCOM\LANMSGEX.EXE
DEVICE=C:\IBMCOM\PROTOCOL\NETBEUI.OS2
DEVICE=C:\IBMCOM\PROTOCOL\NETBIOS.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDLLDD.OS2
DEVICE=C:\IBMCOM\MACS\DIALNDIS.OS2
RUN=C:\IBMCOM\PROTOCOL\LANDLL.EXE
RUN=C:\IBMLAN\NETPROG\LSDAEMON.EXE

DEVICE=C:\CMLIB\ACSLANDD.SYS
DEVICE=C:\CMLIB\CMKFMDE.SYS
DEVICE=C:\OS2\LOG.SYS
RUN=C:\OS2\SYSTEM\LOGDAEM.EXE
RUN=C:\OS2\EPWROUT.EXE 1
RUN=C:\OS2\EPW.EXE
```

Figure 63. CONFIG.SYS Control File for Communication Manager/2

```
[PROT_MAN]

    DRIVERNAME = PROTMAN$

[IBMLXCFG]

    DIALNDIS_NIF = DIALNDIS.NIF
    LANDD_NIF = LANDD.NIF
    NETBEUI_NIF = NETBEUI.NIF

[LANDD_NIF]

    DRIVERNAME = LANDD$
    BINDINGS = DIALNDIS_NIF
    ETHERAND_TYPE = "I"
    SYSTEM_KEY = 0x0
    OPEN_OPTIONS = 0x2000
    TRACE = 0x0FFFF
    LINKS = 8
    MAX_SAPS = 3
    MAX_G_SAPS = 0
    USERS = 3
    TI_TICK_G1 = 255
    T1_TICK_G1 = 200
    T2_TICK_G1 = 3
    TI_TICK_G2 = 255
    T1_TICK_G2 = 250
    T2_TICK_G2 = 10
    IPACKETS = 250
    UIPACKETS = 100
    MAXTRANSMITS = 6
    MINTRANSMITS = 2
    TCBS = 64
    GDTS = 30
    ELEMENTS = 800


[NETBEUI_NIF]

    DRIVERNAME = NETBEUI$
    BINDINGS = DIALNDIS_NIF
    ETHERAND_TYPE = "I"
    USEADDRREV = "YES"
    OS2TRACEMASK = 0x0ffff
    SESSIONS = 40
    NCBS = 95
    NAMES = 21
    SELECTORS = 5
    USEMAXDATAGRAM = "NO"
    ADAPTRATE = 1000
    WINDOWERRORS = 0
    MAXDATARCV = 4168
```

Figure 64 (Part 1 of 2). PROTOCOL.INI Control File for Communication Manager/2

```
    TI = 30000
    T1 = 500
    T2 = 200
    MAXIN = 1
    MAXOUT = 1
    NETBIOSTIMEOUT = 500
    NETBIOSRETRIES = 8
    NAMECACHE = 0
    PIGGYBACKACKS = 1
    DATAGRAMPACKETS = 2
    PACKETS = 350
    LOOPPACKETS = 1
    PIPELINE = 5
    MAXTRANSMITS = 6
    MINTRANSMITS = 2
    DLCRETRIES = 5

[DIALNDIS_NIF]
    DRIVERNAME = SDIALIN$
```

Figure 64 (Part 2 of 2). PROTOCOL.INI Control File for Communication Manager/2

7.1.2 OS/2 LAN Services

We recommend that OS/2 LAN Services runs at a modem speed of 9.6 Kbps or higher to avoid problems that might occur with logons or large file transfers.

The parameter requirements are:

- Change the session timeout value from 45 to 300 in IBMLAN.INI.
- Change the workstation heuristics bit numbers 11,12,13 from 1,1,1 to 0,0,0 in IBMLAN.INI.
- Set the required change parameters required for NetBEUI defined in 6.1.3, “Installation of the OS/2 DIALs Client” on page 108.
- Set the same parameter requirements for NetBIOS on the LAN Server workstation.
- Change the server heuristics bit number 15 from 1 to 9 in IBMLAN.INI on the LAN Server workstation.

These are the control files defined for this configuration:

```
SET AUTOSTART=TASKLIST,FOLDERS
          .
          .
          .
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
          .
          .
          .
RUN=C:\IBMCOM\PROTOCOL\NETBIND.EXE
RUN=C:\IBMCOM\LANMSGEX.EXE
DEVICE=C:\IBMCOM\PROTOCOL\NETBEUI.OS2
DEVICE=C:\IBMLAN\NETPROG\RDRHELP.200
IFS=C:\IBMLAN\NETPROG\NETWKSTA.200 /I:C:\IBMLAN /N
DEVICE=C:\IBMCOM\PROTOCOL\NETBIOS.OS2

DEVICE=C:\IBMCOM\PROTOCOL\LANDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDLLDD.OS2
DEVICE=C:\IBMCOM\MACS\DIALNDIS.OS2
RUN=C:\IBMCOM\PROTOCOL\LANDLL.EXE
```

Figure 65. CONFIG.SYS Control File for OS/2 LAN Services

```
[PROT_MAN]

    DRIVERNAME = PROTMAN$

[IBMLXCFG]

    DIALNDIS_NIF = DIALNDIS.NIF
    LANDD_NIF = LANDD.NIF
    NETBEUI_NIF = NETBEUI.NIF

[LANDD_NIF]

    DRIVERNAME = LANDD$
    BINDINGS = DIALNDIS_NIF
    ETHERAND_TYPE = "I"
    SYSTEM_KEY = 0x0
    OPEN_OPTIONS = 0x2000
    TRACE = 0x0
    LINKS = 8
    MAX_SAPS = 3
    MAX_G_SAPS = 0
    USERS = 3
    TI_TICK_G1 = 255
    T1_TICK_G1 = 15
    T2_TICK_G1 = 3
    TI_TICK_G2 = 255
    T1_TICK_G2 = 25
    T2_TICK_G2 = 10
    IPACKETS = 250
    UIPACKETS = 100
    MAXTRANSMITS = 6
    MINTRANSMITS = 2
    TCBS = 64
    GDTS = 30
    ELEMENTS = 800

[NETBEUI_NIF]

    DRIVERNAME = NETBEUI$
    BINDINGS = DIALNDIS_NIF
    ETHERAND_TYPE = "I"
    USEADDRREV = "YES"
    OS2TRACEMASK = 0x0
    SESSIONS = 40
    NCBS = 95
    NAMES = 21
    SELECTORS = 5
    USEMAXDATAGRAM = "NO"
    ADAPTRATE = 0
    WINDOWERRORS = 0
    MAXDATARCV = 4168
```

Figure 66 (Part 1 of 2). PROTOCOL.INI Control File for OS/2 LAN Services

```
    TI = 60000
    T1 = 10000
    T2 = 2000
    MAXIN = 1
    MAXOUT = 1
    NETBIOSTIMEOUT = 1000
    NETBIOSRETRIES = 8
    NAMECACHE = 0
    PIGGYBACKACKS = 1
    DATAGRAMPACKETS = 2
    PACKETS = 350
    LOOPPACKETS = 1
    PIPELINE = 5
    MAXTRANSMITS = 4
    MINTRANSMITS = 2
    DLCRETRIES = 5

[DIALNDIS_NIF]

    DRIVERNAME = SDIALIN$
```

Figure 66 (Part 2 of 2). PROTOCOL.INI Control File for OS/2 LAN Services

```
; OS/2 LAN REQUESTER INITIALIZATION FILE
            .
            .
            .
  SESSTIMEOUT = 300
  SIZCHARBUF = 512
  SIZERROR = 1024
  SIZWORKBUF = 4096
; THE NEXT LINES HELP YOU TO LOCATE BITS IN THE WRKHEURISTICS ENTRY.
;                            1         2         3
;                  01234567890123456789012345678901234
  WRKHEURISTICS = 11111111213000111100010111201112211
            .
            .
            .
```

Figure 67. IBMLAN.INI Control File for OS/2 LAN Services

7.1.3 NetWare Client for OS/2

We recommend that the NetWare Client for OS/2 runs at a modem speed of 9.6 Kbps or higher to avoid problems that might occur, such as a locked up workstation while starting NetWare.

DIALs Client/2 supports the disconnect mode feature for the OS/2 NetWare Requester, which provides better handling for dial-in connections. It addresses two problems:

- When disconnecting and then reconnecting to a different 8235, the dial-in IPX network number changes, but since the new network number is not picked

up by the OS/2 NetWare Requester, it can no longer communicate with NetWare servers on the remote LAN.

- After disconnecting, the OS/2 NetWare Requester daemon, NWDAEMON, still thinks that there is a network connection; this can cause long delays, especially during OS/2 shutdown.

Connect/2 supports the disconnect mode feature, with the help of the dynamic link library file CN2NW.DLL. Upon connecting, Connect/2 resets NWDAEMON, allowing it to pick up the new IPX network number. Upon disconnecting, Connect/2 disconnects NWDAEMON, allowing OS/2 to shut down gracefully.

The disconnect mode feature is supported by a special patch level of OS/2 NetWare Requester Version 2.11, for which patch files were shipped with DIALs Client/2 Version 3.5. Since that time, Novell has provided a number of *fix packs* for NetWare Requester Version 2.11; for DIALs Client/2 the essential fixes were for Burst Mode Protocol support (improved reliability and performance). Novell cannot guarantee that any of these fix packs contains the disconnect mode feature, but has stated that the feature will be contained in its next release of OS/2 NetWare Requester (Version 2.12). If you have OS/2 NetWare Requester Version 2.11, but you do not have the patch level shipped with DIALs Client/2 Version 3.5, or if you do have the patch level just described but want the improved Burst Mode Protocol support, or if you do not have any patch level containing the disconnect mode feature, then please contact your IBM support representative, who can help you obtain a patch level that will contain both the disconnect mode feature and the Burst Mode Protocol support fixes.

To enable the disconnect mode feature in OS/2 NetWare Requester:

1. Add the following parameter to the NET.CFG file:

```
NETWARE REQUESTER
   DISCONNECT ON
```

2. In CONFIG.SYS, if you had removed the statement:

```
RUN=C:\NETWARE\NWDAEMON.EXE
```

   add it back in, after the line:

```
IFS=C:\NETWARE\NWIFS.SYS
```

   With the disconnect mode feature, you no longer need to detach NWDAEMON after connecting to an 8235. When NWDAEMON loads (at system startup) it is disconnected (as configured in step 1) until you use Connect/2 to connect to an 8235.

3. Shut down your workstation and reboot.

If you cannot use the disconnect mode feature, then you need to remove the following statement from the CONFIG.SYS file:

```
RUN=C:\NETWARE\NWDAEMON.EXE
```

This file now needs to be started manually after the dial-in connection has been made. To start NWDAEMON after you are connected, type `DETACH C:\NETWARE\NWDAEMON.EXE` from an OS/2 command prompt and then press Enter. You can create an icon in the NetWare folder that issues this command rather than entering the command every time.

Here are some additional procedures to increase performance:

- Remove the directories L:\OS2 and P:\OS2 from the PATH= statement in the CONFIG.SYS file.
- Make sure that you have a NET.CFG file that includes the statements:

```
LINK DRIVER odi2ndi

NETWARE REQUESTER
   PREFERRED SERVER (your server name here)
   REQUEST RETRIES 7
```

These are the control files defined for this configuration:

```
SET AUTOSTART=TASKLIST,FOLDERS
         .
         .
         .
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
         .
         .
         .
RUN=C:\IBMCOM\LANMSGEX.EXE

DEVICE=C:\IBMCOM\MACS\DIALNDIS.OS2

REM --- NETWARE REQUESTOR STATEMENTS BEGIN ---
SET NWLANGUAGE=ENGLISH
DEVICE=C:\NETWARE\LSL.SYS
RUN=C:\NETWARE\DDAEMON.EXE
DEVICE = C:\IBMCOM\PROTOCOL\ODI2NDI.OS2
REM -- ODI-DRIVER FILES BEGIN --
REM DEVICE=C:\NETWARE\TOKEN.SYS
DEVICE=C:\NETWARE\ROUTE.SYS
REM -- ODI-DRIVER FILES END --
DEVICE=C:\NETWARE\IPX.SYS
DEVICE=C:\NETWARE\SPX.SYS
REM RUN=C:\NETWARE\SPDAEMON.EXE
REM DEVICE=C:\NETWARE\NMPIPE.SYS
REM DEVICE=C:\NETWARE\NPSERVER.SYS
REM RUN=C:\NETWARE\NPDAEMON.EXE
DEVICE=C:\NETWARE\NWREQ.SYS
IFS=C:\NETWARE\NWIFS.IFS

rem RUN=C:\NETWARE\NWDAEMON.EXE

REM --- NetWare Requestor statements END ---
RUN=C:\IBMCOM\PROTOCOL\NETBIND.EXE
```

Figure 68. CONFIG.SYS Control File for NetWare Client for OS/2

```
[PROT_MAN]

   DRIVERNAME = PROTMAN$

[IBMLXCFG]

   DIALNDIS_NIF = DIALNDIS.NIF
   ODI2NDI_NIF = ODI2NDI.NIF

[ODI2NDI_NIF]

   DRIVERNAME = ODI2NDI$
   BINDINGS = DIALNDIS_NIF
   NETADDRESS = "T400000123456"
   TOKEN-RING = "NO"
   TOKEN-RING_SNAP = "NO"
   ETHERNET_802.3 = "YES"
   ETHERNET_802.2 = "NO"
   ETHERNET_II = "YES"
   ETHERNET_SNAP = "NO"
   TRACE = 0X0

[DIALNDIS_NIF]

   DRIVERNAME = SDIALIN$
```

Figure 69. PROTOCOL.INI Control File for NetWare Client for OS/2

```
LINK DRIVER  ODI2NDI

NETWARE REQUESTER
   PREFERRED SERVER ITSOSRV
   REQUEST RETRIES 7
```

Figure 70. NET.CFG Control File for NetWare Client for OS/2

7.1.4 TCP/IP for OS/2

These are the control files defined for TCP/IP for OS/2:

```
SET AUTOSTART=TASKLIST,FOLDERS
         .
         .
         .
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
         .
         .
         .
RUN=C:\IBMCOM\LANMSGEX.EXE

SET ETC=C:\TCPIP\ETC
SET TMP=C:\TCPIP\TMP
SET READIBM=C:\TCPIP\DOC
SET HOSTNAME=TEST
RUN=C:\TCPIP\BIN\CNTRL.EXE
IFS=C:\TCPIP\BIN\NFS200.IFS

DEVICE=C:\IBMCOM\PROTOCOL\INET.SYS
DEVICE=C:\IBMCOM\PROTOCOL\IFNDIS.SYS
RUN=C:\IBMCOM\PROTOCOL\NETBIND.EXE
DEVICE=C:\IBMCOM\MACS\DIALNDIS.OS2
SET TZ=EST5EDT
SET NFS.PERMISSION.BITS=700
SET NFS.PERMISSION.DBITS=700
```

Figure 71. CONFIG.SYS Control File for TCP/IP for OS/2

```
[PROT_MAN]

   DRIVERNAME = PROTMAN$

[IBMLXCFG]

   DIALNDIS_NIF = DIALNDIS.NIF
   TCPIP_NIF = TCPIP.NIF

[TCPIP_NIF]

   DRIVERNAME = TCPIP$
   BINDINGS = DIALNDIS_NIF

[DIALNDIS_NIF]

   DRIVERNAME = SDIALIN$
```

Figure 72. PROTOCOL.INI Control File for TCP/IP for OS/2

7.1.5 Multiprotocol Environment

This example shows the implementation of a multiprotocol environment on OS/2 with the complete control files.

The software packages used in these tests are:

- OS/2 Warp Connect V3.0
- Communication Manager/2 V1.11
- OS/2 LAN Services V4.0
- NetWare Requester for OS/2 V2.0
- DIALs Client/2 V4.0.2

The control files defined for this environment are:

```
IFS=D:\OS2\HPFS.IFS /CACHE:2048 /CRECL:4 /AUTOCHECK:D
PROTSHELL=D:\OS2\PMSHELL.EXE
SET USER_INI=D:\OS2\OS2.INI
SET SYSTEM_INI=D:\OS2\OS2SYS.INI
SET OS2_SHELL=D:\OS2\CMD.EXE
SET AUTOSTART=PROGRAMS,TASKLIST,FOLDERS,CONNECTIONS,LAUNCHPAD
SET RUNWORKPLACE=D:\OS2\PMSHELL.EXE
SET COMSPEC=D:\OS2\CMD.EXE
LIBPATH=D:\MPTN\DLL;D:\IBMCOM\DLL;.;D:\USERDLLS;
D:\IBMLAN\NETLIB;D:\MUGLIB\DLL;D:\OS2\DLL;D:\CMLIB\DLL;
D:\OS2\MDOS;D:\;D:\OS2\APPS\DLL;D:\MMOS2\DLL;D:\GRPWARE;
D:\NSC\DLL;D:\TCPIP\DLL;D:\TCPIP\UMAIL;D:\NETWARE;
SET PATH=D:\MPTN\BIN;D:\IBMCOM;D:\CMDS;D:\OS2UTILS;
D:\IBMLAN\NETPROG;D:\MUGLIB;D:\OS2;D:\CMLIB;D:\OS2\SYSTEM;
D:\OS2\MDOS\WINOS2;D:\OS2\INSTALL;D:\;D:\OS2\MDOS;
D:\OS2\APPS;D:\MMOS2;D:\NSC;D:\TCPIP\BIN;D:\TCPIP\UMAIL;
L:\OS2;P:\OS2;D:\NETWARE;
SET DPATH=D:\IBMCOM;D:\OS2UTILS;D:\IBMLAN\NETPROG;D:\IBMLAN;
D:\MUGLIB;D:\OS2;D:\CMLIB;D:\OS2\SYSTEM;D:\OS2\MDOS\WINOS2;
D:\OS2\INSTALL;D:\;D:\OS2\BITMAP;D:\OS2\MDOS;D:\OS2\APPS;
D:\MMOS2;D:\MMOS2\INSTALL;D:\GRPWARE;D:\NSC;D:\NETWARE;
BASEDEV=DETNE2.SYS
SET PROMPT=$I[$P]
SET HELP=D:\OS2\HELP;D:\HELPLIB;D:\OS2\HELP\TUTORIAL;
D:\MMOS2\HELP;d:\tcpip\help;D:\TCPIP\UMAIL;D:\CMLIB;
SET GLOSSARY=D:\OS2\HELP\GLOSS;
SET IPF_KEYS=SBCS
PRIORITY_DISK_IO=YES
FILES=20
BASEDEV=IBMKBD.SYS
DEVICE=D:\IBMCOM\PROTOCOL\LANPDD.OS2
DEVICE=D:\IBMCOM\PROTOCOL\LANVDD.OS2
DEVICE=D:\IBMCOM\LANMSGDD.OS2 /I:D:\IBMCOM
DEVICE=D:\IBMCOM\PROTMAN.OS2 /I:D:\IBMCOM
DEVICE=D:\OS2\BOOT\TESTCFG.SYS
DEVICE=D:\OS2\BOOT\DOS.SYS
DEVICE=D:\OS2\BOOT\PMDD.SYS
BUFFERS=90
IOPL=YES
DISKCACHE=D,LW
MAXWAIT=3
MEMMAN=SWAP,PROTECT
SWAPPATH=D:\OS2\SYSTEM 2048 2048
BREAK=OFF
THREADS=512
PRINTMONBUFSIZE=134,134,134
COUNTRY=001,D:\OS2\SYSTEM\COUNTRY.SYS
SET KEYS=ON
SET BOOKSHELF=D:\IBMLAN\NETPROG;D:\OS2\BOOK;D:\MMOS2;
d:\tcpip\doc;D:\CMLIB\BOOK;d:\ebookie;
SET SOMIR=D:\OS2\ETC\SOM.IR;D:\OS2\ETC\WPSH.IR;
D:\OS2\ETC\WPDSERV.IR
SET SOMDDIR=D:\OS2\ETC\DSOM
REM SET DELDIR=C:\DELETE,512;D:\DELETE,512;E:\DELETE,512;
```

Figure 73 (Part 1 of 3). CONFIG.SYS Control File for Multiprotocol Environments

```
BASEDEV=PRINT01.SYS
BASEDEV=IBM1FLPY.ADD
BASEDEV=IBM2FLPY.ADD
BASEDEV=IBM1S506.ADD
BASEDEV=XDFLOPPY.FLT
BASEDEV=OS2DASD.DMD
rem SET EPMPATH=D:\OS2\APPS;
SET EPMPATH=D:\ebookie;
PROTECTONLY=NO
SHELL=D:\OS2\MDOS\COMMAND.COM D:\OS2\MDOS
FCBS=16,8
RMSIZE=640
DEVICE=D:\OS2\MDOS\VEMM.SYS
DOS=LOW,NOUMB
DEVICE=D:\OS2\MDOS\VXMS.SYS /UMB
DEVICE=D:\OS2\MDOS\VDPMI.SYS
DEVICE=D:\OS2\MDOS\VDPX.SYS
DEVICE=D:\OS2\MDOS\VWIN.SYS
DEVICE=D:\OS2\MDOS\VW32S.SYS
DEVICE=D:\OS2\BOOT\OS2CDROM.DMD /Q
IFS=D:\OS2\BOOT\CDFS.IFS /Q
DEVICE=D:\OS2\MDOS\VCDROM.SYS
BASEDEV=SBCD2.ADD
DEVICE=D:\OS2\MDOS\VMOUSE.SYS
DEVICE=D:\OS2\BOOT\POINTDD.SYS
DEVICE=D:\OS2\BOOT\MOUSE.SYS
DEVICE=D:\OS2\BOOT\COM.SYS
DEVICE=D:\OS2\MDOS\VCOM.SYS
CODEPAGE=437,850
DEVINFO=KBD,US,D:\OS2\KEYBOARD.DCP
DEVINFO=SCR,BGA,D:\OS2\BOOT\VIOTBL.DCP
SET VIDEO_DEVICES=VIO_SVGA
DEVICE=D:\OS2\ATIO.SYS
SET MMBASE=D:\MMOS2;
SET DSPPATH=D:\MMOS2\DSP;
SET NCDEBUG=4000
DEVICE=D:\MMOS2\SSMDD.SYS
DEVICE=D:\MMOS2\ROSTUB.SYS
CALL=D:\IBMCOM\PROTOCOL\NETBIND.EXE
RUN=D:\IBMCOM\LANMSGEX.EXE
SET ETC=D:\MPTN\ETC
DEVICE=D:\MPTN\PROTOCOL\SOCKETS.SYS
DEVICE=D:\MPTN\PROTOCOL\AFOS2.SYS
DEVICE=D:\MPTN\PROTOCOL\AFINET.SYS
DEVICE=D:\MPTN\PROTOCOL\IFNDIS.SYS
RUN=D:\MPTN\BIN\CNTRL.EXE
CALL=D:\OS2\CMD.EXE /Q /C D:\MPTN\BIN\MPTSTART.CMD
DEVICE=D:\IBMCOM\PROTOCOL\NETBEUI.OS2
DEVICE=D:\IBMLAN\NETPROG\RDRHELP.200
```

Figure 73 (Part 2 of 3). CONFIG.SYS Control File for Multiprotocol Environments

```
REM --- NetWare Requester statements BEGIN ---
DEVICE=D:\NETWARE\LSL.SYS
RUN=D:\NETWARE\DDAEMON.EXE
DEVICE=D:\IBMCOM\PROTOCOL\ODI2NDI.OS2
REM DEVICE=D:\NETWARE\TOKEN.SYS
DEVICE=D:\NETWARE\ROUTE.SYS
DEVICE=D:\NETWARE\IPX.SYS
DEVICE=D:\NETWARE\SPX.SYS
RUN=D:\NETWARE\SPDAEMON.EXE
rem DEVICE=D:\NETWARE\NMPIPE.SYS
rem DEVICE=D:\NETWARE\NPSERVER.SYS
rem RUN=D:\NETWARE\NPDAEMON.EXE NP_COMPUTERNAME
DEVICE=D:\NETWARE\NWREQ.SYS
IFS=D:\NETWARE\NWIFS.IFS
RUN=D:\NETWARE\NWDAEMON.EXE
DEVICE=D:\NETWARE\NETBIOS.SYS
RUN=D:\NETWARE\NBDAEMON.EXE
DEVICE=D:\NETWARE\VIPX.SYS
DEVICE=D:\NETWARE\VSHELL.SYS
REM --- NetWare Requester statements END ---
IFS=D:\IBMLAN\NETPROG\NETWKSTA.200 /I:D:\IBMLAN /N
DEVICE=D:\IBMCOM\PROTOCOL\NETBIOS.OS2
RUN=D:\IBMLAN\NETPROG\LSDAEMON.EXE
RUN=D:\OS2\SYSTEM\LOGDAEM.EXE
RUN=D:\OS2\EPW.EXE
RUN=D:\OS2\EPWROUT.EXE 1
DEVICE=D:\OS2\LOG.SYS
SET NWDBPATH=D:\IBMLAN\NETPROG
SET DLSINI=D:\IBMLAN\NETPROG\NETGUI.INI
SET INIT_FILE_NAMES=NETGUI
SET INIT_FILE_RANGES=200
SET WPS_COMMUNICATION=YES
SET LOCPATH=D:\IBMLAN\XPG4\LOCALE
SET LANG=ENUS437
SET TMP=d:\tcpip\tmp
DEVICE=d:\tcpip\bin\vdostcp.vdd
DEVICE=d:\tcpip\bin\vdostcp.sys
RUN=d:\tcpip\bin\VDOSCTL.EXE

DEVICE=D:\CMLIB\ACSLANDD.SYS
DEVICE=D:\CMLIB\CMKFMDE.SYS
SET CMPATH=D:\CMLIB
DEVICE=D:\OS2\EPWDD.SYS
RUN=D:\OS2\EPWDDR3.EXE
DEVICE=D:\IBMCOM\PROTOCOL\LANDD.OS2
DEVICE=D:\IBMCOM\PROTOCOL\LANDLLDD.OS2
RUN=D:\IBMCOM\PROTOCOL\LANDLL.EXE
DEVINFO=SCR,BGA,D:\OS2\VIOTBL.DCP
SET VIO_SVGA=DEVICE(BVHVGA,BVHSVGA)
DEVICE=D:\OS2\MDOS\VSVGA.SYS
DEVICE=D:\OS2\MDOS\VAD32.SYS
SET HOSTNAME=WTR05112
SET TZ=EST5EDT
DEVICE=D:\IBMCOM\MACS\DIALNDIS.OS2
```

Figure 73 (Part 3 of 3). CONFIG.SYS Control File for Multiprotocol Environments

```
[PROT_MAN]

   DRIVERNAME = PROTMAN$

[IBMLXCFG]

   landd_nif = landd.nif
   netbeui_nif = netbeui.nif
   odi2ndi_nif = odi2ndi.nif
   tcpip_nif = tcpip.nif
   DIALNDIS_nif = DIALNDIS.nif

[NETBIOS]

   DriverName = netbios$
   ADAPTER0 = netbeui$,0

[landd_nif]

   DriverName = LANDD$
   BINDINGS = DIALNDIS_nif
   ETHERAND_TYPE = "I"
   SYSTEM_KEY = 0x0
   OPEN_OPTIONS = 0x2000
   TRACE = 0x0
   LINKS = 16
   MAX_SAPS = 5
   MAX_G_SAPS = 0
   USERS = 6
   TI_TICK_G1 = 255
   T1_TICK_G1 = 200
   T2_TICK_G1 = 3
   TI_TICK_G2 = 255
   T1_TICK_G2 = 250
   T2_TICK_G2 = 10
   IPACKETS = 250
   UIPACKETS = 100
   MAXTRANSMITS = 6
   MINTRANSMITS = 2
   TCBS = 64
   GDTS = 30
   ELEMENTS = 800

[netbeui_nif]

   DriverName = netbeui$
   BINDINGS = DIALNDIS_nif
   ETHERAND_TYPE = "I"
   USEADDRREV = "YES"
   OS2TRACEMASK = 0x0
   SESSIONS = 64
   NCBS = 128
   NAMES = 32
   SELECTORS = 15
   USEMAXDATAGRAM = "NO"
```

Figure 74 (Part 1 of 2). PROTOCOL.INI Control File for Multiprotocol Environments

```
   ADAPTRATE = 0
   WINDOWERRORS = 0
   MAXDATARCV = 16384
   TI = 60000
   T1 = 10000
   T2 = 2000
   MAXIN = 1
   MAXOUT = 1
   NETBIOSTIMEOUT = 2000
   NETBIOSRETRIES = 3
   NAMECACHE = 1000
   RNDOPTION = 1
   PIGGYBACKACKS = 1
   DATAGRAMPACKETS = 10
   PACKETS = 350
   LOOPPACKETS = 8
   PIPELINE = 5
   MAXTRANSMITS = 6
   MINTRANSMITS = 2
   DLCRETRIES = 10
   FCPRIORITY = 5
   NETFLAGS = 0x0

[odi2ndi_nif]

   DriverName = odi2ndi$
   BINDINGS = DIALNDIS_nif
   NETADDRESS = "T400082355112"
   TOKEN-RING = "NO"
   TOKEN-RING_SNAP = "NO"
   ETHERNET_802.3 = "YES"
   ETHERNET_802.2 = "NO"
   ETHERNET_II = "YES"
   ETHERNET_SNAP = "NO"
   TRACE = 0x0

[tcpip_nif]

   DriverName = TCPIP$
   BINDINGS = DIALNDIS_nif

[DIALNDIS_nif]

   DRIVERNAME = SDIALIN$
```

Figure 74 (Part 2 of 2). PROTOCOL.INI Control File for Multiprotocol Environments

```
; OS/2 LAN Requester initialization file

[networks]

  net1 = NETBEUI$,0,LM10,34,70,14
; This information is read by the redirector
at device initialization time.

[requester]

  charcount = 16
  chartime = 250
  charwait = 3600
  keepconn = 600
  keepsearch = 600
  maxcmds = 16
  maxerrorlog = 100
  maxthreads = 10
  maxwrkcache = 64
  numalerts = 12
  numcharbuf = 10
  numservices = 7
  numworkbuf = 15
  numdgrambuf = 14
  othdomains =
  printbuftime = 90
  sesstimeout = 45
  sizcharbuf = 512
  sizerror = 1024
  sizworkbuf = 4096
  useallmem = No
;The next lines help you to locate bits in the wrkheuristics
;entry.
;                            1         2         3         4
;                  01234567890123456789012345678901234567890
  wrkheuristics = 11111111213111111100010111201112210012111
  wrkservices = MESSENGER
  wrknets = NET1
  Computername = WTR05112
  Domain = WTRDM

[messenger]

  logfile = messages.log
  sizmessbuf = 4096

[replicator]

  replicate = IMPORT
  importpath = D:\ibmlan\repl\import
  tryuser = yes
  password =
```

Figure 75 (Part 1 of 2). IBMLAN.INI Control File for Multiprotocol Environments

```
[Peer]


[Server]


[services]

  messenger = services\msrvinit.exe
  replicator = services\replicat.exe
  requester = services\wksta.exe
```

Figure 75 (Part 2 of 2). IBMLAN.INI Control File for Multiprotocol Environments

7.2 DOS/Windows Environment

The software packages used in these tests are:

- IBM DOS V7.0
- Windows V3.1
- DIALs Client for Windows V4.0
- NetWare Client V1.21
- NetWare Server V4.0
- TCP/IP for DOS from IBM V2.1.1 with CSD 2.1.1.4
- LAN Support Program V1.38
- Personal Communication V4.1
- DOS LAN Services V4.0
- OS/2 LAN Server V4.0
- Client Access/400 V3.1.1

In the DOS/Windows environment, it is always important to consider the amount of memory available for the application. If you face a memory shortage problem, try to load all the devices in the high memory block, making available the lower 640 KB as much as possible.

7.2.1 NetWare Client

The considerations for the 8235 Management Facility are:

- General: Protocol = IPX
- General: Functions = Dial-In

These are the control files defined for this configuration:

```
FILES=40
BUFFERS=10
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
STACKS=9,256
LASTDRIVE=Z
```

Figure 76. CONFIG.SYS Control File in a NetWare Client Environment

```
SET DIALS=C:\DIALS
@CALL C:\NWCLIENT\STARTNET
C:\WINDOWS\SMARTDRV.EXE
@ECHO OFF
PATH C:\DIALS;C:\WINDOWS;C:\DOS;%PATH%
PATH C:\NWCLIENT\;%PATH%
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
```

Figure 77. AUTOEXEC.BAT Control File in a NetWare Client Environment

```
SET NWLANGUAGE=ENGLISH
C:\NWCLIENT\LSL.COM
@call C:\DIALS\DIALS.BAT
REM C:\NWCLIENT\NTR2000.COM
C:\NWCLIENT\IPXODI.COM
C:\NWCLIENT\ROUTE.COM
C:\NWCLIENT\VLM.EXE
```

Figure 78. STARTNET.BAT Control File in a NetWare Client Environment

```
Link Driver DIALODI

Link Driver NTR2000
        PORT A20
        FRAME TOKEN-RING MSB

NetWare DOS Requester
        FIRST NETWORK DRIVE = F
        NETWARE PROTOCOL = NDS BIND
```

Figure 79. NET.CFG Control File in a NetWare Client Environment

```
@echo off
echo Dial-in Networking Options:
echo.
:chooselr
C:\DIALS\CHOOSELR
echo.
if errorlevel=2 goto local$node

rem DIALs driver goes here
:remote$node
C:\DIALS\DIALODI.EXE
goto node$done

rem LAN NIC driver goes here
:local$node
C:\NWCLIENT\NTR2000.COM
goto node$done

:node$done
```

Figure 80. DIALS.BAT Control File in a NetWare Client Environment

The INSTALL program on the NetWare Client V1.21 assumes that you are on Drive A or B, depending on which diskette drive you are running from. An error will occur if you are not in the diskette drive when running the INSTALL program.

7.2.2 TCP/IP for DOS

The considerations for the 8235 Management Facility are:

- General: Protocol = IP
- General: Functions = Dial-In
- IP General: define IP address of device
- IP General: define IP network mask
- IP General: define IP broadcast address
- IP General: define IP address of default router
- IP General: define IP address of name server
- IP Addresses: define IP address assignment scheme

These are the control files defined for this configuration:

```
FILES=50
BUFFERS=10
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
STACKS=9,256
DEVICE = C:\DOS\ANSI.SYS
DEVICE = C:\TCPDOS\BIN\PROTMAN.DOS /I:C:\TCPDOS\ETC
DEVICE = C:\TCPDOS\BIN\DOSTCP.SYS
rem DEVICE = C:\TCPDOS\BIN\IBMTOK.DOS
DEVICE = C:\DIALS\DIALNDIS.EXE
```

Figure 81. CONFIG.SYS Control File in a TCP/IP for DOS Environment

```
SET DIALS=C:\DIALS
C:\TCPDOS\BIN\NETBIND
SET ETC=C:\TCPDOS\ETC
C:\WINDOWS\SMARTDRV.EXE
@ECHO OFF
path c:\dials;c:\windows;c:\dos;%path%;c:\tcpdos\bin;
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
SET WIN$=C:\WINDOWS
CALL TCPSTART
```

Figure 82. AUTOEXEC.BAT Control File in a TCP/IP for DOS Environment

```
[PROTMAN]
DriverName=PROTMAN$

[TCPIP_V21]
Drivername=DOSNDIS$
Bindings=DIALNDIS,,,

[IBMTOK]
; IBM Token Ring
; IBMTOK.DOS
    DriverName = IBMTOK$

[DIALNDIS]
DriverName = SDIALIN$
```

Figure 83. PROTOCOL.INI Control File in a TCP/IP for DOS Environment

TCP/IP for DOS V2.1.1 from IBM supports the Windows 3.1 operating system. It is important to install the TCP/IP for DOS CSD.

7.2.3 Personal Communication

The considerations for the 8235 Management Facility are:

- General: Protocol = NetBEUI
- General: Functions = Dial-In
- Bridging: define attached ring number if token-ring
- Bridging: define internal ring number if token-ring

The attached ring number specifies the number of the token-ring to which the 8235 is attached and the internal ring number specifies a virtual token-ring number for the 8235 when using the source-routing bridge.

Note: You need to install 8235 DIALs Client V4.0.3 or higher to have Personal Communication working. With 8235 DIALs Client V4.0.2 you may have your system hang depending on the hardware you are using.

These are the control files defined for this configuration:

```
FILES=30
BUFFERS=10
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
STACKS=9,256
LASTDRIVE=Z
DEVICE=C:\LSP\PROTMAN.DOS /I:\LSP
DEVICE=C:\DIALS\DIALNDIS.EXE
DEVICE=C:\LSP\DXMAOMOD.SYS 001
DEVICE=C:\LSP\DXMEOMOD.SYS
DEVICE=C:\LSP\DXMTOMOD.SYS ES=1 EST=1 O=N CF=Y T1=10 T2=10 TI=10
DEVICE=C:\NET\DLSHELP.SYS
```

Figure 84. CONFIG.SYS Control File in a Personal Communication Environment

```
SET DIALS=C:\DIALS
C:\LSP\NETBIND
C:\DOS\SMARTDRV.EXE
@ECHO OFF
PATH C:\PCOMWIN;C:\DOS;C:\DIALS;C:\WINDOWS;%PATH%;
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
SET WIN$=C:\WINDOWS
```

a Personal Communication Environment

Figure 85. AUTOEXEC.BAT Control File in

```
[protman]
DriverName=PROTMAN$

[DXMAIDXCFG]
DIALNDIS_NIF=DIALNDIS.NIF

[DXMEO_MOD]
DriverName=DXMEO$
Bindings=DIALNDIS_NIF

[DIALNDIS_NIF]
DriverName=SDIALIN$
```

a Personal Communication Environment

Figure 86. PROTOCOL.INI Control File in

7.2.4 LAN Services for DOS/Windows

The considerations for the 8235 Management Facility are:

- General: Protocol = NetBEUI
- General: Functions = Dial-In
- Bridging: define attached ring number if token-ring
- Bridging: define internal ring number if token-ring

The attached ring number specifies the number of the token-ring to which the 8235 is attached and the internal ring number specifies a virtual token-ring number for the 8235 when using the source-routing bridge.

These are the control files defined for this configuration:

```
FILES=30
BUFFERS=10
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
STACKS=9,256
LASTDRIVE=Z
DEVICE=C:\LSP\PROTMAN.DOS /I:\LSP
DEVICE=C:\DIALS\DIALNDIS.EXE
DEVICE=C:\LSP\DXMAOMOD.SYS 001
DEVICE=C:\LSP\DXMEOMOD.SYS
DEVICE=C:\LSP\DXMTOMOD.SYS ES=1 EST=1 O=N CF=Y T1=10 T2=10 TI=10
DEVICE=C:\NET\DLSHELP.SYS
```

Figure 87. CONFIG.SYS Control File in a DOS LAN Services Environment

```
SET DIALS=C:\DIALS
C:\LSP\NETBIND
C:\DOS\SMARTDRV.EXE
@ECHO OFF
PATH C:\DOS;C:\DIALS;C:\NET;C:\NWDBPATH;C:\WINDOWS;%PATH%;
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
SET WIN$=C:\WINDOWS
```

Figure 88. AUTOEXEC.BAT Control File in a DOS LAN Services Environment

```
[protman]
DriverName=PROTMAN$

[DXMAIDXCFG]
DIALNDIS_NIF=DIALNDIS.NIF

[DXMEO_MOD]
DriverName=DXMEO$
Bindings=DIALNDIS_NIF

[DIALNDIS_NIF]
DriverName=SDIALIN$
```

Figure 89. PROTOCOL.INI Control File in a DOS LAN Services Environment

7.2.5 Client Access/400

The considerations for the 8235 Management Facility are:

- General: Protocol = NetBEUI
- General: Functions = Dial-In
- Bridging: define attached ring number if token-ring
- Bridging: define internal ring number if token-ring

The attached ring number specifies the number of the token-ring to which the 8235 is attached and the internal ring number specifies a virtual token-ring number for the 8235 when using the source routing bridge.

Note: As noted in 7.2.3, “Personal Communication” on page 169, the Personal Communication 5250 module of this solution will only work with 8235 DIALs Client for Windows V4.0.3 or higher.

These are the control files defined for this configuration:

```
FILES=30
BUFFERS=10
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
STACKS=9,256
LASTDRIVE=Z
DEVICE=C:\LSP\PROTMAN.DOS /I:\LSP
DEVICE=C:\DIALS\DIALNDIS.EXE
DEVICE=C:\LSP\DXMA0MOD.SYS 001
DEVICE=C:\LSP\DXME0MOD.SYS
DEVICE=C:\LSP\DXMT0MOD.SYS ES=1 EST=1 O=N CF=Y T1=10 T2=10 TI=10
DEVICE=C:\NET\DLSHELP.SYS
```

Figure 90. CONFIG.SYS Control File in a Client Access/400 Environment

```
SET DIALS=C:\DIALS
C:\LSP\NETBIND
C:\DOS\SMARTDRV.EXE
@ECHO OFF
PATH C:\CAWIN;C:\DOS;C:\DIALS;C:\WINDOWS;%PATH%;
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
SET WIN$=C:\WINDOWS
```

Figure 91. AUTOEXEC.BAT Control File in a Client Access/400 Environment

```
[protman]
DriverName=PROTMAN$

[DXMAIDXCFG]
DIALNDIS_NIF=DIALNDIS.NIF

[DXME0_MOD]
DriverName=DXME0$
Bindings=DIALNDIS_NIF

[DIALNDIS_NIF]
DriverName=SDIALIN$
```

Figure 92. PROTOCOL.INI Control File in a Client Access/400 Environment

7.2.6 IBM LAN Client

At the time this redbook was written, there was no support for the IBM LAN Client V2.0 in the DIALs Client environment although development is being done to support it in a future release.

7.2.7 Dual Environment

When a notebook PC is used as the client workstation, it is usually used in two different situations:

- Remote connection through the 8235
- Local connection through the LAN

This scenario implements the need for having both situations configured in the notebook PC. The type of connection will then be selected at boot time using the menu function in the CONFIG.SYS control file.

In this scenario, the application that will be installed is the DOS LAN Services. The same procedure can be used with any other application.

The considerations for the 8235 Management Facility are:

- General: Protocol = NetBEUI
- General: Functions = Dial-In
- Bridging: define attached ring number if token-ring
- Bridging: define internal ring number if token-ring

The attached ring number specifies the number of the token-ring to which the 8235 is attached and the internal ring number specifies a virtual token-ring number for the 8235 when using the source-routing bridge.

These are the control files defined for this configuration:

```
[Menu]
menuitem=ndisloc, PC connected locally through the token-ring LAN
menuitem=ndisrem, PC connected remotely through the 8235
[Common]
FILES=30
BUFFERS=10
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
STACKS=9,256
LASTDRIVE=Z
[ndisloc]
DEVICE=C:\NET\DXMAOMOD.SYS 001
DEVICE=C:\NET\DXMCOMOD.SYS
DEVICE=C:\NET\DXMTOMOD.SYS s=20 c=20
DEVICE=C:\NET\DLSHELP.SYS
[ndisrem]
DEVICEhigh=C:\LSP\PROTMAN.DOS /I:\LSP
DEVICEhigh=C:\DIALS\DIALNDIS.EXE
DEVICEhigh=C:\LSP\DXMAOMOD.SYS 001
DEVICEhigh=C:\LSP\DXMEOMOD.SYS
DEVICEhigh=C:\LSP\DXMTOMOD.SYS ES=1 EST=1 O=N CF=Y T1=10 T2=10 TI=10
DEVICEhigh=C:\NET\DLSHELP.SYS
```

Figure 93. CONFIG.SYS Control File in a Dual Environment

```
SET DIALS=C:\DIALS
if "%config%"=="ndisrem" C:\LSP\NETBIND
C:\DOS\SMARTDRV.EXE
@ECHO OFF
PATH C:\DOS;C:\DIALS;C:\NET;C:\NWDBPATH;C:\WINDOWS;%PATH%;
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
SET WIN$=C:\WINDOWS
```

Figure 94. AUTOEXEC.BAT Control File in a Dual Environment

```
[protman]
DriverName=PROTMAN$

[DXMAIDXCFG]
DIALNDIS_NIF=DIALNDIS.NIF

[DXMEO_MOD]
DriverName=DXMEO$
Bindings=DIALNDIS_NIF

[TCPIP_V21]
DriverName=DOSNDIS$
Bindings=DIALNDIS_NIF

[DIALNDIS_NIF]
DriverName=SDIALIN$
```

Figure 95. PROTOCOL.INI Control File in a Dual Environment

7.2.8 Multiprotocol Environment

Chapter 2, “8235-I40 Description” on page 7 discusses both environments, the ODI and NDIS interface to the communication driver. When dealing with a multiprotocol environment, it is necessary to decide which interface will be used as a common base for the upper-layer software.

Figure 96 on page 175 shows a multiprotocol implementation using NDIS as the common base. The ODI2NDI software implements the conversion between both interfaces so that Novell′s software like the NetWare Client or LAN Workplace can still run over an ODI interface. The ODI2NDI software comes with the DIALs Client package.

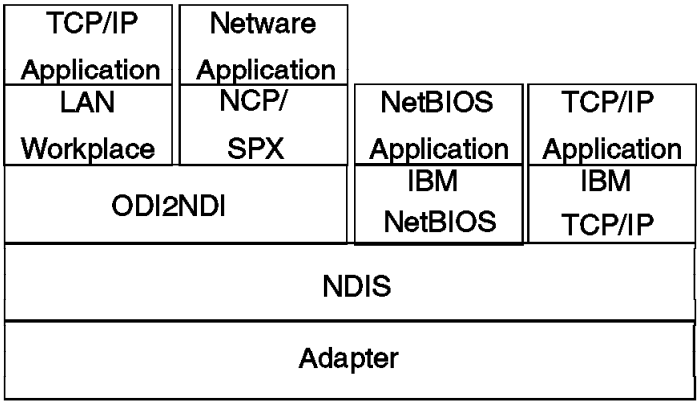


Figure 96. NDIS/ODI Multiprotocol Implementation

7.2.8.1 Mixed ODI/NDIS Multiprotocol Environment

This session shows an example of a mixed ODI/NDIS environment. The software tested here are:

- NetWare Client V1.21
- TCP/IP for DOS V2.1.1.4

These are the control files defined for this configuration:

```
FILES=50
BUFFERS=10
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
STACKS=9,256
DEVICE=C:\DOS\ANSI.SYS
DEVICE=C:\LSP\PROTMAN.DOS /I:C:\LSP
DEVICE=C:\DIALS\DIALNDIS.EXE
DEVICE=C:\LSP\DXMAOMOD.SYS 001
DEVICE=C:\LSP\DXMEOMOD.SYS
DEVICE=C:\LSP\DXMTOMOD.SYS ES=1 EST=1 O=N CF=Y T1=10 T2=10 TI=10
DEVICE=C:\TCPDOS\BIN\DOSTCP.SYS
rem DEVICE=C:\TCPDOS\BIN\IBMTOK.DOS
LASTDRIVE=Z
```

ODI/NDIS Multiprotocol Environment

Figure 97. CONFIG.SYS Control File in a Mixed

```
SET DIALS=C:\DIALS
SET ETC=C:\TCPDOS\ETC
C:\WINDOWS\SMARTDRV.EXE
@ECHO OFF
path c:\dials;c:\windows;c:\dos;%path%;
c:\tcpdos\bin;c:\nwclient;c:\ibm8235
set SBOOTP=c:\ibm8235
set IBM8235=c:\ibm8235
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
SET WIN$=C:\WINDOWS
CALL C:\NWCLIENT\STARTNET
CALL C:\TCPDOS\BIN\TCPSTART
```

a Mixed ODI/NDIS Multiprotocol Environment

Figure 98. AUTOEXEC.BAT Control File in

```
[PROTMAN]
DriverName=PROTMAN$

[DXMAIDXCFG]
DIALNDIS_NIF=DIALNDIS.NIF

[DXME0_MOD]
DriverName=DXME0$
Bindings=DIALNDIS_NIF

[ODI2NDI_MOD]
DriverName=ODI2NDI$
ETHERNET_802.3="YES"
Bindings=DIALNDIS_NIF

[TCPIP_V21]
DriverName=DOSNDIS$
Bindings=DIALNDIS_NIF

[DIALNDIS_NIF]
DriverName=SDIALIN$
```

a Mixed ODI/NDIS Multiprotocol Environment

Figure 99. PROTOCOL.INI Control File in

```
Link Driver NTR2000
    PORT A20
    FRAME TOKEN-RING MSB

NetWare DOS Requester
    FIRST NETWORK DRIVE = F
    NETWARE PROTOCOL = NDS BIND
```

Mixed ODI/NDIS Multiprotocol Environment

Figure 100. NET.CFG Control File in a

```
SET NWLANGUAGE=ENGLISH
C:\NWCLIENT\LSL.COM
C:\DIALS\ODI2NDI
REM C:\NWCLIENT\NTR2000.COM
C:\LSP\NETBIND
C:\NWCLIENT\IPXODI.COM
rem C:\NWCLIENT\ROUTE.COM
C:\NWCLIENT\VLM.EXE
```

in a Mixed ODI/NDIS Multiprotocol Environment

Figure 101. STARTNET.BAT Control File

It is important to note that you can only run NETBIND after you have loaded ODI2NDI. This is reflected in the file STARTNET.BAT.

7.2.8.2 ODI-Only Multiprotocol Environment

Working in a single adapter interface is simpler than having both interfaces simultaneously. This session shows an example of a multiprotocol environment over ODI.

The software tested here are:

- NetWare Client V1.21
- LAN Workplace for DOS/Windows

These are the control files defined for this configuration:

```
  .
  .
LSL
DIALODI
IPXODI
TCPIP
VLM
  .
  .
```

Figure 102. AUTOEXEC.BAT Control File in an ODI Multiprotocol Environment

```
Link Driver NE2000
 INT 5
 PORT 300
 MEM D0000
 FRAME Ethernet_802.3
 FRAME Ethernet_II
 Protocol IPX 0 Ethernet_802.3

Link Support
 Buffers 8 1500
 MemPool 4096

Protocol TCPIP
 PATH SCRIPT     C:\NET\SCRIPT
 PATH PROFILE    C:\NET\PROFILE
 PATH LWP_CFG    C:\NET\HSTACC
 PATH TCP_CFG    C:\NET\TCP
 ip_router       9.24.104.1
 ip_netmask      255.255.255.0
 ip_address      9.24.104.91

NetWare DOS Requester
 FIRST NETWORK DRIVE = F
 NETWARE PROTOCOL = BIND NDS
```

Figure 103. NET.CFG Control File in an ODI Multiprotocol Environment

DIALs Client automatically updates LAN Workplace with the IP address it has been assigned. However, in order to prevent LAN Workplace from attempting to obtain an address with BOOTP or RARP, you must specify a dummy IP address in your NET.CFG file.

7.2.8.3 NDIS-Only Multiprotocol Environment

As in ODI, working with NDIS as a single adapter interface is simpler than having both interfaces simultaneously. This session shows an example of a multiprotocol environment over NDIS.

The software tested here are:

- LAN Support Program V1.38
- DOS LAN Services V4.0
- TCP/IP for DOS V2.1.1

These are the control files defined for this configuration:

```
FILES=30
BUFFERS=10
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
STACKS=9,256
LASTDRIVE=Z
DEVICEhigh=C:\LSP\PROTMAN.DOS /I:\LSP
DEVICEhigh=C:\DIALS\DIALNDIS.EXE
DEVICEhigh=C:\LSP\DXMAOMOD.SYS 001
DEVICEhigh=C:\LSP\DXMEOMOD.SYS N ,16,0,0,0
DEVICEhigh=C:\LSP\DXMTOMOD.SYS ST=16
S=16 ES=1 EST=1 C=16 N=18 O=N DS=1024
R=1024 MO=1 MI=1 T1=10 T2=10 TI=10 CF=Y
DEVICEhigh=C:\NET\DLSHELP.SYS
DEVICEhigh=C:\DOS\ANSI.SYS
DEVICEhigh=C:\TCPDOS\BIN\DOSTCP.SYS
```

Figure 104. CONFIG.SYS Control File in an NDIS Multiprotocol Environment

```
SET ETC=C:\TCPDOS\ETC
SET DIALS=C:\DIALS
C:\LSP\NETBIND
C:\DOS\SMARTDRV.EXE
@ECHO OFF
path c:\dos;c:\dials;c:\net;c:\nwdbpath;c:\windows;%path%;C:\TCPDOS\BIN;
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
SET WIN$=C:\WINDOWS
```

Figure 105. AUTOEXEC.BAT Control File in an NDIS Multiprotocol Environment

```
[protman]
DriverName=PROTMAN$

[DXMAIDXCFG]
DIALNDIS_NIF=DIALNDIS.NIF

[DXMEO_MOD]
DriverName=DXMEO$
Bindings=DIALNDIS_NIF

[TCPIP_V21]
DriverName=DOSNDIS$
Bindings=DIALNDIS_NIF

[DIALNDIS_NIF]
DriverName=SDIALIN$
```

Figure 106. PROTOCOL.INI Control File in an NDIS Multiprotocol Environment

The device drivers in this example were loaded in the upper memory block to leave the regular 640 KB available. It is important here to install the TCP/IP for DOS CSD V2.1.1.4.

7.3 DOS Environment

From V4.0 on, IBM will also deliver a separate DOS-specific version of the DIALs Client code, the 8235 Dial-In Client for DOS. This session shows the workstation configuration for NetWare Client in a DOS-only environment.

These are the control files defined for this configuration:

```
FILES=40
BUFFERS=10
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\SETVER.EXE
LASTDRIVE=Z
```

Figure 107. CONFIG.SYS Control File in a NetWare Client Environment

```
@CALL C:\NWCLIENT\STARTNET
@ECHO OFF
set path=c:\dos;%path%;c:\dialsdos
PATH C:\NWCLIENT\;%PATH%
set DIALS=c:\dialsdos
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
```

Figure 108. AUTOEXEC.BAT Control File in a NetWare Client Environment

```
Link Driver DIALODI

Link Driver NTR2000
               PORT A20
               FRAME TOKEN-RING MSB

NetWare DOS Requester
               FIRST NETWORK DRIVE = F
               NETWARE PROTOCOL = NDS BIND
```

Figure 109. NET.CFG Control File in a NetWare Client Environment

```
SET NWLANGUAGE=ENGLISH
C:\NWCLIENT\LSL.COM
C:\DIALSDOS\DIALODI.EXE
C:\NWCLIENT\IPXODI.COM
C:\NWCLIENT\ROUTE.COM
C:\NWCLIENT\VLM.EXE
```

Figure 110. STARTNET.BAT Control File in a NetWare Client Environment

7.4 Windows 95 Environment

As mentioned earlier, Windows 95 already includes its own dialer, the Dial-Up Networking application. It allows you to work in three different protocol environments:

- IPX
- NetBEUI
- TCP/IP

These three protocols can work separately or simultaneously. To configure which protocol you want to work with, start the Network configuration in the Control Panel window. Figure 111 on page 182 shows you the Network Configuration window where the Dial-Up Adapter was defined with all the protocols possible.

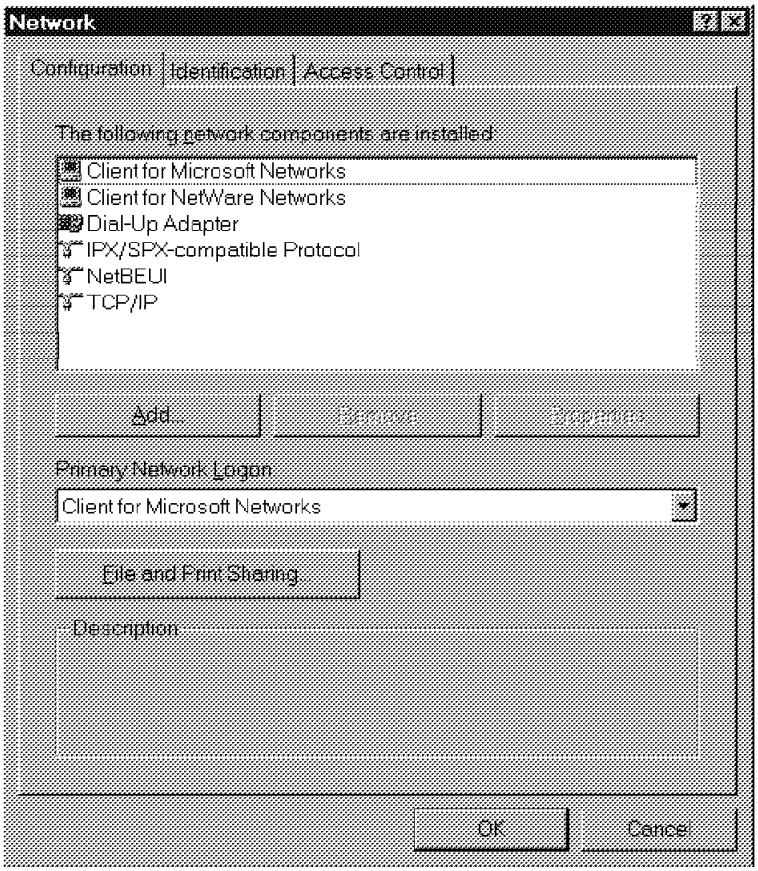


Figure 111. Network Configuration Window in Windows 95

Selecting the **Dial-Up Adapter** and clicking on **Properties** will display the window shown in Figure 112 on page 183. This window is used to configure the protocols to which the Dial-Up Adapter will bind (in our case, IPX, NeTBEUI and TCP/IP).

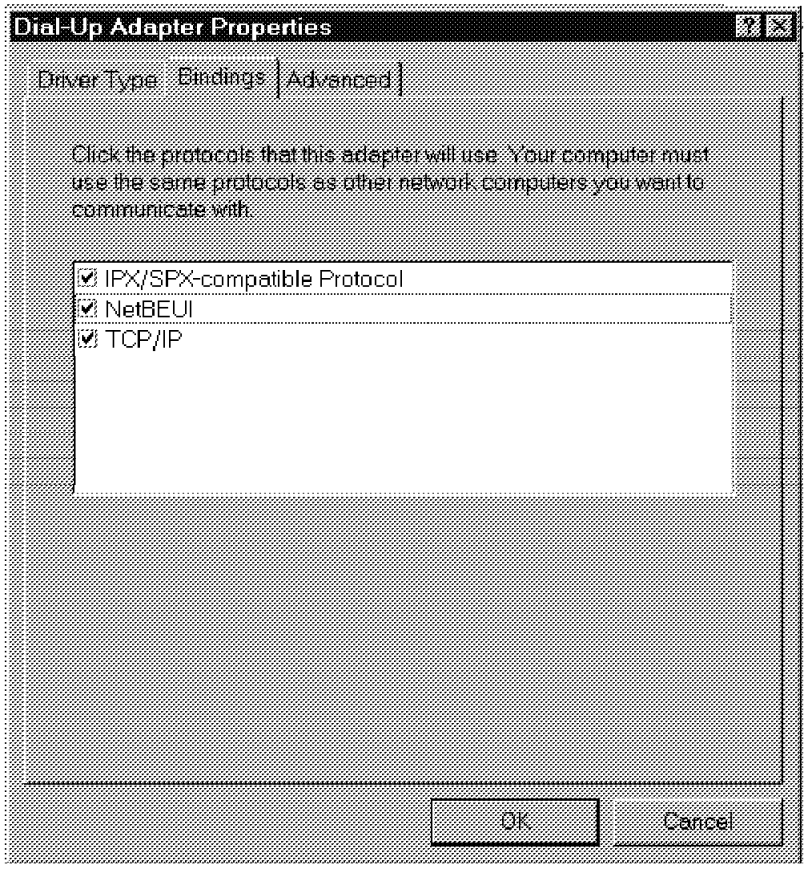


Figure 112. Dial-Up Adapter Properties Configuration Windows in Windows 95

When the Dial-Up Adapter was bound to IPX, NetBEUI and TCP/IP, the system was configured to be able to work with any of those protocols. To actually select which protocols would be activated at dial-in time, it is necessary also to configure the Dial-Up Networking application in Windows 95.

To start the Dial-Up Networking application, click on the **My Computer** icon and click on **Dial-Up Networking** inside the My Computer window.

Click once on the connection defined in the Dial-Up Networking window and click on **File**. Then select the **Properties** pull-down menu to configure which protocols will be activated during dial-in. This procedure will show the connection general configuration as shown in Figure 113 on page 184.

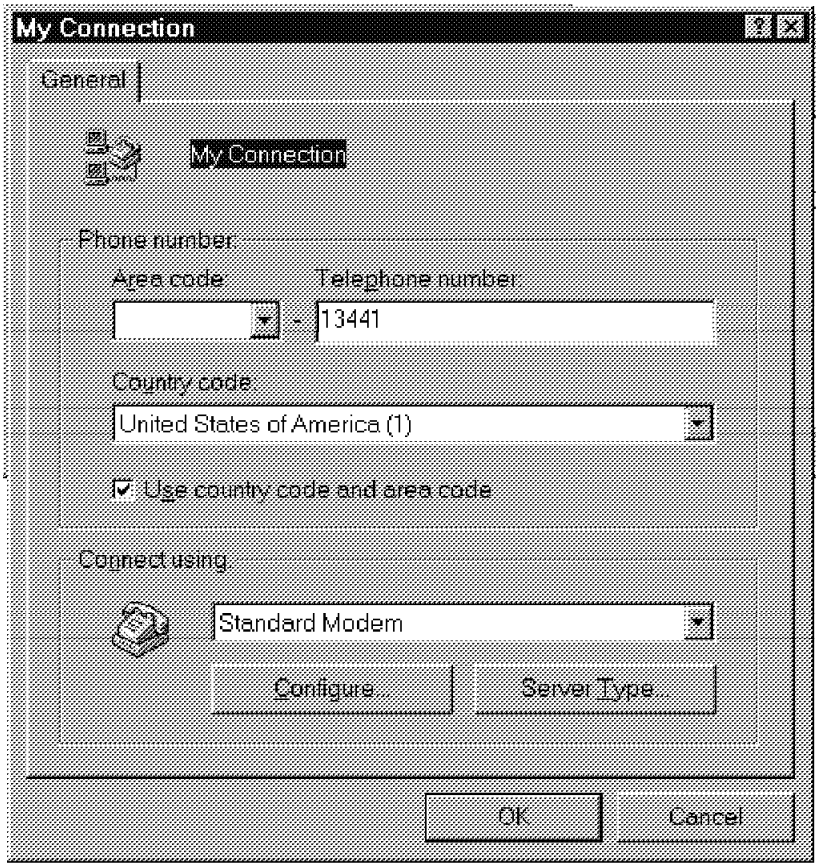
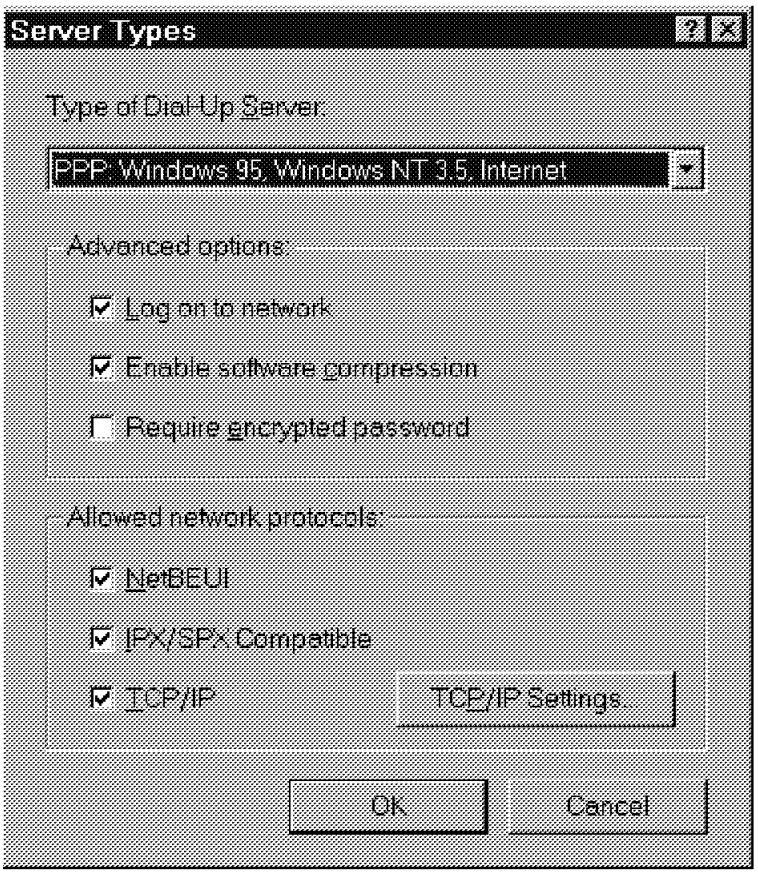


Figure 113. General Dial-Up Networking Configuration in Windows 95

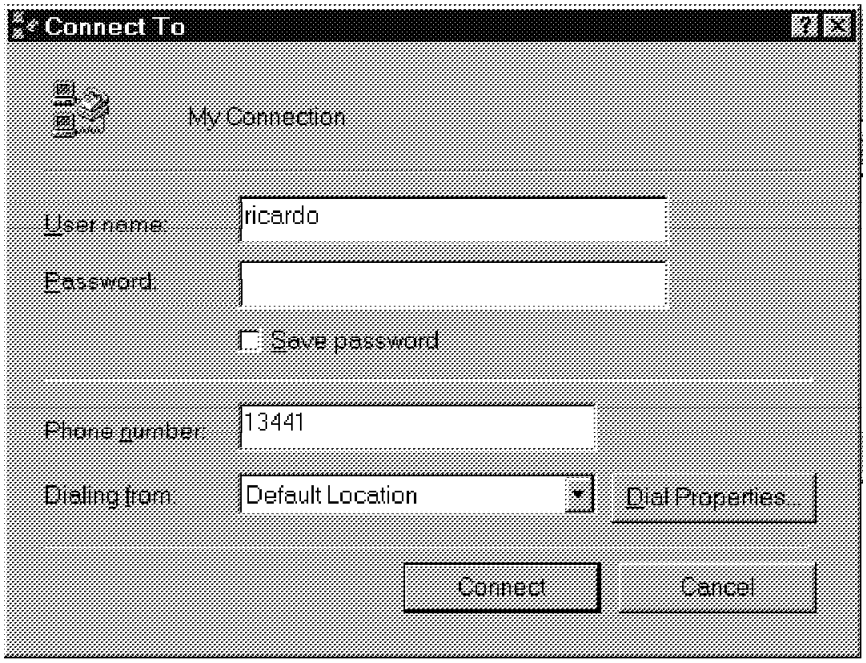
To configure the protocols to be used, click on **Server Types**, which will display the Server Type configuration window shown in Figure 114 on page 185.



Dial-Up Networking in Windows 95

Figure 114. Server Type Configuration for

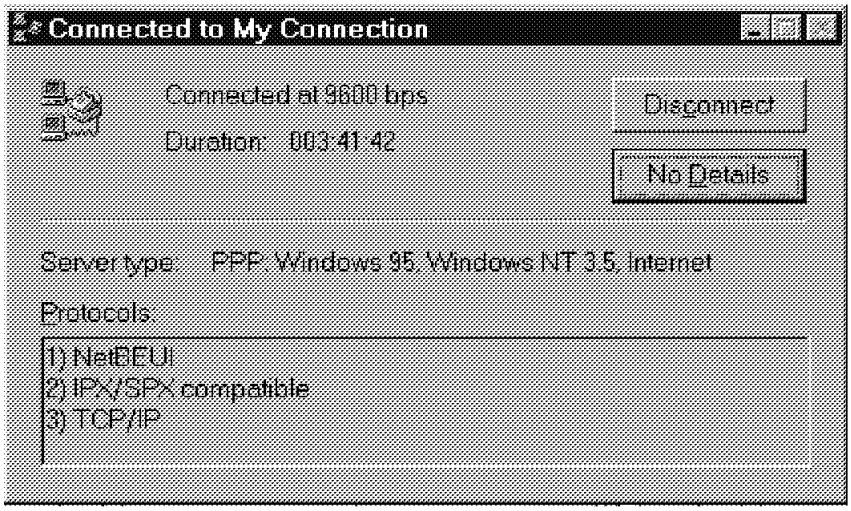
Select the protocols needed and click on **OK**. The system is ready to dial. Click on **Connect** in the Connection window of the Dial-Up Networking application as shown in Figure 115 on page 186.



Networking Application in Windows 95

Figure 115. Connection Window of Dial-Up

After getting the connection and going through the protocol handshaking, the Connection window will show you the protocols enabled for that connection as shown in Figure 116.



Networking After Establishing Dial-In Connection

Figure 116. Connection Windows of Dial-Up

The system is now able to run any IPX, NetBEUI or TCP/IP application.

7.5 Windows and WaveRunner ISDN

This section discusses the implementation of the WaveRunner ISDN adapter on a workstation in a Windows 95 environment.

7.5.1 8235 Management Facility in Windows 95

The recommended level is to use the 8235 Management Facility V4.5.3 or higher.

Special Notes

- To run the 8235 Management Facility via IPX, only one instance of the Microsoft IPX/SPX compatible drivers is allowed.
- If you have Novell servers that you are getting to with Windows 95, then you need to add the following line to the saved configuration file. Click on **Get Configuration** then **Save as** from the **File** pull-down menu. The file is in text format so you can use your favorite editor to edit the file. Put the configuration to the 8235 to help clear up a few problems that may occur on the clients:

```
[Netware]
  <--look for this section in your configuration file
DefaultNearestServer=<server closest to the 8235>
```

- Be sure to use the Microsoft Client and not the Novell client, especially if you are using Bindery Security. Microsoft's client does not support NetWare NDS in its initial release. A future upgrade should add this support.

7.5.2 Dial-In Client configuration

1. Do not use the Dials software for Windows 3.X.
   It does not work and is not supported and may cause problems.
2. Check your **Network Setup** to see that you have installed **Dial-In Adapter**. If you have not, then install it by clicking on the **Add Adapter** button and going through the procedure in Windows 95.
3. Install a modem on the machine you are going to use.
4. Go into the control panel then select the modem icon.
5. Click on the **Add** button, then select the **Next** button. At this point Windows 95 will try to detect your modem, but it is not always sucessful so you have to manually select your device.

Notice

If you will be using the WaveRunner internal modem, we recommend that you select the **IBM WaveRunner ISDN V.120/Modem driver (analog)** for this purpose. If this selection does not meet your requirements (dial-in), then you should choose **Hayes Smartmodem 2400** or **** Default Settings ****, in that order. The Hayes modem string uses many universal default variable that we have seen working fine with this configuration. We have had few problems using the WaveRunner analog modem.

One thing you may wish to check is that you are not using the IBM WaveRunner V.120/Modem drivers (ISDN). If you are using these drivers, a timeout condition will occur when the connection is not established within the ISDNDialTimeout parameter in the Dials.ini File. To resolve this, try the following:

- Changing the installed modem type
- Changing ISDN=No in the modems.ini file
- Changing ISDNDialTimeout to a value above 60 in the DIALS.ini

The first choice is recommended, as there are many appropriate selections that can be made that will work perfectly for your purposes.

7.5.3 Connection Step

- After you have installed the driver and WaveRunner, you can see the configuration of your Windows network, like this:

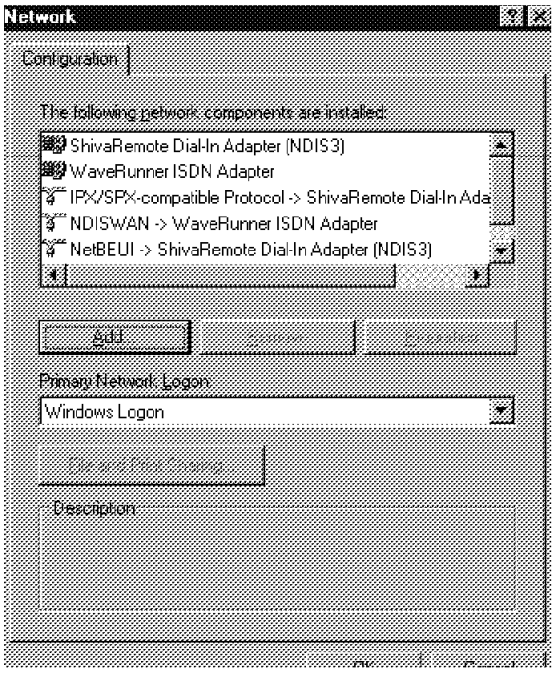


Figure 117. Network Configuration

Note: The IBM Windows 95 Dial-In client was not available at the time this book was being developed; the driver name should be **IBM Dial-In Adapter** for the IBM Dial-In Networking Client.

- Select the **WaveRunner ISDN Adapter** to configure your ISDN line (must be provided by your Telephone Company).

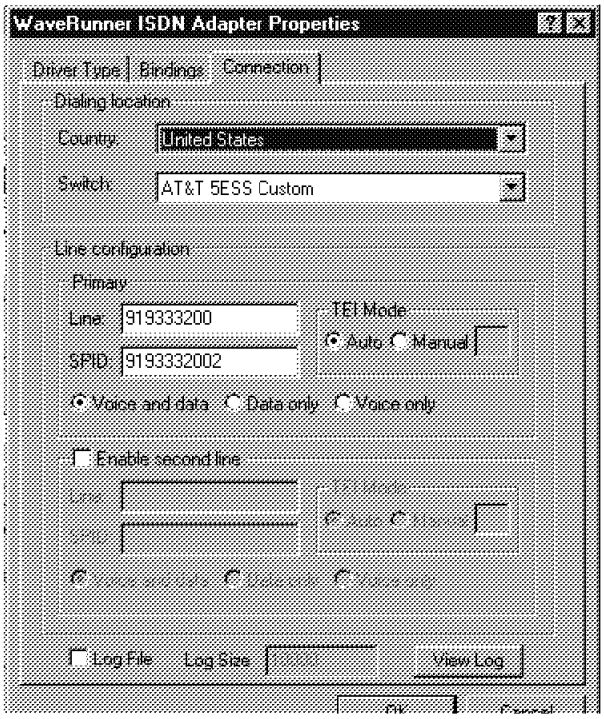


Figure 118. WaveRunner Adapter

- Then go to ISDN Connection Wizard to create the new connections. Add your name and click **Next**.

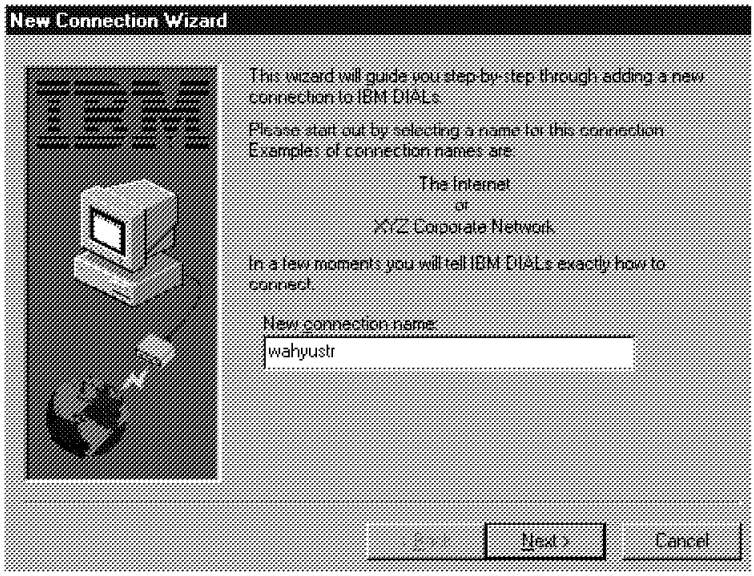


Figure 119. Create New Connection

- Select the modem and type the ISDN phone number, then click **Next**.

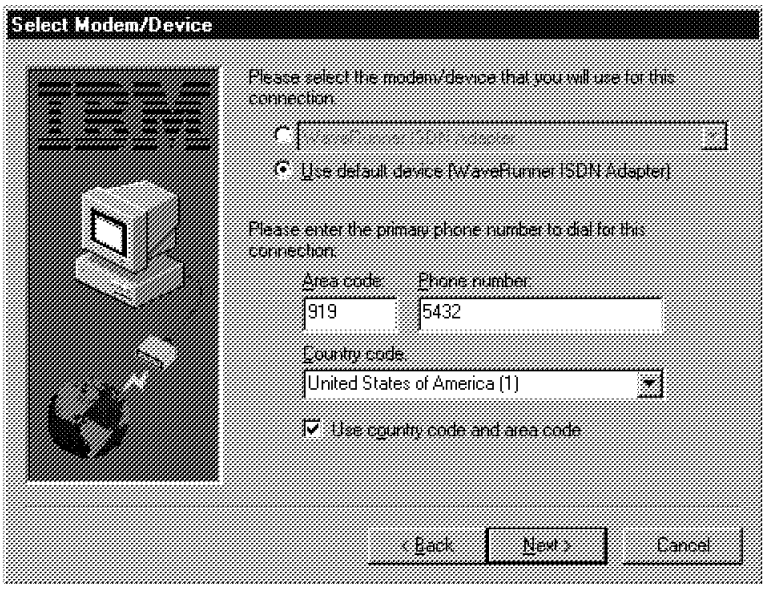


Figure 120. Modem and Phone Selection Menu

- If you have finished, you will see the panel below. Click **Finish**.

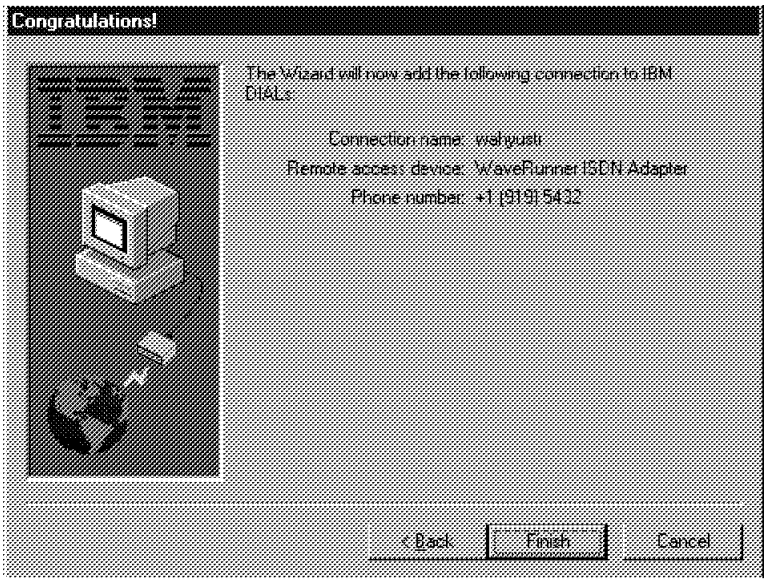


Figure 121. Congratulations Panel

Note: The use of the phone number 5432 in the previous examples is due to the lab environment in which these tests were conducted.

Now that you have finished creating your new ISDN connection, follow these steps to connect your 8235-I40 using the ISDN line:

- First, select IBM Dials v5.0. Choose **General** and fill in the User Name, Password and Phone Number fields. Then click **Connect**.

  Note: Obtain your user name and password from a System Administrator who is authorized to create user IDs on the 8235-I40.

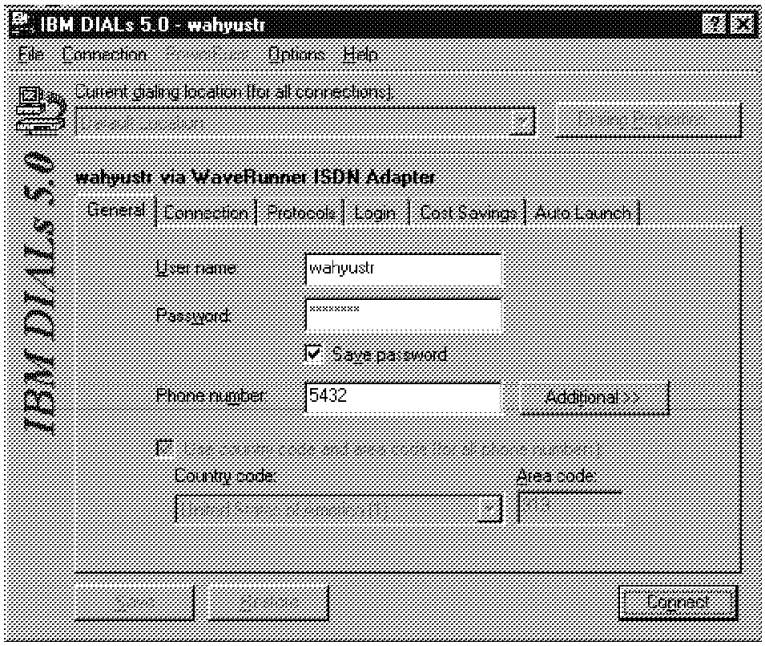


Figure 122. General Page

- You may configure your own connections, or you can use the defaults. Next are samples of Configured Connection windows.

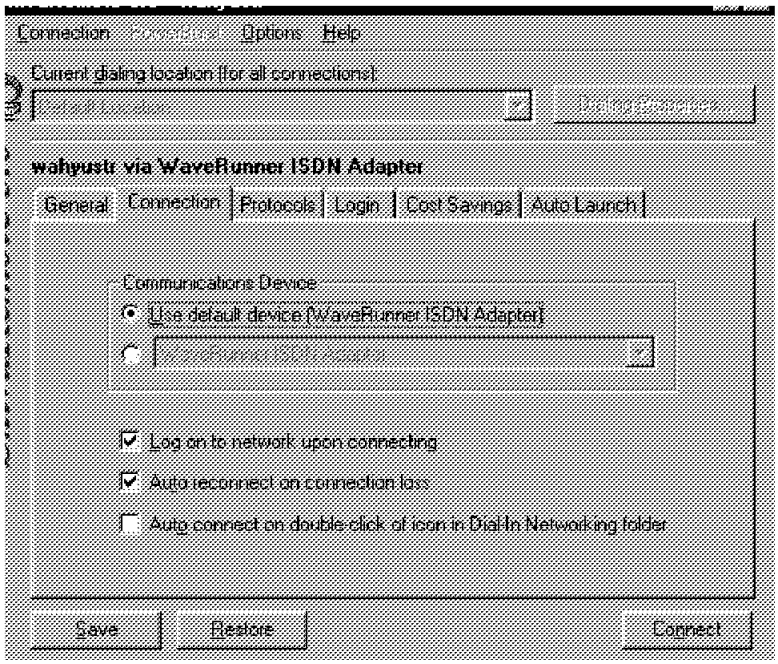


Figure 123. Connect via WaveRunner ISDN Adapter (Connection Page)

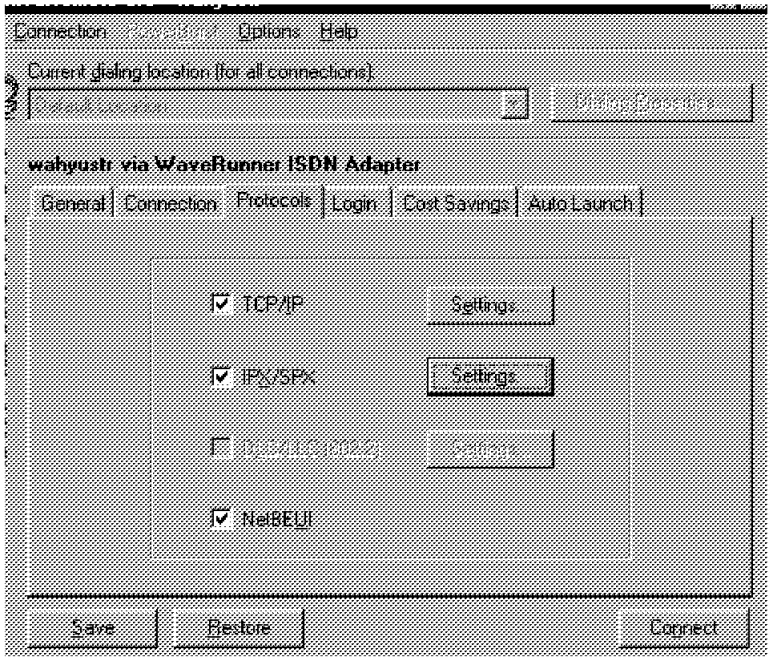


Figure 124. Connect via WaveRunner ISDN Adapter (Protocols Page)

Note: Protocols which are not bound to the **Dial-In Adapter** will be greyed out on this configuration page.

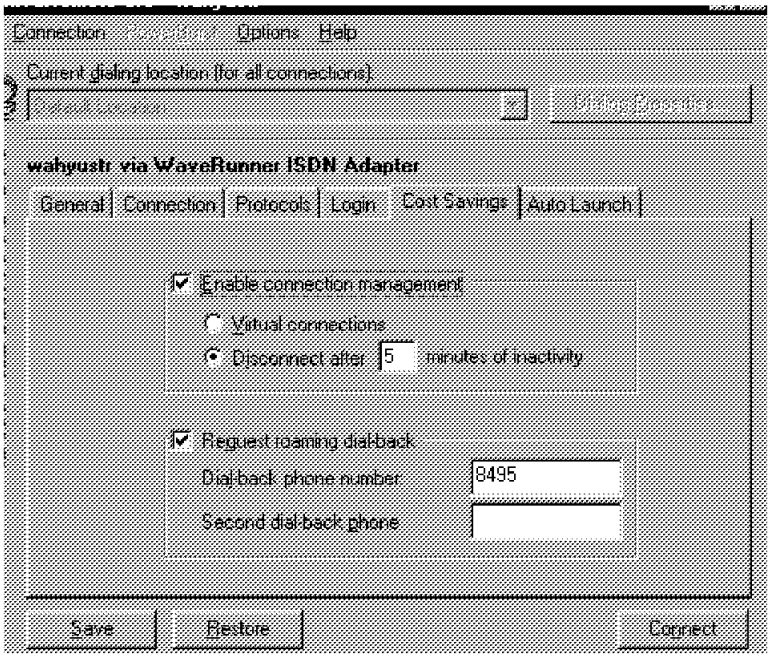


Figure 125. Connect via WaveRunner ISDN Adapter (Cost Savings Page)

- When you have finished the configuration, click **Connect**. You will see the window below.

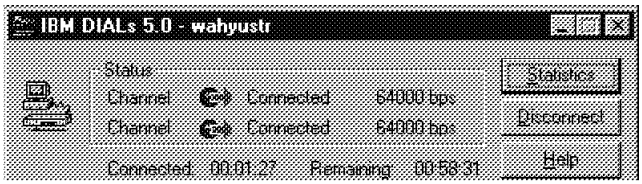


Figure 126. Window after Connection Is Made

7.5.4 Monitoring

The following windows show the capabilities of the software to monitor your connection to the 8235-I40.

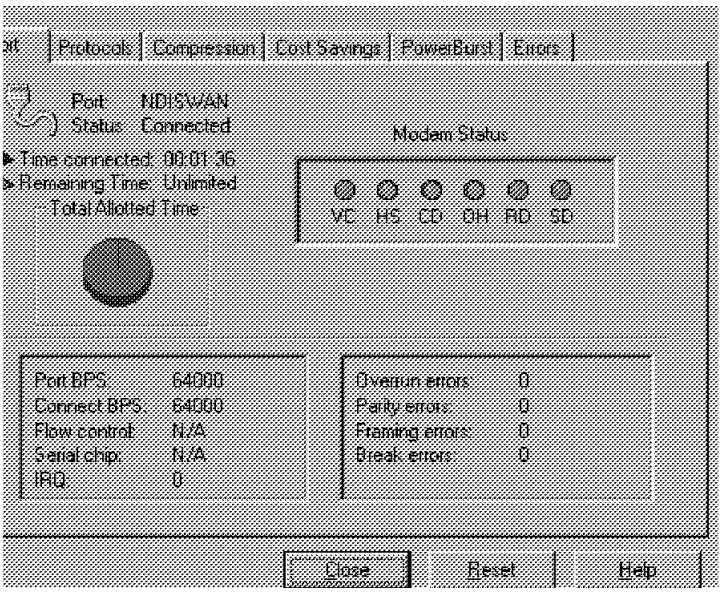


Figure 127. Performance Monitor (Port panel)

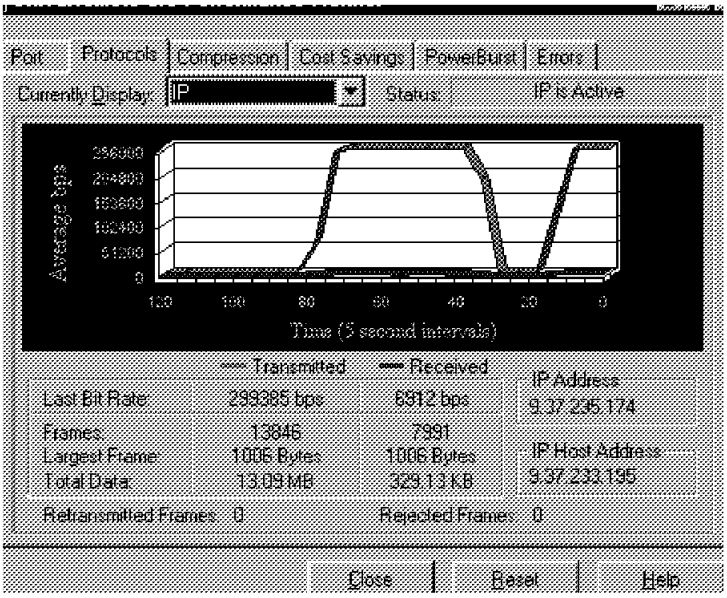


Figure 128. Performance Monitor (Protocol panel)

On the protocol panel, there is a drop down menu to select the appropriate protocol to view statistics for. Here we can see the throughput in both graphic and numerical format, as well as protocol specific information.

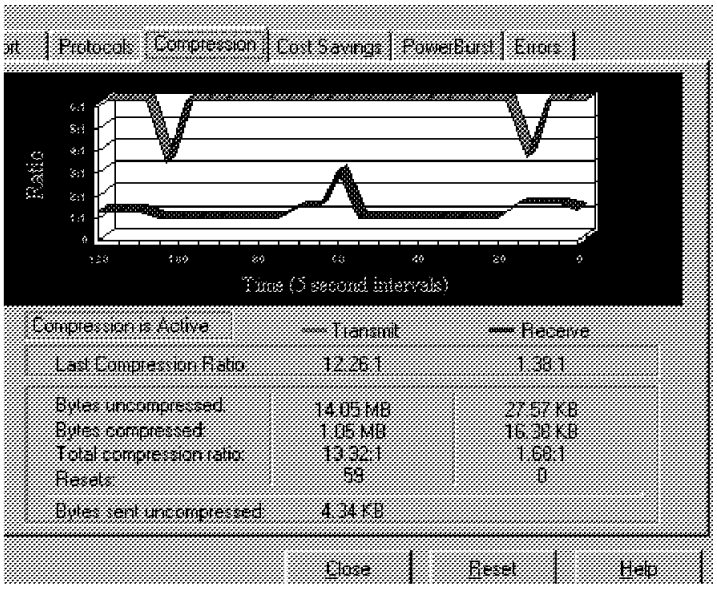


Figure 129. Performance Monitor (Data Compression panel)

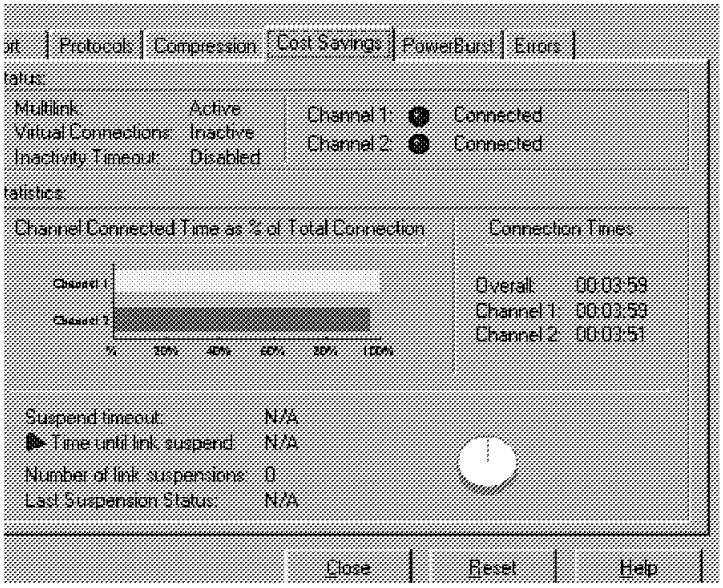


Figure 130. Performance Monitor (Cost Savings panel)

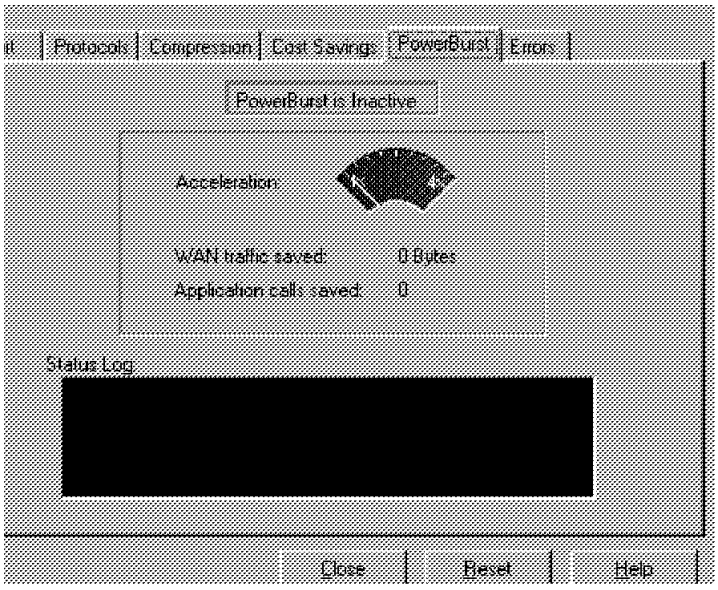


Figure 131. Performance Monitor (Powerburst panel)

Note: PowerBurst will only be active if a key has been purchased for use on the 8235 the dial-in user has connected to.

Chapter 8. Dial-Out Client

Dial-Out is an application that lets you communicate from your workstation across your LAN through the 8235 to access a telephone network.

When you use Dial-Out, instead of dialing out through a modem directly attached to your workstation, you dial out through one of the 8235 ports, which is connected to an internal or external communications device. You can use Dial-Out to access remote services such as bulletin board systems (BBS), online services, or commercial services such as Internet Service Providers or Prodigy. The following figure shows you the Dial-Out topology.

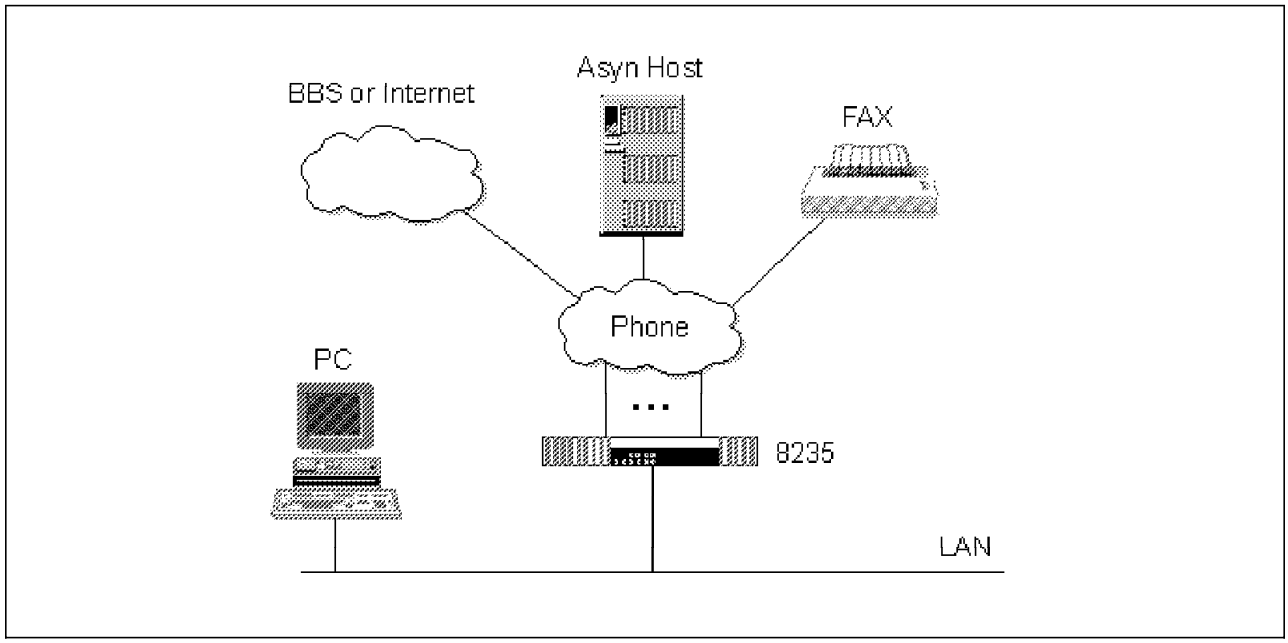


Figure 132. Topology of a Dial-Out Solution

You can connect to the 8235 for dialing out through any Windows telecommunications software or any DOS package that supports the Interrupt 14 (INT14) or NetWare Asynchronous Services Interface (NASI) program interfaces. 8235 Dial-Out lets you share each port and telephone line on your 8235 among all the users of your network, one user at a time. You can also install multiple 8235s or an 8235 with multiple ports to provide simultaneous Dial-Out services to many users.

There are two main components to the 8235 Dial-Out software package:

- 8235 Dial-Out Driver: This driver redirects communication between your Windows software and the COM port it is trying to use. For example, your communications software might be set to use COM2, but the Dial-Out driver intercepts that and sends all of the data across the network to the 8235 instead of through your COM port.
- Chooser: This program lets you select which of the 8235s on the network you want to use for dialing out, as well as which COM ports to redirect to the 8235s you select.

8.1 Installation of Dial-Out Clients (OS/2)

The installation example shown here is on the OS/2 operating system. Run the install from the Dial-Out diskette and follow the procedures requested. For versions before 4.5, at the end of the installation, it will check if you have IPX installed in your system. If you do not, it will present the panel shown in Figure 133. Versions 4.5 and higher support dial-out over either the TCP/IP or IPX protocol.

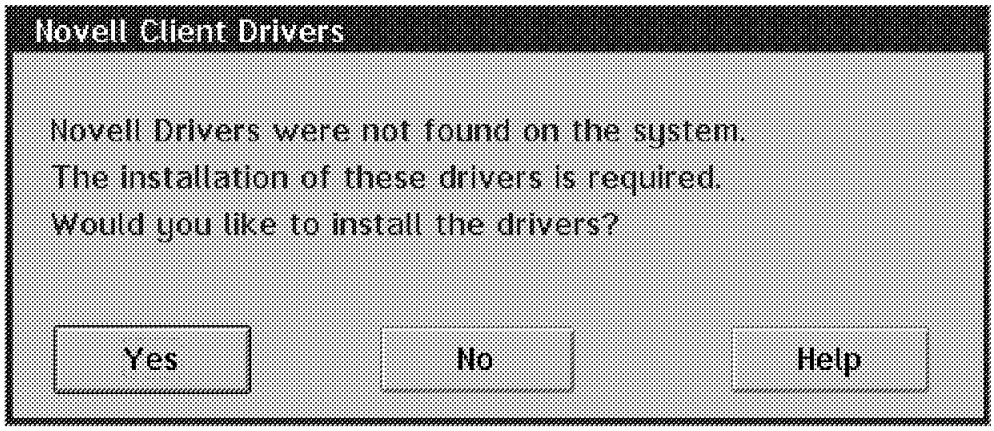


Figure 133. Installing Novell Client Drivers

The installation program then requests the type of LAN you are using as shown in Figure 134.

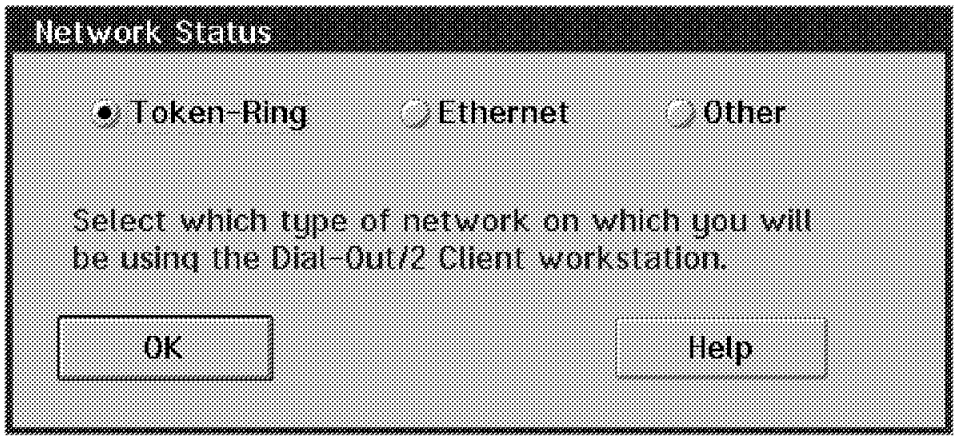


Figure 134. LAN Type Request

Installation is completed with the panel shown in Figure 135 on page 199.

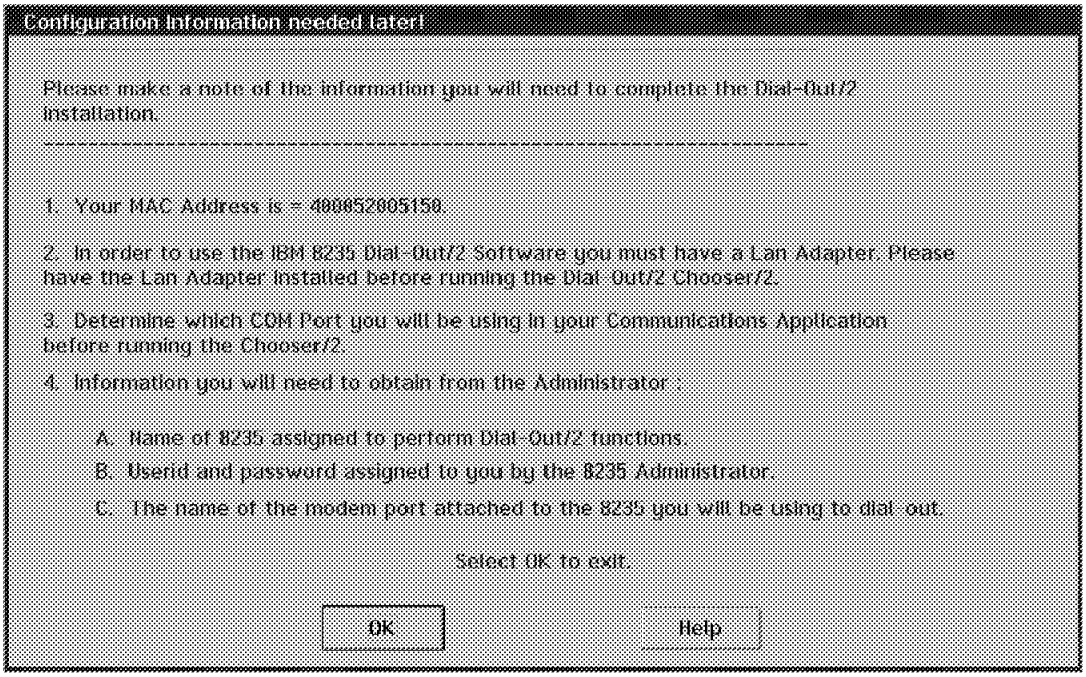


Figure 135. Conclusion of the Dial-Out Installation

The installation program creates the folder shown in Figure 136.

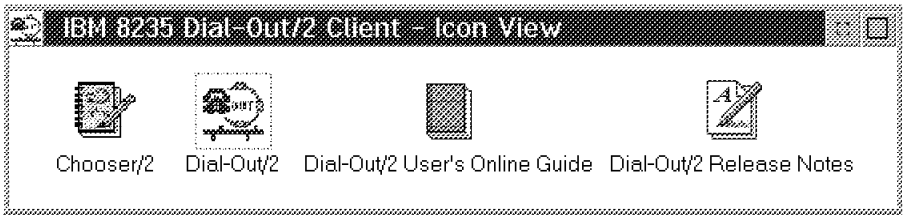


Figure 136. Dial-Out Folder Contents

8.2 Configuring and Using Dial-Out

When the Chooser/2 application is started, you will get the panel shown in Figure 137 on page 200, where you can select the 8235 that will be used for Dial-Out.

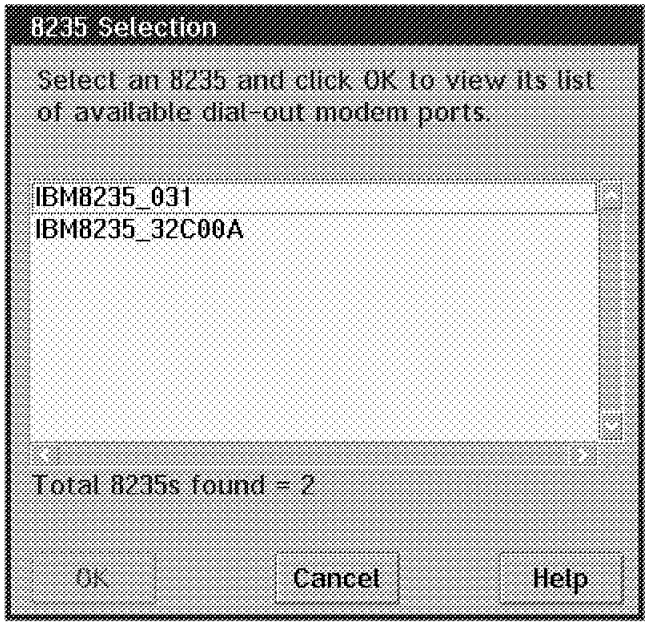


Figure 137. Chooser/2 Device Search Panel

Once the 8235 is selected, the port redirection panel appears as shown in Figure 138 on page 201 where you can:

- Enter your username
- Enable Dial-Out
- Redirect the COM ports of your PC

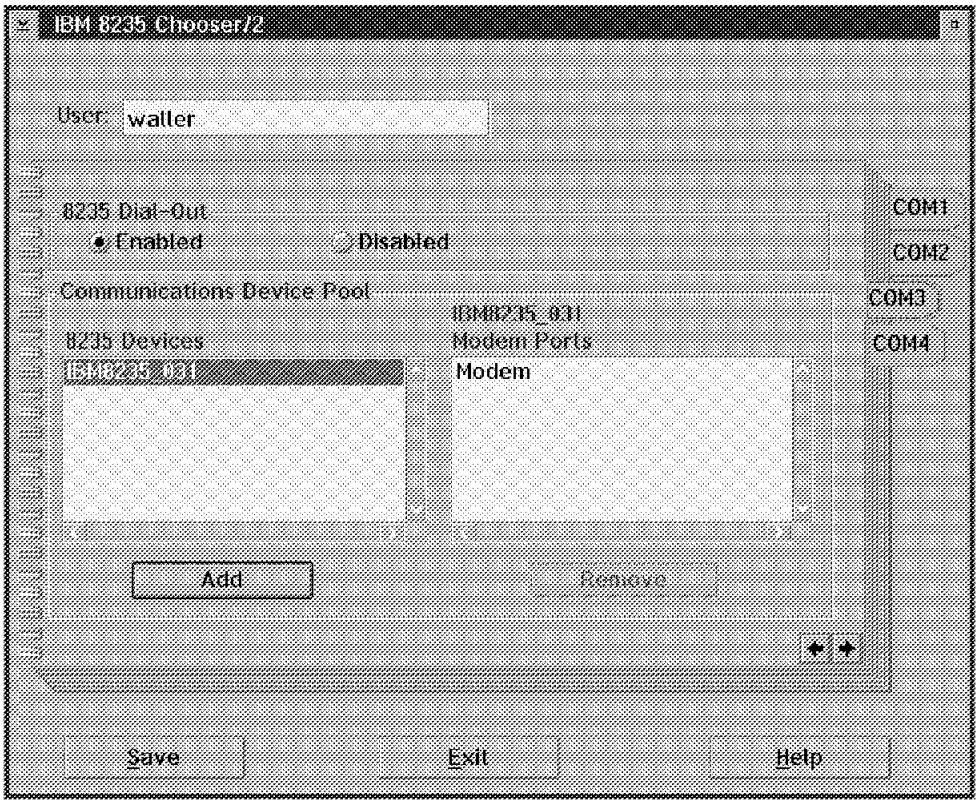


Figure 138. Chooser/2 Port Redirection Panel

When you click on **Add** you will be asked to select the port that will be used. You can choose between modem ports, port pools or even the command shell. This procedure will end the client configuration. After saving and exiting, the client will notify you if it is necessary to reboot before using the dial-out client.

Once configured, you can now double-click on **Dial-Out/2** in the Dial-Out folder. A login box will appear
as shown in Figure 139.

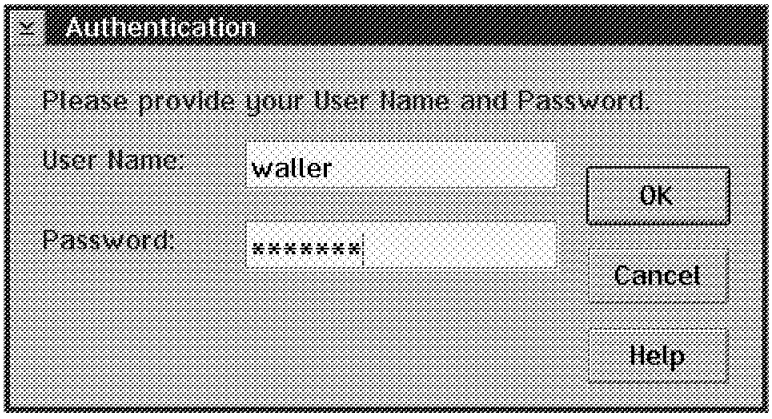


Figure 139. Dial-Out Logon Panel

Input your password and click on **OK** to start the Dial-Out connection procedure. If no errors are detected you will be informed of the successful connection and you will get the modem status panel as shown in Figure 140 on page 202.

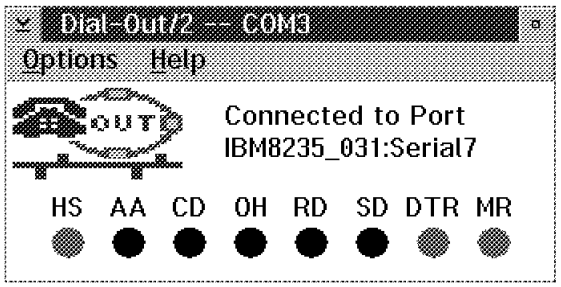


Figure 140. Modem Status Panel

Note: The 8235 itself also has to be configured for Dial-Out. Use the 8235 Management Facility to enable Dial-Out on the device and for the user that will be using it.

8.3 Installation of Dial-Out Clients (Windows 95)

First, load the Windows 95 Dial-Out driver by running SETUP.EXE from the A: Drive. Just go through the normal steps; after installation the machine will restart.

8.3.1 Setting Up COM Ports

Follow the instructions in this section to select the COM ports you want to redirect and to specify the 8235 you want to use for dialing out.

Note that you only have to redirect the ports once. Once you have set up the COM ports and the 8235 you want to use for dialing out, you do not have to run the Chooser again unless you want to change this setup. The procedures are:

- Open the **Chooser95** icon located in the control panel.
- Click the tab of the COM port (COM1 through COM4) you want to use for dialing out through the 8235.
- Click **Browse Network** to open the Browse Network dialog box.
- In the Browse Network dialog box, select the device you want to use for dialing out through the current COM port, then click **Add Selection to COMx.** Repeat this step for each of the 8235s you might want to use to dial out using this COM port.

  Note: If you cannot find your device on the network, deselect the **Show Only Usable Devices** checkbox from the **Advanced Options** page.
- When you have added the devices you want, return to the Chooser95 window.
- Select the Redirect checkbox (so that it contains a checkmark) to begin redirecting activity in this COM port to the selected 8235. This adds a lightning bolt to the tab for this COM to indicate that the port has been redirected.
- To change the order of the devices in the device list, drag the 8235

up or down in the list.

You do not need to open the Chooser again except to redirect other ports, change your currently redirected ports or change your user name or other preferences.

8.4 Setting Up the 8235 in the Modems Control Panel

If you are using a Windows 95 communications package, such as Hyperterminal, Dial up Networking, or Microsoft Fax, you must set up the 8235 in the Modems control panel before you can use it to dial out.

This must be done because all 32-bit communications software (that is, software written for Windows 95 instead of Windows 3.1x) uses the information created by the Modems control panel to find a modem for dialing out. 16-bit (Windows 3.1x) communications software looks directly to the COM port on your workstation to dial out and ignores the information in the Modems control panel.

8.5 Prerequisites

Before following these instructions, you must follow the instructions in Setting Up COM Port and 8235 to redirect a COM port to use and 8235 to dial out. Once you have redirected one or more COM ports, follow the instructions here to set up the 8235 in the Modems control panel. These are the procedures:

- Open the Modems control panel by opening the **Control Panel** folder and double clicking the **Modems** icon.
- In the window that follows click **Add**.
- Check **Don′t detect my modem; I will select it from a list** and then click **Next**.
- In the dialog box that appears, select the manufacturers and modem type connected to the 8235 you will be using to dial out. For example, if you are dialing out through an 8235 containing a V.34 modem module, you would select **IBM** in the list of manufacturers on the left and **8235 V.34 Modem module** from the list on the right.. Then click **Next.**
- Select the COM port you have redirected using 8235 Dial-Out for Windows 95. Then click **Next**.
- When Windows 95 completes installing ypur modem, click **Finish**.
- If you redirected other COM port using the Chooser95 control panel click **Add** again to repeat these instructions for each COM port you redirected. Otherwise click on **Close** to exit the Modems control panel.

Tips

Windows 95 cannot detect a modem automatically through 8235 Dial-Out because the modem is not directly connected to a COM port on your workstation. For this reason, you will have to select the modem in your 8235 from a list provided by Windows 95.

Some 8235s contain internal adapters, while others can contain external modems of any brand and model. Contact your network administrator for the modems used with the 8235.

Chapter 9. LAN-to-LAN Connections

LAN-to-LAN Connections are a function of the 8235 that allows data traffic to be routed between two physically connected 8235s. Either end of the LAN-to-LAN connection can originate the call linking the networks. Once the link has been established, the 8235s can route any of the supported protocols traffic (IP, IPX, and AppleTalk) between the networks. Multiple Protocols can run simultaneously and different LAN physical interface connections are supported, including a connection from Ethernet to token-ring. NetBEUI/LLC is not supported for LAN-to-LAN connections.

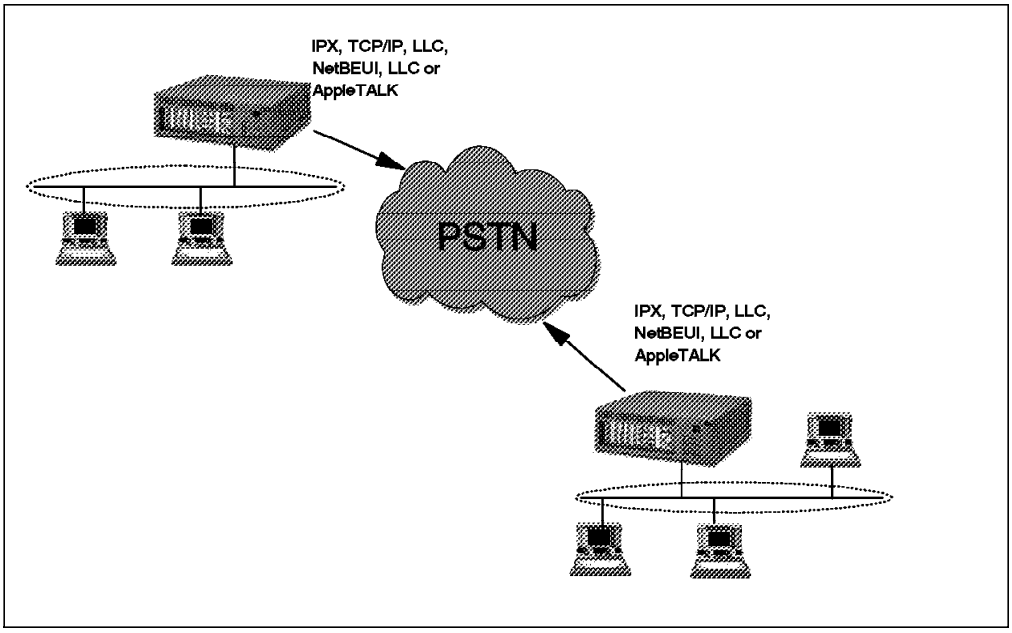


Figure 141. The Scenario

9.1 Configuring an 8235 DIALs Server to

Answer a Multilink LAN-to-LAN Session

This procedure describes how to use the 8235 Management Facility to configure an 8235 Server to answer LAN-to-LAN multilink connections using PPP Multilink Protocol (MLP).

Channel aggregation allows LAN-to-LAN connections to bundle two to eight together to form a single, wider and faster connection, providing greater throughput and less delay.

9.1.1 Prerequisites

- You configured the 8235 for LAN-to-LAN connections.
- You must have configured the origination device for a LAN-to-LAN site. You must also have configured in the originating device's 8235 User List or primary authentication server's user list a user name with LAN-to-LAN privileges.

- The user ID and password associated with the LAN-to-LAN connection must be added into the authentication list of the answering device.

9.1.2 Steps

1. In the Device List window, either double-click the device you want to configure or select the device and choose **Get Configuration** from the Actions menu.

   The general Configuration page appears.

2. In the Function area, choose the **LAN-to-LAN Answer** check box.

Table 25. PPP Multilink Protocol Settings

Check box	If Enabled	If Disabled
Enable	Enables PPP multilink so that the 8235 can aggregate multiple communication channels together to form a single,wider and faster connection	Disables PPP multilink. 8235 can have only one communication channel on each physical connection.
Fragment packets>__bytes	Any packets that contain more than the specified number of bytes are fragmented into equal smaller packets that are transmitted simultaneously across each link in the multilink connection.	Packet are distributed unfragmented over the link of the multilink connection.

3. Close the Configuration windows. A dialog box appears asking if you want to send the configuration changes to the device.
4. Click on the following:
   - **Yes** to set the configuration to the device and close the windows.
   - **No** to close the windows without setting the configuration to the device
   - **Cancel** to return to the Configuration windows.

9.2 Configuring an 8235 to Answer LAN-to-LAN Virtual Connections

Follow these steps to configure an 8235 to answer a LAN-to-LAN Virtual Connection. If you configure a phone group for virtual connections, the 8235 supports only IP and IPX protocols for those connections. AppleTalk, NetBEUI, and LLC are not supported for use with LAN-to-LAN Virtual Connections.

9.2.1 Prerequisites

- You must have configured the device to answer LAN-to-LAN connections.
- You must have configured a phone group for the device.
- Before you can initiate the LAN-to-LAN virtual connection, you must also configure the originating device.
- You must configure for the answering device a user name with LAN-to-LAN privileges either in the 8235 User list or in the user list for the primary authentication server you are using.
- Your must only use IP or IPX protocols. Virtual connections are not supported for the AppleTalk, NetBEUI or LLC protocols.

9.2.2 Steps

1. In the Device List windows, either double-click the device you want to configure or select the device and choose **Get Configuration** from the action menu.
2. In the Protocols area, click **IP**, **IPX** or both check boxes.
3. in the Function area, click the **LAN-to-LAN Answer** check box.
4. Choose **Virtual Connections** from the Configure drop-down list.
5. Configure the following parameters:
   - Click the **Enable Virtual Connections** check box.
   - In the Maximum Number of Connections field, enter the maximum number of connections (including virtual connections) that can be made to the 8235 at one time. You can enter a value up to 255.

     The 8235 Management Facility automatically sets this value according to the cards configured for the device in the Slots Configuration page.

     Note: Each virtual connection made through the 8235 uses memory. To minimize memory utilization, do not configure the 8235 for more virtual connections than you need. In addition, if a suspended virtual connection tries to resume and there are no physical resources available on which to resume, the connection is lost.
   - In the Function area, click the **LAN-to-LAN** check box.
   - In the Suspend LAN-to-LAN Link ID Inactive field, enter the time in seconds that the LAN-to-LAN connection can be inactive (not transmitting meaningful data) before the connection is suspended.
   - In the Resume LAN-to-LAN Conditions area, you can optionally select one or both the following options:

   Check the **Temporarily Reconnect to Update Routing Tables** check box and enter a value in the minutes field if you want the LAN-to-LAN virtual connection to automatically resume if it has been suspended for the time specified in the minutes field.

This allows the 8235s on either end of the virtual connection to periodically exchange update routing and SAP database information, providing updated information on the available network resources (servers and hosts).

Check the **Temporarily Reconnect for Routing Table** check box and select an option from the Routing Table Change Type drop-down list if you want the LAN-to-LAN virtual connection to resume the connection upon a particular type of routing table entry.

This ensures that the 8235s on either end of the virtual connection are updated each time there is a change in available network resources of the type specified in the drop-down list.

Note: If your network includes many servers and hosts, activating this check box can cause LAN-to-LAN virtual connections to resume often. If you expect servers and hosts to be coming online or going down frequently, you should disable this check box.

6. Choose **Phone Groups** from the configure drop-down list.
   The Phone Groups Configuration page appears.
7. In the Phone Groups list, double-click the phone group you want to enable LAN-to-LAN virtual connections or select the phone group and click **Edit**.
   The Phone Groups General Configuration page appears.
8. Configure the following parameters:
   - In the Protocols area, enable either the **IP, IPX**, or both LAN-to-LAN check boxes.
   - In the Virtual Connections area, click the **LAN-to-LAN** check box.
   - In the LAN-to-LAN area, click the **Answer** check box.
   - Click **OK** to save your changes and close the Phone Groups Configuration dialog box.
9. Repeat steps 6 and 7 for each phone group you want to be enabled for virtual connections.

   Note: We recommend that you attach a phone group enabled for virtual connections to only one incoming pool.
10. Close the Configuration Window.
    A dialog box appears asking if you want to send the configuration changes to the drives.
11. Click one of the following:
    - **Yes** to set the configuration to the device and close the window.
    - **No** to close the window without setting the configuration to the device.
    - **Cancel** to return to the Configuration window.

9.3 Configuring a LAN-to-LAN Function

To configure the LAN-to-LAN function you need to:

- Enable the LAN-to-LAN function in the General Option.
- In the panel you can also configure disconnect timeout, compression and multilink.
- Enable the LAN-to-LAN function at the port level.

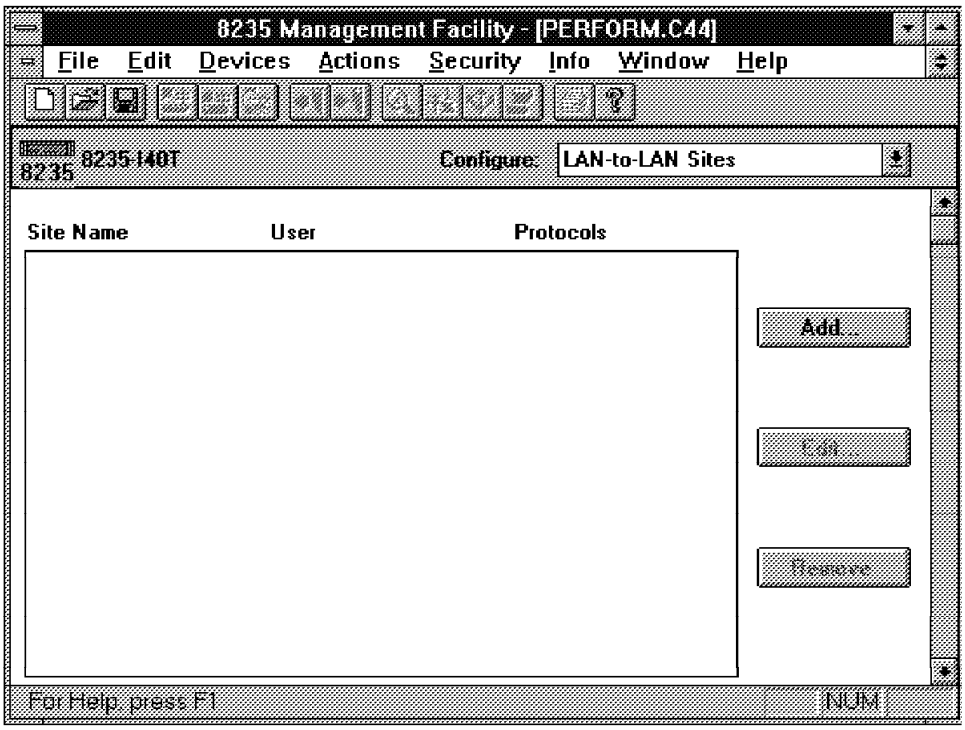


Figure 142 (Part 1 of 5). LAN-to-LAN

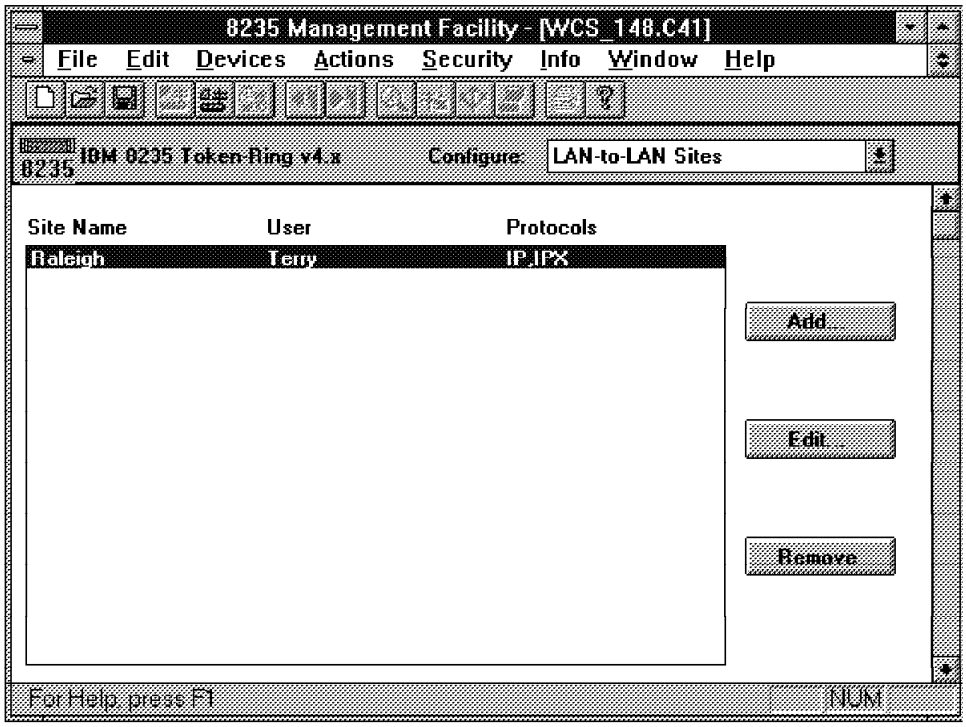


Figure 142 (Part 2 of 5). LAN-to-LAN

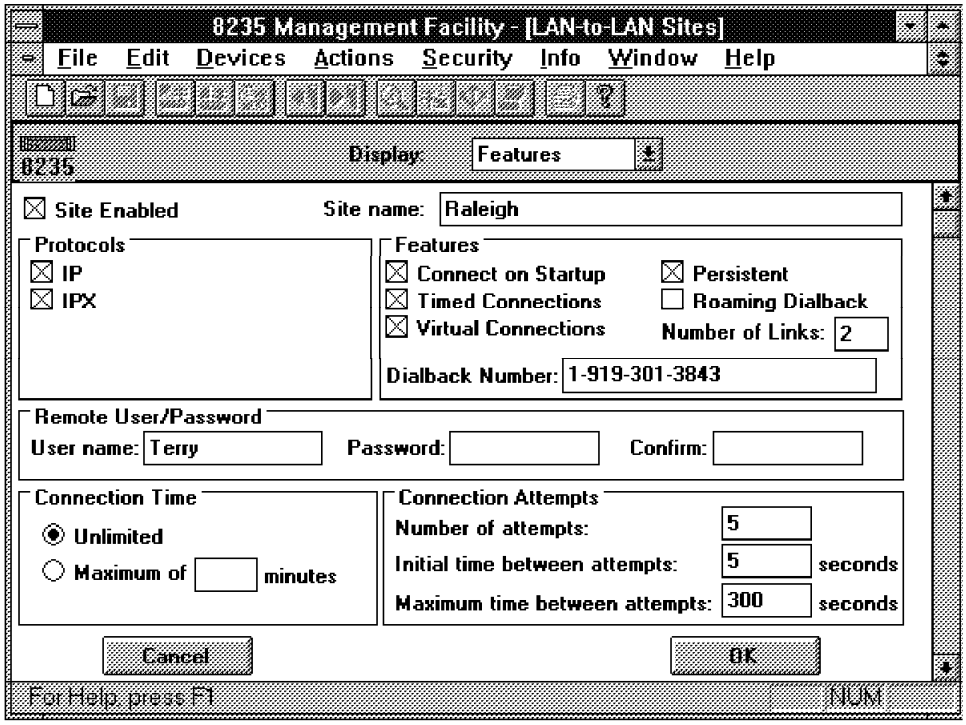


Figure 142 (Part 3 of 5). LAN-to-LAN

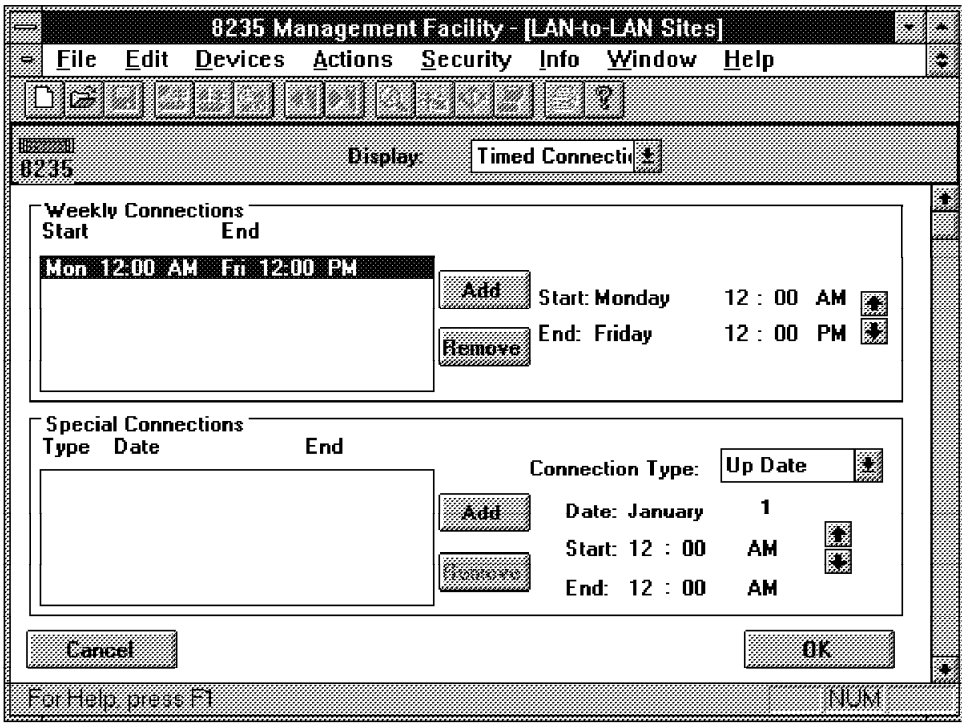


Figure 142 (Part 4 of 5). LAN-to-LAN

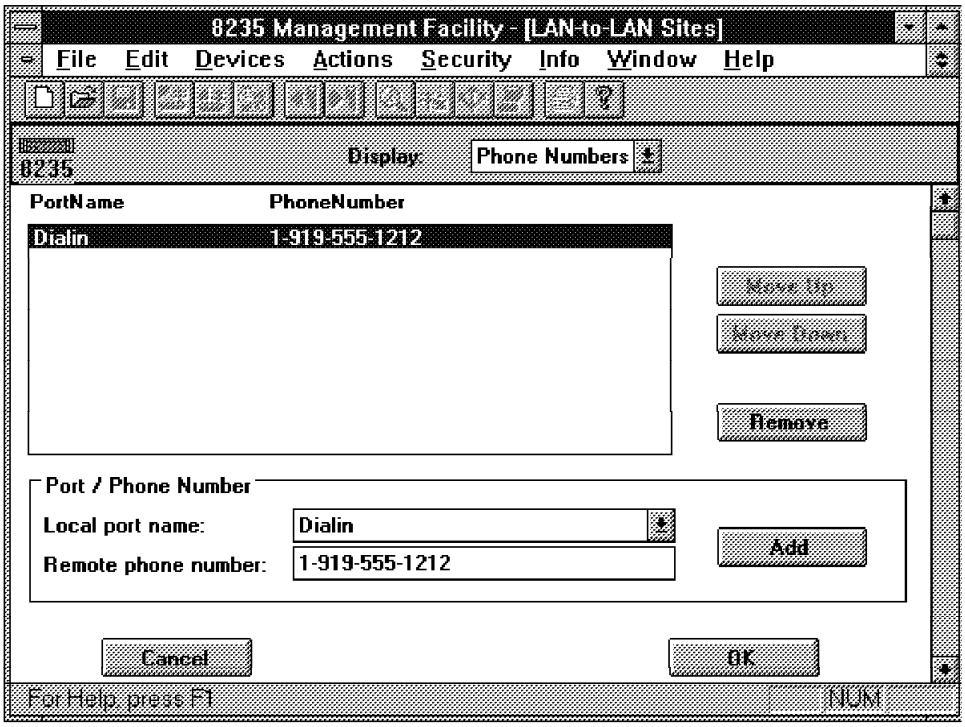


Figure 142 (Part 5 of 5). LAN-to-LAN

Note: There may be more pages to complete depending on the features you select.

9.4 Configuring Timed Connections

One of the ways you can start a LAN-to-LAN connection is by configuring timed connections in the Timed Connections configuration page. A timed connection specifies the weekday and the start and stop times of your connections. You can configure timed connections for each day of the week (Monday through Sunday). You can also configure special connections that specify a date and time that the LAN-to-LAN connection is up (when it is ordinarily down) or a specific day the connection is down (when it is ordinarily up).

While a timed connection is active, it is considered to be persistent; therefore, idle timeouts and maximum connect times do not apply to timed connections. If a timed connection cannot be established, repeated attempts are made using the port pools to establish a connection for as long as the timed connection is configured to be active.

9.5 Configuring Maximum Connection Time

A site can be configured for the maximum time that a LAN-to-LAN connection is allowed to be active. This time is set in minutes. Connection time is the amount of time a site can be dialed in for any one time. You can select unlimited time or a maximum number of minutes.

The following explains the two options:

- **Unlimited**
  - The LAN-to-LAN connection has unlimited connection time. This is the default setting.
- Maximum of x minutes
  - The LAN-to-LAN connection has the specified number of minutes to be connected to the 8235 before being automatically disconnected.

Follow these steps to set a maximum connection time:

- Click **Maximum of x minutes**.
- Enter the maximum access time in minutes. You must enter a whole number (that is, 1, 5, 60, and so on). The default is 0.

If you do not enter a number of minutes or if you enter 0 in this field, no maximum time is set and the duration of the LAN-to-LAN connection is not limited.

Note: You can configure maximum connection time in the destination 8235 for the user who is being used for authentication. Display the User List in the Connect Time group box. If maximum connection time is enabled on both the source and destination 8235s, the server with the shorter interval specified is used.

9.6 Practical Experience with LAN-to-LAN Connections

LAN-to-LAN implements routing for IP and IPX and there are some procedures you need to follow when configuring this feature on the 8235. They are actually related to the nature of the routing environment that is defined when using LAN-to-LAN.

In the IPX environment, when we reconfigured an 8235 and left the autosense frame type enabled, it restarted with the IPX network number of the original network. If both networks have the same network number, the 8235 will not route between them and you will will have timeouts occurring in this connection. The solution was to enable specific frame types with the default network locked. It then restarted with a different network number and the routing was possible.

In the IP environment, we have to be careful with this same procedure. Different subnet addresses have to be defined for each side of the LAN-to-LAN connection. Otherwise, the 8235 will not be able to route between the networks.

9.6.1 LAN-to-LAN Summary

- Token-ring or Ethernet
- Router for IP, IPX and AppleTalk
- Configuration and access enabled at 8235
- Performance
  - Similar to remote bridge at 64 kbps
  - 1 file transfer
  - 10 using terminal emulation

  Note: These numbers change significantly with 8235-I40
- Use NetWare Client 32 for Windows 3.1 (GPF with Client 16) when using the LANConnect program
- Can be set up for leased-line connection

Chapter 10. 8235 Security

Security is an increasingly important feature of remote access products. Most of this chapter applies to the dial-in part. Regarding security features, you can split the environment into three different areas:

- The 8235 itself
- The WAN side of the 8235: all components that are connected to the WAN ports, such as modems, the client systems and possible external security devices.
- The LAN side of the 8235: all components that can have a LAN connection with the 8235. In the security context discussed here, these will be security servers.

We discuss the main security features and options available in three groups, as shown in Figure 143:

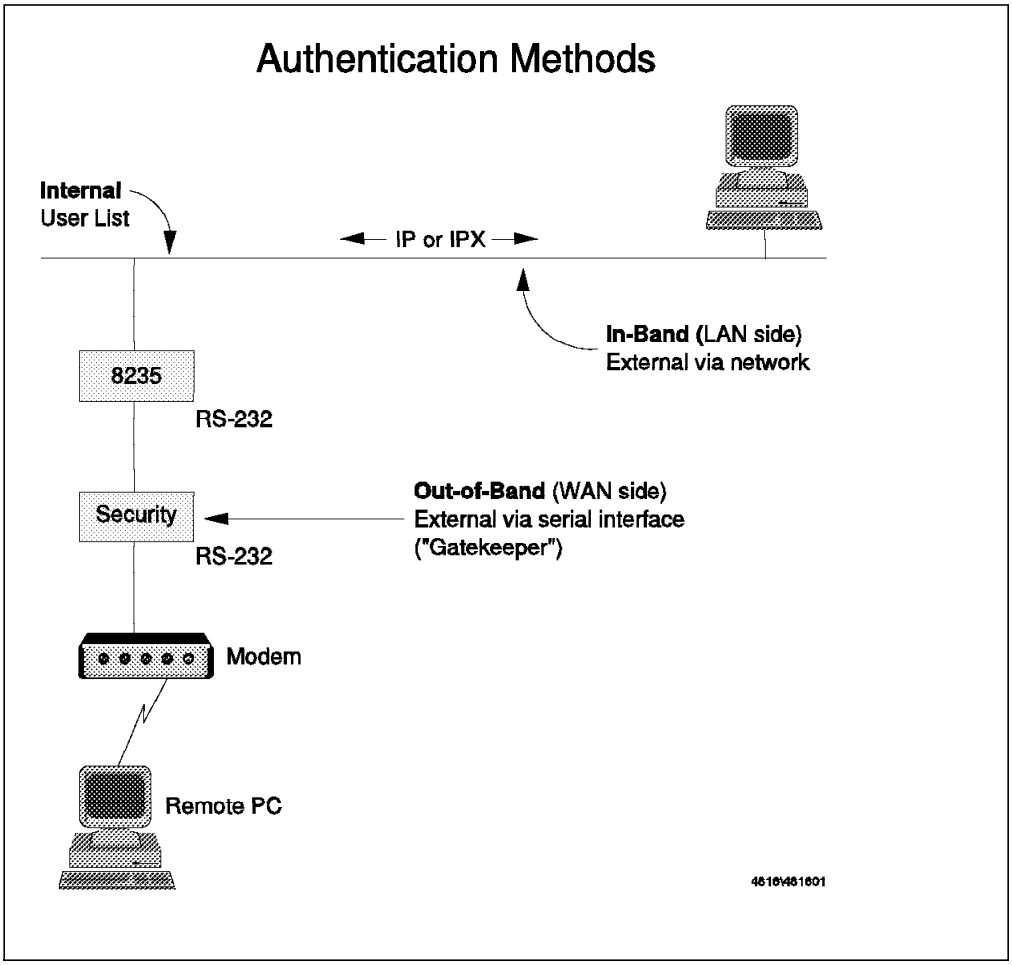


Figure 143. Overview of Security Options

- 8235 built-in security

  This includes user ID and password protection as well as other features.
- The WAN side

This is also referred to as out-band. We cover the *Gatekeeper* devices that have been tested with the 8235.

- The LAN side

  This is also referred to as in-band. We cover the six supported third-party methods.

This discussion includes options built into the product, external options with explicit support within the range of 8235 components, and *black-box* external options of which the 8235 is not aware.

A basic aspect, sometimes underestimated, is *physical access* to the device. We generally recommend that you protect the 8235 physically at your location; you can do so by placing the device in a secure room or cabinet that can maintain the correct operating environment. This is not only for security reasons, but also to ensure uninterrupted operation.

As users do not need access to the physical device during routine work, placing the device in a secure, out-of-the-way location should not cause any inconvenience. Furthermore, the device can be administered from any location through the IPX or IP protocols, or through a dial-in or LAN-to-LAN connection. Only during initial installation and in case of maintenance should physical access to the device be necessary.

The ultimate goal of the 8235's security architecture on the LAN side is to allow any security server on the LAN to be used by any user requiring authentication, regardless of what protocol the user is using; for example, an ARA Version 2.0 dial-in user can be authenticated via the NetWare Bindery. You can choose any centralized security method and use that method for all authentications.

10.1 Security Options on WAN Side of 8235

This section includes two areas that are closely related:

- The DIALs clients themselves, their configuration options and how they support third-party components
- The third-party security devices that have been tested with the 8235 and the DIALs clients and possible special considerations that apply

10.1.1 DIALs Client Security

The security features of the 8235 product are mainly carried out by the 8235 box itself and additional external security servers on the LAN. There is not much a DIALs client can do to improve its own security by itself, given the fact that a potential intruder can steal the machine on which the DIALs client is running. A simple, but important feature is that the client does not store its password. If a configuration file is stored while the password field is filled in, the password will not be stored.

Any other security feature needs to be outside the client by the very nature of the problem. However, the client has to support those external security options. Here is how it works.

10.1.1.1 Third-Party Security Feature

The DIALs client has a feature to provide support for entering third-party security information using a terminal interface.

If you are calling an 8235 that uses a third-party security device, you need to enter the security information (in addition to your dial-in name and password) when you connect to the remote network. For this to be possible you need to be able to enter a dialog mode, receiving prompts and typing answers. To configure the DIALs client (applies to DOS, Windows and OS/2 version) for this, do the following:

1. On the main DIALs Client Connect window select the **Options** button to get the Connection File Options window.
2. Select **Third-Party Security Device Installed**. Depending on whether you see what you type or not, enable the **Echo Characters locally** check box.

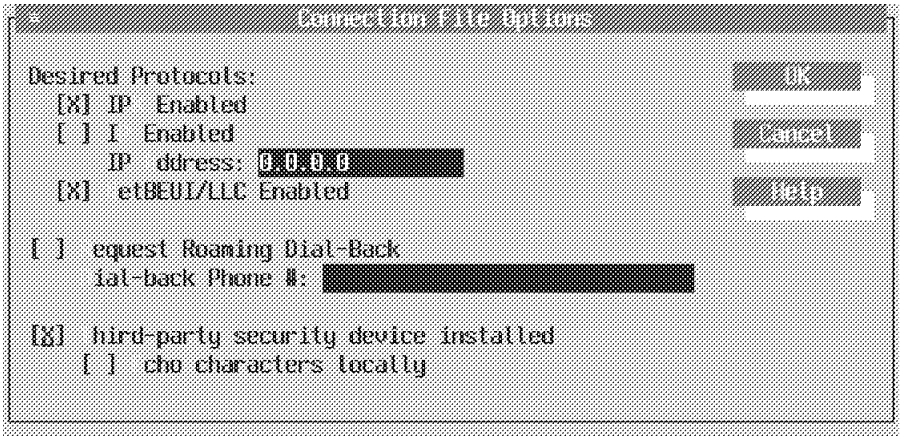


Figure 144. Connection File Options (DOS). For OS/2 Connection File Options, compare Figure 166 on page 243.

3. When you use these settings to dial in, the DIALs client will open an interactive terminal window for you to communicate with the security device, once the modems have connected. This is named the Third-Party Security window.

   Note: If this does not work under DOS (as it did not in our test) use the manual dialing option of the DOS client instead.

4. The dialog that follows depends on the security device being used. Follow the instructions that appear to enter the required security information.

   Note: You may have to press Enter twice or more times in order to get the prompt from that device. Do this if no prompt appears.

5. When you have completed entering the security information, click on **Continue** to continue establishing the dial-in connection. (In the case of the DIALs Client for DOS, press F10 to continue.) The DIALs Client takes over and continues the dial-in process.

10.1.1.2 Automating Third-Party Security

The DIALs Client can enter third-party security information for you automatically, either when you press certain function keys or when the third-party security phase begins.

Note: Although the DIALs Client can send any text string to the third-party security device, this is not a general-purpose scripting tool. This feature cannot interpret the messages sent by the security device in any way.

To set up automatic third-party security responses:

- Open the connection file with any text editor or word processing program as long as you save the file as an ASCII (plain text) file when you have completed your updates. Connection files have an .IR extension (as in DIALIN.IR) and are generally stored in your \DIALS directory.
- Find the [SECURITY] section of the dial-in connection file and add any of the following information.

  ```
  [SECURITY]
  SecurityDevice=Yes
  SecurityEcho=No
  F7=This text is sent when the F7 key is pressed\13
  F8=This text is sent when the F8 key is pressed\13
  AutoSend=This text is sent automatically when security starts\13
  ```

  You can set the first two options (SecurityDevice and SecurityEcho) in the Connection File Options dialog box in the DIALs Client Connect program. The lines beginning with F7=, F8=, and AutoSend= should be added to the connection file manually. The text following F7 and F8 is sent to the third-party security device whenever you press those function keys on your keyboard. The text following AutoSend is sent automatically when the third-party security phase of establishing a dial-in connection begins.

  The following list describes the rules for automating third-party security entries:

  - You can include any character in the automatic text string by entering a backward slash (\) and the decimal ASCII code for that character. For example, adding \13 to the text string sends a carriage return (Return or Enter). Other common values are \10 for a line feed and \9 for a Tab character.
  - Add a backward slash followed by a comma (as in \,) to tell the DIALs Client to pause for one-half second before sending additional information. Entering four commas (as in \,,,,) would tell the DIALs Client to pause for two seconds.
  - Send a backward slash followed by an exclamation point (as in \!) to tell the DIALs Client that the third-party security phase is complete, just as if you had clicked on the Continue button if you were entering this information manually.
- When you have finished entering information in the [SECURITY] section, save and close the dial-in connection file. Be sure to save the file as an ASCII text file.

Note: If you experience problems with this feature and the OS/2 DIALs client 4.0, obtain an updated version of that client. The version shipped originally does not carry out the Autosend and pressing F7 or F8 doesn't work; only Ctrl+F7 and

Ctrl+F8 work with that version. In addition, it does not carry out the , pause, but terminates the string instead.

10.1.1.3 Advanced Security Dialog

This is a feature of the DIALs client for Windows *only* and OS/2.

If you are calling an 8235 that uses a supported third-party security device (such as SecurID from Security Dynamics, Inc.) that is able to use the Advanced Security dialog box in the DIALs Client, you will need to enter the security information (in addition to your dial-in name and password) when you connect to the remote network. To use the Advanced Security dialog box, make sure that both of the following conditions are true:

- The 8235 is Version 4.0 (or later) and is configured to use Advanced Security.
- The DIALs client is also at Version 4.0, at least.
- You did *not* select the Third-Party Security Device Installed check box in the Connection File Options dialog box.

If you are dialing in to an 8235 earlier than Version 4.0, you must select the **Third-party security device installed** check box. In this case, you will not see the Advanced Security dialog box when you dial in; instead, you will see the Third-Party Security window.

To enter third-party security information in the Advanced Security dialog box:

1. Use the DIALs Client Connect program to establish a connection with the 8235.

   When the 8235 modem answers and negotiates a connection with your modem, the Advanced Security dialog box appears. The name and appearance of this dialog box vary depending on which security device is in use and how it is configured. For example, this dialog might appear with a Digital Pathways security device installed:

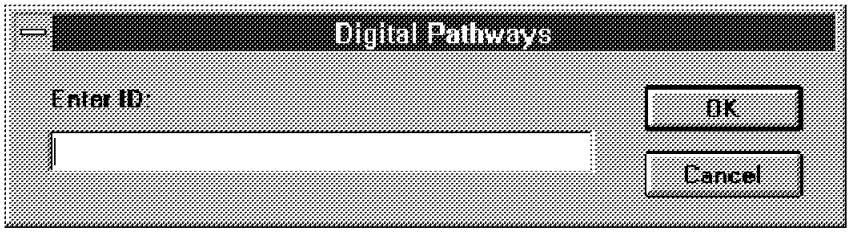


Figure 145. Enhanced Security Dialog

2. Follow the instructions that appear in the dialog box to enter the required security information.
3. When you have completed entering your information, the DIALs Client takes over and continues with the dial-in connection.

The advanced security dialog support in the client is generic from the client's perspective. All it does is process a *dialog box script* sent by the 8235 by displaying the requested dialog box (title bar and 1-3 entry fields with prompts), waiting for the user response, and then sending the response back to the 8235. The client does not care about the contents of the fields, it only passes it on. The benefit of this approach is that there will not be any changes needed in the client when a future release of the 8235 will support more external security servers.

Note: In another example, the TACACS+ server called Blockade for IBM 8235, described in “Configuring and Using Blockade Authentication” on page 241, there is no dialog at all. Everything is handled automatically by the DIALs Client. This is because the information is static, including only the user ID and password. These can be extracted from the respective Connect window fields.

10.1.2 External WAN Security Devices

There are two manufacturer′s devices that have been tested to work with the 8235. Others may well work, too. The concept of these products, as shown in Figure 143 on page 215, is to be transparent and invisible for both client and 8235, once the authentication is done. The two products tested are:

- Security Dynamics ACM
- Digital Pathways′ Defender 5000

These devices work with the same token devices as their software LAN side counterparts, the Security Dynamics ACE server (see 10.3.2.1, “SecurID” on page 249) and the Digital Pathways server (10.3.2.2, “Digital Pathways Defender Security Server” on page 251). They differ in terms of number of supported users, number of ports and scaleability. For a general discussion of token devices and two-factor authentication, refer to 10.3.2, “Two-Factor Authentication-Only Solutions” on page 249.

There are pros and cons for this approach:

- Pros
  - Can use other serial service in addition to 8235
  - Strong accounting and management
- Cons
  - Cannot be used with 8235 modem cards
  - Different (yet another) configuration
  - Different troubleshooting
  - Different modem configuration (make sure your modem′s speed is supported)

To overcome the problem of the integrated modems, there is another approach: a device that attaches directly to the telephone line. The modem is then attached to the security device in turn. However, attaching to a public phone line requires homologation, so a product like this might not be available in all countries.

10.2 8235 Built-In Security

The main security feature built in to the 8235 is the user list and its capabilities for both global settings that apply to all users and user-specific profiles with detailed user privilege configurations.

In addition to that, there are several other integrated security features. They are described in 10.2.3, “Other Built-In Security Features” on page 232.

10.2.1 User List

The 8235 and the Management Facility store user information in the 8235 disk-based files called *User Lists*.

When User List security has been configured, the 8235 controls the access of Dial-In, Dial-Out, and LAN-to-LAN users by the means of User Lists. After you download the User List to the 8235, it stores the User List in non-volatile RAM, which means that this information is not lost when you switch the 8235 off.

Note: However, we recommend that you store the user list on your Management Facility′s hard disk prior to sending it to the device. Otherwise, if there is a problem with the 8235 and you cannot continue, you will lose your work. You can always retrieve the list from disk and re-attempt sending it once the problem is removed.

What can you do with a user list?

- Create a new one: Select **File** then **New** from the Management Facility menu bar and you get a dialog box from which you choose **User List**.
- Open a user list file for editing: Select **File** then **Open** from the menu bar and pick the file name you want from the dialog box. The file extension is SMU. If you have recently worked on a user list file, it may still be offered in the Recent File list of the **File** drop-down list.
- Pull the user list from the selected 8235 by selecting **Get User List** from the Security menu.

In all the cases above, you will be able to manipulate the user list in the same way using Management Facility panels. When you are finished, you can:

- Store the user list on your disk by selecting either **Save** or **Save as** from the File menu.
- Send it to the device from which you had previously obtained it or send it to the selected device, if you have just created it. Select **Set User List** from the Security menu.

If you want to remove a user list that has previously been sent to a device, you can select **Clear User List** from the Security menu. These functions allow you to create the same user list for a number of 8235 devices without having to retype every parameter for each box. This is an advantage when you have several 8235s. However, if users are allowed to change their own password, you must be careful not to end up with different passwords on each machine. It is recommended to use centralized user lists in this case.

10.2.1.1 Global Settings

The Management Facility page for user list editing is as shown in Figure 146 on page 222. It has seven buttons on the top. The upper three obviously relate to editing user entries. The **Unlock User** button is explained in the context of the global user list options. The seventh button, not shown in Figure 146 on page 222 is labeled **IP Filters** and is only available in versions 4.5 and above. IP Filtering is detailed in 5.4.3.4, “IP Filtering” on page 94.

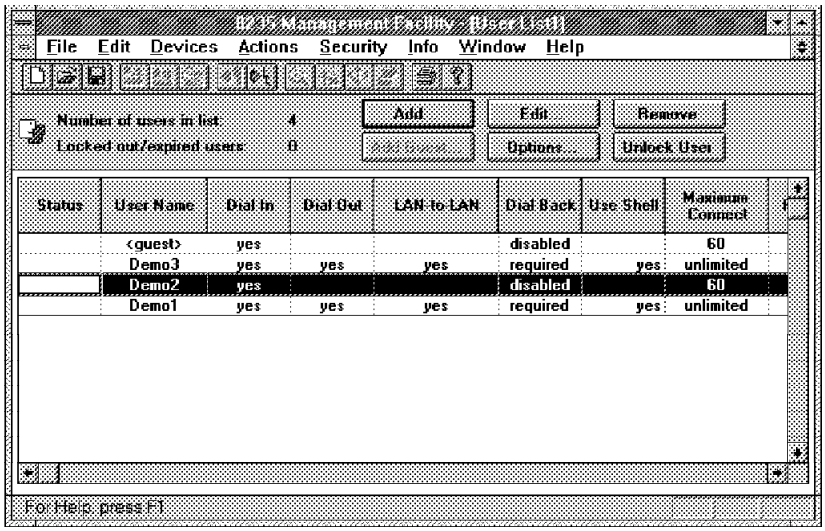


Figure 146. User List with 4 Users Including Guest from v.4.0.2

User List Options: Select the **Options...** button to get to the User List Options dialog box (Figure 147). These settings apply to the entire user list and hence affect all users.

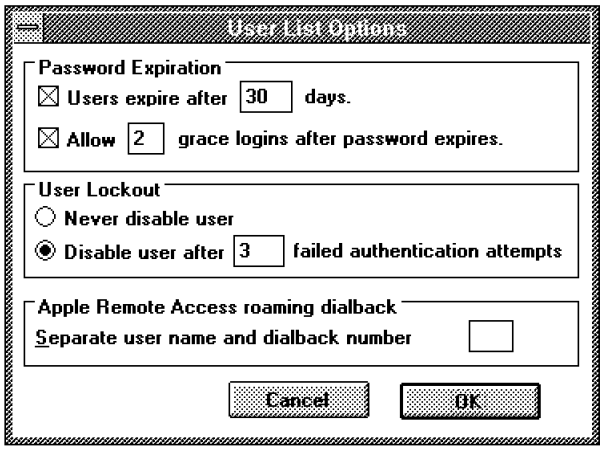


Figure 147. User List Options

There are three groups:

1. The Password Expiration group allows you to control user password expiration and the number of grace logins after a user's password expires. A grace login allows a user to be admitted even though the user's password has expired. However, the correct password is still required for the login to be successful. Login will fail if a wrong password is used. When the limit for grace logins is reached and the user still does not have a valid password, the user will no longer be admitted.

   Note: The user gets a warning message that the password is expired after completion of dial-in, as shown in Figure 148 on page 223. The text of this message is misleading. It refers to the 8235 password, even if NetWare is not used.

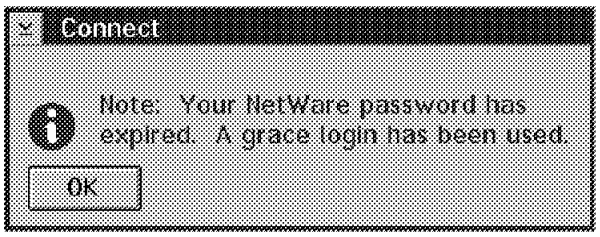


Figure 148. Grace Login Message

The user should then immediately change the password using the Tools menu. The dialog box that will appear (see Figure 149) allows you to set a new password that takes effect immediately.

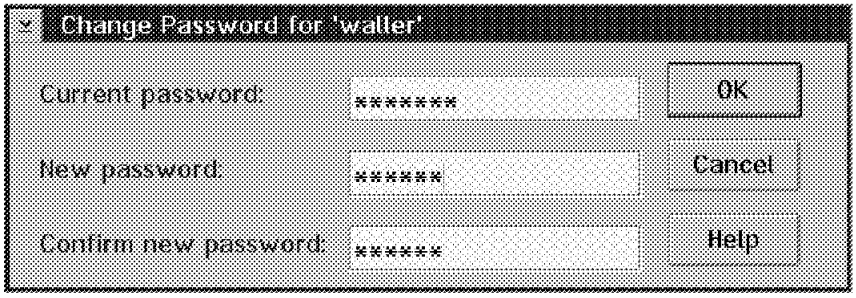


Figure 149. Password Change

In case this attempt fails, an error message as shown in Figure 150 will be displayed.

Note: Change password is only supported by Release 3.5 and later. The user is not allowed to enter an empty password field and thus remove the password. Only the administrator can set up users without a password.

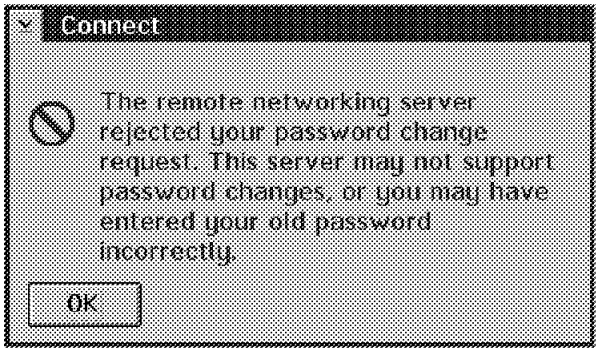


Figure 150. Password Change Error

2. The User Lockout group on the User List Options window allows you to set a limit to the number of attempts to log in with an invalid password. Activation of this limit should be considered to stop hackers that found a valid user ID to automatically test passwords until they find the right one. If the limit is exceeded, the user needs to be manually unlocked by the administrator, by selecting the **Unlock User** button on the user list window. For multiple select you can hold down the Ctrl key while selecting users with the mouse. The unlock applies to all selected user entries.

There is a statistics field counting the number of failed logins per user on the User List window (use the lower scroll bar to shift the user list to the left to see this field). Each time a dial-in user sees the following dialog box (Figure 151 on page 224), this counter is increased by one, but is reset to zero if the correct user ID and password combination is entered. No information is given whether it was the user ID or the password that was wrong. This is done in order to make it more difficult to break in.

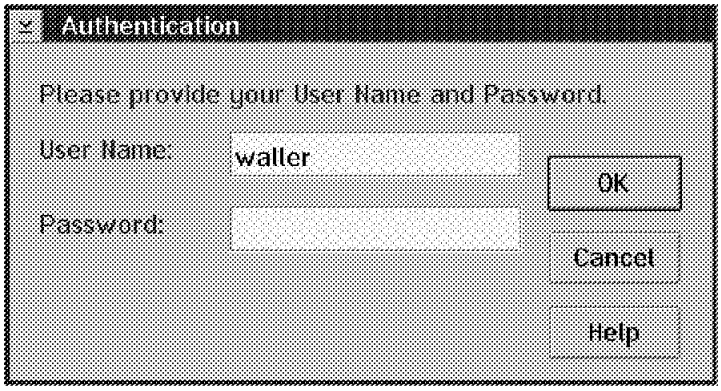


Figure 151. Invalid Login

If you make changes to the User Lockout group, you may get a message as shown in Figure 152. Selecting OK resets the lockout count to zero for all users.

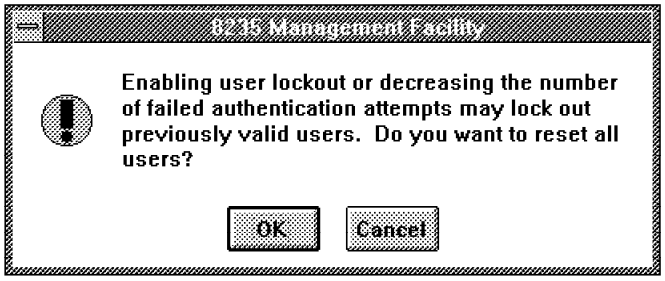


Figure 152. Warning Message Regarding Lockout

3. The Apple Remote Access roaming dial-back group on the User List Options window contains the dial-back delimiter for providing a roaming dial-back number. A roaming dial-back user provides the dial-back number in the Apple Remote Access client application by appending it to the user ID, separated by the character you specify here.

The User Guest: The 8235 provides a special guest account. A guest user does not require a password and has only dial-in privileges. To allow guest access, click on the **Add Guest** button. A Guest entry appears in the User List. This is always the first entry in the User List, and there is no password for the guest user. The only parameter you can alter is the connect time limit (see Figure 153 on page 225). Note that the actual user ID is <guest>, but someone connecting with this user ID would only type **guest** to connect.

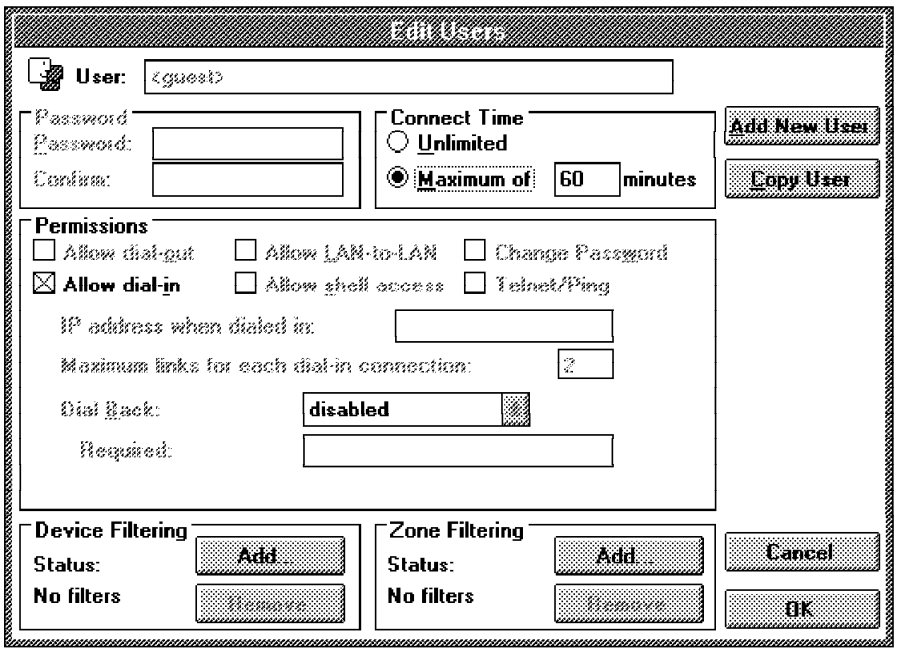


Figure 153. User Guest without Options

10.2.1.2 User Profile

When you edit a selected user (from the user list page, Figure 146 on page 222) or add a new one, you will get the following screen. The user name will be defaulted to <userx>, where x is a number. You can overwrite this with any name you want. You should not use root, supervisor, or <guest>, as these are reserved names.

Note

Multiple users may be logged in with the same user ID at one time. In this case the user ID becomes a user group definition. However, if individual attributes such as IP address and fixed dial-back are used, this is not possible.

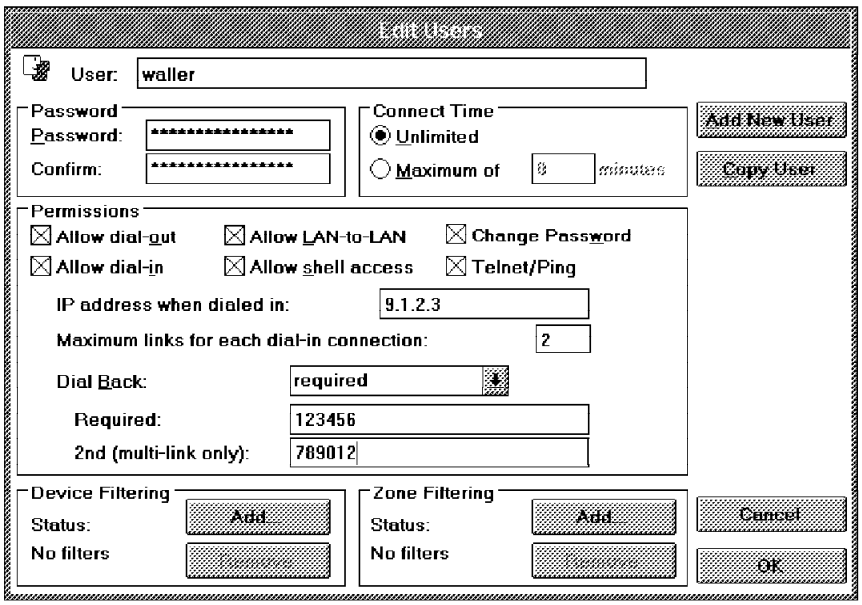


Figure 154. Edit a User Profile

There are five areas on this screen:

- Password
- Connect Time
- Permissions
- Device Filtering (AppleTalk specific)
- Zone Filtering (AppleTalk specific)

Password: The password can be up to 16 characters long. It can be case-sensitive, if so configured (see 10.2.1.3, “Security Options via Additional Configurations Page” on page 229). It can be forced to be mixed case, it can be forced to have a minimum length and it can contain spaces. You may call this a pass-phrase.

When you complete this field, the password is encrypted immediately. You will always see 16 *, no matter what the actual length of the password is. Any storage of the password takes place in encrypted form.

Confirmation of the same password in the Confirm field completes this group of parameters.

Connect Time: User connect time is the amount of time a user can be dialed in during any one session. It is set by the two Connect Time radio buttons. If you allow unlimited connection time, a user who is connected for long periods of time prevents others from using that port. Additionally, an unrestricted user can run up costly telephone charges. We recommend that you set a maximum connection time for all users. If a limit is set, the user will be warned 5 minutes before his connection time expires, so there is ample time to save all work. No further warning will be given; however, after the user is disconnected, a dialog box will appear (Figure 155 on page 227), which allows for easy reconnection.

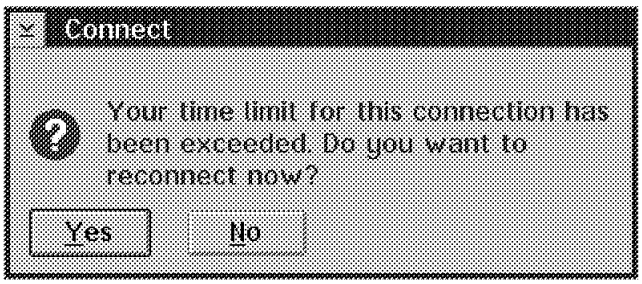


Figure 155. Connection Time Expired

During the entire dial-in session, the remaining connection time will be displayed in the bottom line of the Connect application next to the connected time. In case of unlimited connection time, only the connected time is displayed.

Permissions: Check Boxes: The upper part contains check boxes to individually allow or disallow a particular function for this user. They are:

- Dial-out
- Dial-in
- LAN-to-LAN
- Shell access
- Change password
- Telnet/Ping

1. The *dial-out* feature allows one user at a time to use any one external or built-in modem to connect with bulletin boards, online services, or any other system your communications software lets you access. ISDN BRI cards are currently not supported for dial-out.

   You must enable the dial-out check box on the General configuration and Ports configuration pages for this to be possible.

2. *Dial-in* is the feature to which most of the other permissions in this group relate. This will, in many cases, be the only feature that you want to allow. Dial-in is supported by all interface types of all models of the 8235.

   You must enable dial-in on the General configuration and Ports configuration pages before users can dial in to the 8235.

3. *LAN-to-LAN* privileges allow a user to initiate a LAN-to-LAN routing connection between two 8235s. The user also needs shell access to be able to perform this task.

   Note: You must enable LAN-to-LAN on the General configuration and Ports configuration pages before users are allowed to establish a LAN-to-LAN connection with the 8235. There is a distinction between LAN-to-LAN originate and LAN-to-LAN answer. This distinction, however, does not apply to the user ID, only to the 8235 configuration.

4. You can enable *command shell access* for a user. If you do, that user is allowed to connect to the shell through Telnet or dial-in. The shell is a command line interface providing a limited set of commands (mainly for display) to normal users and full management capability for a user with administrator privileges. Shell access is a prerequisite for LAN-to-LAN connection establishment, because this is done via a shell command.

5. If you enable users for *Change Password*, those users can change their passwords at any time. Passwords are confirmed before they are accepted. If you set a password expiration period, we recommend that no users be prevented from changing their own password. If a user changes a password, no one else, not even the administrator has access to it, because it is stored in encrypted form. However, the administrator can reset the password at any time.

   If users have been given shell access, they can change their passwords using the shell command `passwd`.

6. If you enable a user for *Telnet/Ping*, that user is allowed to issue Ping commands from the 8235 and to establish Telnet sessions. Obviously, shell access is a corequisite for this option.

   Note: Telnet is the only way to communicate via dial-in with the 8235 for users with nonprogrammable terminals.

IP address when dialed in: This field allows you to assign IP addresses on a per-user basis. This is one out of four methods to assign IP addresses. The other methods are:

- Supplied by the user when dialing in (fixed)
- Assigned for a port pool (dynamic)
- Obtained from a DHCP server (dynamic)

For non-administrator users, we recommend not to allow the user to supply the IP address. Consequently, specifying an IP address in the user list is the preferred method for the user to get a fixed IP address. This way the user will not be allowed to use any IP address different from the one given here, and thus cannot disrupt other users′ communication in the network.

If an IP address is not available from any of the four sources, the user can connect to the 8235 but cannot use IP.

Maximum Links for each Dial-In Connection: This number represents the number of ports a user can use for virtual connections and channel aggregation using MLP when dialing in. If you have installed modules that have two channels, such as an ISDN BRI module, each channel can be counted as a port. This value must be either 1 or 2 for dial-in. Only LAN-to-LAN connections can use more than two links.

Dial-Back Drop-Down List: If the dial-back feature is enabled for a dial-in user, after the dial-in user connects to the 8235, the 8235 hangs up and calls the dial-in user back. It is using the telephone number supplied by the user when roaming dial-back is enabled. This dial-back number can also be configured in the User List.

The Dial-back pop-up menu contains three menu selections for using the dial-back feature:

Disabled This selection does not allow the user to be called back.

Roaming This selection allows dial-in users to enter their own dial-back telephone numbers. This feature is useful for reversing the telephone charges for dial-in users who are off-site and seldom at the same telephone number. The dial-back telephone number is typed into the Dial-back Phone number field in the DIALs client′s Connection File Options dialog box at dial time.

Required The telephone number entered in the Dial Back field is dialed back each time the dial-in user connects to the 8235.

Phone Numbers for Fixed Dial-Back: If you have selected **Required** from the drop-down list, the fixed dial-back number must be entered here. If the multilink option is to be used with this user, a second number is required for the additional B channel. It is entered in the second (multilink only) field. This field is valid only when the 8235 has been configured to support an ISDN BRI module.

Note: If your telephone system requires that you dial a prefix number to get an outside line, you can enter this prefix in the Dial-Back Prefix group box of the Configuration for Port x page. This method allows you to have different ports attached to different lines that may require different prefixes. The user does not need to know about the prefix required for the port being used. This prefix may even include the distinction between tone and pulse dialing. There is a subcommand of the modem dial command regarding this, which can be included in the dial prefix. The dial prefix and the user-provided call-back number will be appended (in this order) to an ATD modem command.

10.2.1.3 Security Options via Additional Configurations Page

There are further refinements to the user list concept that cannot be set via the Management Facility′s configuration pages. The purpose of the Additional Configuration page is to accommodate all parameters (not only security) that are not otherwise supported in the graphical interface.

The format of configuration and user files is similar to the Windows INI files. It is made of sections, starting with a section header (coded with square brackets, see the following example) and followed by keyword parameters belonging to this section. A section header can appear several times, the parameters are merged into one section when the file is loaded into the 8235.

```
[Section]
Parameter1=value1
Parameter2=value2
```

Enabling Password Case Sensitivity:

```
[Security]
CaseSensitive=1
```

This makes entered passwords case-sensitive. Even though the administrator password is not stored in the user list with the others, this applies to it as well.

Enforcing a Minimum Password Length:

```
[Security]
MinPasswordLength=4
```

This imposes a minimum password length of four (four is only an example). It does not apply to the administrator password.

Enforcing Mixed Case Passwords:

```
[Security]
ForceMixedCase=1
```

Users have to use a mix of uppercase and lowercase letters if they change their password. This does not apply to the administrator password.

Note: In all of the above cases, the user will get the same reply: The authentication dialog box will be repeated if this was an attempt to log in

(Figure 151 on page 224). If it was an attempt to change the password, the password change dialog box will be displayed again (see Figure 149 on page 223).

Sending a Message at Login (Banner):

```
[Security]
Banner="\nThis is Guenter's Banner message.\nHi there and|
welcome to our 8235!"
BannerRequired=1
```

Note: n forces a new line, and | is the continuation character for any configuration parameter that does not fit into a single line.

The Banner Required=1 parameter defines that nobody is allowed in who is not able to display the banner message. You should not use this parameter if you have DIALs clients for DOS in use; they cannot view banner messages. The DOS client will not be allowed in and a message will be written to the log. On the other hand, command shell sessions are able to receive banner messages.

A banner being displayed looks like this:

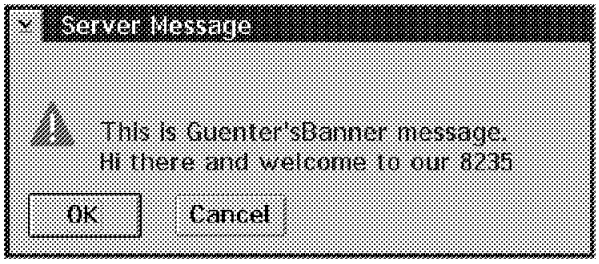


Figure 156. Banner Message

10.2.2 Configuring Internal User List and User List Server

Now that you know what the user list is and how it can be used to enable an enormous range of functions and options, you will see here how the 8235 is configured to utilize it.

10.2.2.1 Internal User List

On the Security Configuration page, you simply click on the **Internal User List** radio button. The right part of the User Authentication Area will turn into a configuration area as shown in Figure 157 on page 231. If this is the only 8235 you have at this time, you are finished.

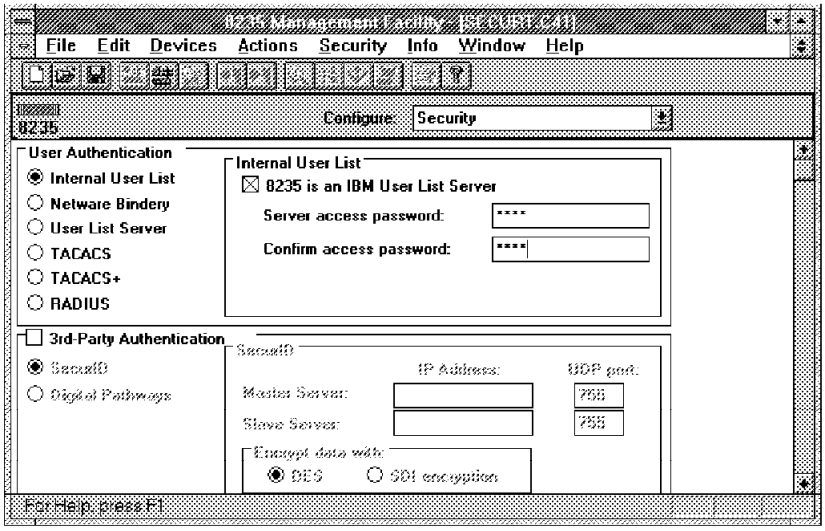


Figure 157. Security Page

If you have other 8235s in your network that are supposed to use this one as a user list server, you must enable the check box in the Internal User List area. Furthermore, you must have enabled the IP protocol on both machines. IP will be used as the communication protocol to validate user logins.

Optionally you can set a password here. If you do, this password will be required for any other 8235 trying to utilize this 8235 for authentication of its users.

When you save this configuration you have set up a user list server. The next section describes how you set up other 8235s to use this server as their external authorization method.

10.2.2.2 User List Server Access

To set up an 8235 for user authorization through a centralized 8235 user list server, you select the **User List Server** radio button on the Security page. The right part of the User Authentication Area will turn into a configuration area as shown in Figure 158. The area heading text is misleading. It is not *this* 8235 that is a user list server; it is the one with the IP address specified here.

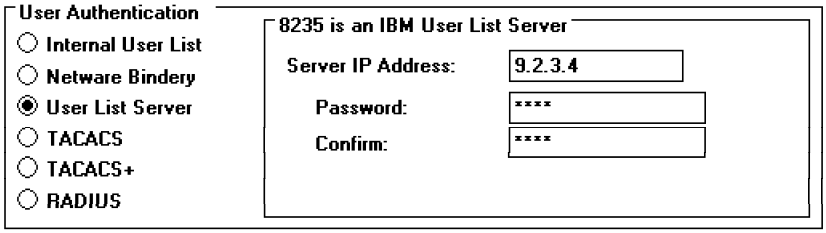


Figure 158. Security Page

The password must match the one defined on the user list server (if any). For maximum protection we recommend that you use a password.

The benefits of using a user list server are as follows:

- If you have large user lists, they fill up memory in the 8235. Having only one box with this burden frees the others of possible memory constraints. So you

either get better performance or avoid having to purchase extra memory for all machines.

- If you have more than one 8235 and you want to enable your users to change their passwords, using a single user list server will ensure a coherent user list database.

There is, however, one drawback. A single user list server is a single point of failure in the sense that manual action by a system administrator is required if that server fails. Another 8235 must be loaded with the user list (which should be saved regularly if users are allowed to change their own passwords) and set up as a user list server. If possible it should get the same IP address as the failing one; otherwise, all other 8235s in the network must have the IP address parameter for their user list server changed to the new value.

To overcome this situation there is a shell parameter allowing the definition of up to three user list servers. The following two examples show:

- A single user list server with encrypted password. This was done by the Management Facility.

  ```
  [Security]
  ShivaServer=9.1.2.3,kloLwOnx67C62ih.*cnPMg*xpS
  ```

- Three user list servers without any passwords. This was done via the Additional Configuration page.

  ```
  [Security]
  ShivaServer=9.3.4.5;9.4.5.6;9.5.6.7
  ```

In order to have both password protection and backup servers at the same time, you will have to define one server at a time on the security page, save the configuration file on your disk, do the same for each of the other servers and merge the computed passwords manually with an ASCII editor. The format for this is as follows:

```
ShivaServer=IPaddr,password;IPaddr2,password2;IPaddr3,password3
```

This is not guaranteed to solve all problems. In particular, if users change their own passwords, you are back to the problem of coherence. However, multiple user list servers should be considered as an option to increase availability during an unattended period.

10.2.3 Other Built-In Security Features

The ordinary user passwords are stored in the user list. However, there is password information in the configuration file as well. This chapter tells you where. The general rule is that no password is ever stored without encryption.

10.2.3.1 The Administrator Password, Shell Access

We strongly recommend that you assign a non-trivial administrator password to each 8235. Otherwise, an unauthorized person can reconfigure it. For a dial-in box like the 8235, this is even more important than for other devices, because it accepts switched connections.

Note: The password is not stored in the user list, but in the device configuration.

This password is required for any attempt, not only to reconfigure the device or the user list, but also to obtain information such as statistics, log file or port status. Furthermore, port and connection management functions require this password.

Note: The password is the same one that is used to authenticate the root user in the command shell. This shell user has the same privileges as an administrator using the Management Facility. An ordinary shell user (with non-administrator privileges) can obtain administrator privileges by typing the shell command `enable`. The user will be prompted for the administrator password. After completion of this command, the last character of the prompt will have changed from > to #.

Note: When you receive your new 8235 (or do a pin reset), there is no administrator password. On the other hand, if you have configured a password and do not remember it, you need to do a pin reset to recover from this dead-lock situation. Any configuration and user list changes since the last save of those files will be lost.

Assigning an administrator password to the 8235: To assign an administrator password to a device, perform the following steps:

1. From the Device List window, select the device to which you want to assign a password.
2. Select **Set Administrator Password** from the Security menu. The Set Administrator dialog box appears.
3. If there is an administrator password already configured in the particular device, type it in the Current Password field. If there is no password assigned to the device, type the new password in the New Password field. The password can be up to 16 characters long.

   Note: For security reasons, the password is masked as you enter it. An asterisk replaces each character you type. Passwords are currently case-insensitive.
4. Because the typed password does not appear on the screen, you have to confirm it.

   If you do not type it in the Confirm field exactly the same way, it will not be changed; the Management Facility will display an error message instead.

   The administrator password is assigned to the 8235 once you click **OK**. The change takes effect immediately.
5. To remove a password that you have set before, follow the same steps as above; however, leave the New Password and Confirm fields empty.

10.2.3.2 Security Features Specific to Configuration Options

LAN-to-LAN: For the establishment of LAN-to-LAN connections, a user ID-based process is used. A user ID authorized for LAN-to-LAN is required on the local side, and a user ID authorized for LAN-to-LAN is required on the remote side (see 10.2.1, “User List” on page 221). However, this process requires storage of user ID and password information in the configuration (site definition) in addition to the respective user list.

AppleTalk: If AppleTalk is enabled, device and zone filtering can be used effectively to limit access to certain parts of the network for particular ARA clients or groups.

Token-Ring: If bridged protocols are used on token-ring, a parameter can be set in the Additional Configurations page to the effect that source route bridging is deactivated in the 8235. The 8235 then only bridges these protocols from the

dial-up line into the segment to which it is attached. NetBIOS and LLC 802.2 access now is limited to that ring.

Note: This parameter exists because there are token-ring networks that do not employ source route bridging. In those cases the 8235 needs to be able to turn it off. The security aspect is a side effect.

The parameter is coded like this:

```
[Token_Ring:SR]
Enabled=0
```

10.3 External LAN Security Devices

8235 Version 4.0 or later directly supports six third-party authentication databases:

- NetWare Bindery
- TACACS server
- TACACS+ server
- RADIUS server
- Security Dynamics ACE server
- Digital Pathways Defender server

The Bindery as well as the 8235 user lists can store a full user profile. RADIUS is also capable of full authorization. TACACS and TACACS+ support can work with a generic user profile that applies to all users being authorized by these methods.

SecurID and Defender, however, validate only the user identity; they cannot supply a profile for the user. Their additional benefit is that they require a token to be provided by the user in addition to user ID and password. This token (a character string) is obtained from a token device in possession of the person owning the user ID.

The way to think about such a security design is that SecurID is used to *authenticate* users; the other databases are used to both *authenticate users and to authorize access* to the 8235's services. The same applies respectively to Defender Server.

The token methods are used in conjunction with any one of the authorization methods. For example, you can use SecurID to authenticate users and the NetWare Bindery to set up departmental access privileges for groups of users. The 8235 then prompts separately for the user name and password for each method of authentication; this allows you to use some forms of authentication for group authorizations (for example, SecurID authenticates the individual, who then logs in to the Bindery with a user ID of *Sales* to obtain Sales group permissions).

Note: If an 8235 is configured to use external security and cannot access the external security server when a user dials in, then the authentication fails, and the 8235 denies service to the user. For this reason, it is advisable, if possible, to have back-up security servers available to avoid a single point of failure.

10.3.1 Servers Providing Authentication and Authorization

The following methods are mutually exclusive. The activation of any of them also excludes the activation of both internal user lists and the user list server. However, there may still be an internal user list to provide global settings for the chosen method via a special generic user ID.

You can choose and configure all those methods on the User Authentication Area (upper part) of the Security Configuration page, which appears when you choose **Security** on the Configure drop-down list. When you select the respective radio button, the right part of this area will turn into a configuration area for the selected method.

10.3.1.1 NetWare Bindery

Note

The 8235 has Bindery Services support only for NetWare 3.x, not for 4.x. The corresponding service offered by NetWare 4.x, NDS (NetWare Directory Service) is currently not supported by the 8235.

Do *not* attempt to use NetWare 4.x Bindery emulation instead. It is not supported; it does not work. The reason for this is the fact that Bindery emulation does not support the slash-commands (see Table 26 on page 237) used by the 8235 to store user profile information that otherwise would go into the internal user list.

NetWare Bindery is a database that resides on a NetWare network server in the network and communicates with an 8235 over IPX. This database contains profiles of users of the network. These profiles define each user's name, password, dial-back number, and permission to use one or more 8235 functions (Dial-In, Dial-Out, and LAN-to-LAN).

Configure Bindery on the 8235: Once you have enabled Bindery, the security page will look as shown in Figure 159.

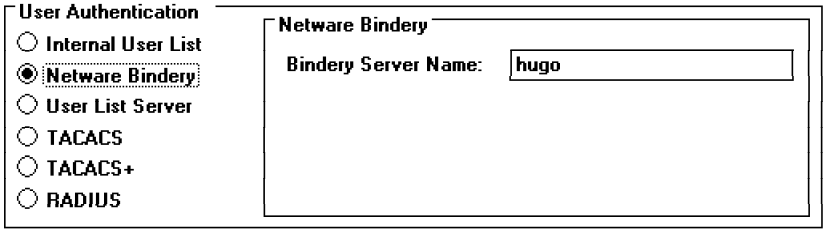


Figure 159. NetWare Bindery

Now enter the name of the NetWare Bindery server in the Bindery server name field. This completes the part on the 8235 side. You can now save the configuration and/or send it to the device.

Using Bindery Services: You must initially use the Management Facility to use the Bindery Services Utility because it creates the groups that you need. To edit Bindery items later, you can use the Bindery Services Utility on any PC or Novell NetWare for Macintosh tools on a Macintosh.

Follow these steps to create Bindery user groups for your NetWare Bindery database authentication. Users in these groups have dial-in, dial-out, and

LAN-to-LAN privileges, respectively. Users can be assigned to more than one group. To create these groups, you need a user with Supervisor privileges on that server.

1. Choose **Bindery** from the Security menu. The Bindery Services window appears.

   Note: In order for Bindery to become selectable from that menu, you need to have loaded the NetWare command shell beforehand.

2. Select the Bindery server that you want from the Servers drop-down list. If you have not logged in to the server yet, a Login dialog box appears. Enter your user name and password in the fields provided and click on **OK**. The names of all users who have accounts on that server appear.

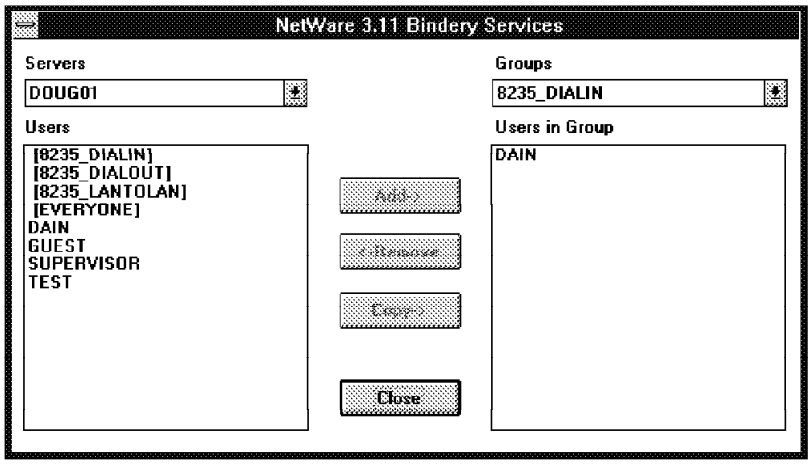


Figure 160. Bindery Services Utility

3. Select the 8235_DIALIN, 8235_DIALOUT, or 8235_LANTOLAN group from the Groups drop-down list. If this is the first time you invoke this function with this server, those groups have just been created for you. Otherwise, a list of users already in that group may appear.
4. To add users to the group, select the user names you want to add and then click on **Add** or **Copy**. The selected names appear in the Users in Group list.
5. To remove users from the group, select the user names you want to remove and then click on **Remove**. The selected names have been deleted from the Users in Group list. Repeat the previous three steps until all required Bindery groups have been defined.
6. To enable the dial-back feature or specify additional permissions for any user, double-click on the user's name. The Dial-Back dialog box appears.
7. To require fixed dial-back for the user, enable the Yes check box and enter a telephone number in the Dial-Back Phone Number field.
8. Enable the No check box if you do not want to require fixed dial-back for this user.
9. If you do not enter a dial-back number in the Dial-Back Phone Number field, you can use this field to specify permissions for the user (see Table 26 on page 237 for possible options).

   Note: The first character of each command must be a slash (/) for the 8235 to interpret the dial-back parameters as a user configuration. There is no

method of verifying those commands. If an entry contains an error, the bindery database will accept it. This may cause problems during user login.

10. Click on **OK** to save your changes.
11. Select **Close** to close the Dial-Back dialog box.

Table 26. User Configuration Parameters. Compare with Figure 154 on page 226.

Parameter	Description
/max=<number>	Limits user connection time to <number> minutes. Does not apply to dial-out or LAN-to-LAN connections. Zero means unlimited.
/do	Dial-out
/di	Dial-in
/rt	Remote routing (LAN-to-LAN). Requires the /max command as well.
/sh	Enables command shell access (required to initiate LAN-to-LAN connections).
/pw	Gives you the ability to change your own password.
/tp	User may use telnet and ping shell commands.
/ip=<IP address>	User-specific IP address
/ml=number	Sets the maximum number of links the user can use during dial-in connections. The valid values are 1 or 2.
/fd	Dial-back required. Requires the /db command as well.
/db=<telephone number>	Sets user's stored dial-back telephone number.
/db2=number	Sets user's second stored dial-back number (single-users dial-in only) for multilink.
/rd	Enables roaming dial-back to the number provided on dial-in.
/cf	Allows user to change configuration via shell.

Note: The first character in the dial-back field must be a slash (/) for the 8235 to interpret the dial-back parameter as a user configuration.

10.3.1.2 TACACS

The Terminal Access Controller Access Control System (TACACS) is a security protocol used to communicate between 8235s and an IP authentication database. It is based on UDP.

An 8235 functions as a proxy TACACS client for dial-in users. It forwards the user's ID and password to a centralized database that also has the TACACS protocol. The centralized database looks up the information and sends back an accept or deny message, which either allows or denies the user access. This process is entirely transparent to the dial-in user.

Note: Although TACACS runs over IP, the dial-in user need not be using IP to be authenticated by an 8235 using TACACS. However, a 8235 using TACACS must have IP enabled. For more information about TACACS, refer to RFC 1492, *An Access Control Protocol, Sometimes Called TACACS*. TACACS and other remote access security protocols are designed to support thousands of remote connections. In a large network, the user database is usually large, and is best kept on a centralized server.

Note: The centralized server can either be a TACACS database or a database like the UNIX password file /etc/passwd with TACACS protocol support. For

example, the UNIX server with TACACS passes requests to the UNIX database and sends the accept or reject message back to the access server.

In *extended TACACS,* enhancements were made to support new and advanced features:

- Multiple TACACS servers.
- *syslog* - sends accounting information to a UNIX host.
- *connect* - the user is authenticated into the access server shell and can Telnet or initiate SLIP or PPP or ARA.

Extended TACACS is multiprotocol-capable and can authorize connections with:

- SLIP
- Enable
- PPP (IP or IPX)
- ARA
- EXEC
- Telnet

Configure TACACS on the 8235: TACACS is enabled by selecting the **TACACS** radio button in the User Authentication group of the security configuration page. The TACACS dialog box appears to the right.

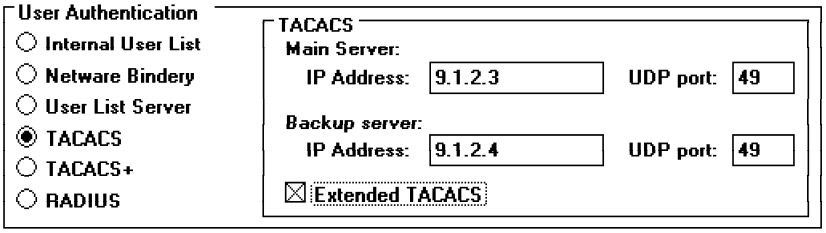


Figure 161. TACACS Configuration

Type the IP address of your main TACACS server and the UDP port number for this server. If that has been changed on the server, use the correct value. Otherwise, accept the port 49 default.

Follow the same steps for the backup server if you have one.

The default TACACS type is simple TACACS. If, instead, you are using Extended TACACS, enable the **Extended TACACS** check box.

Changing the User Profile for TACACS Users: The default user profile for all TACACS users allows dial-in, dial-out, shell access, and unlimited connect time. If you need to change this profile, create a user with the desired profile and the name TACACS in your user list. This user profile will override the default TACACS profile.

Note: The TACACS protocol does not support the Change Password function.

LAN-to-LAN and roaming dial-back are supported in the TACACS user profile. (LTL is on by default.) Required dial-back is not supported since this is a global profile for all users being authenticated via TACACS. The same applies to user-specific IP address. To revert to the default values, delete the TACACS user from the device′s user list.

As an alternative you can modify the TACACS permissions through the Additional Configuration page. The command line for the default setting is:

```
[Security]
TACACSUser=/di/do/sh
```

For a complete list of options refer to Table 26 on page 237 and keep in mind the above-mentioned restrictions.

Note: The changes that you make to the TACACSUser line apply to all TACACS and TACACS+ users.

10.3.1.3 TACACS+, BLOCKADE

TACACS+ is a completely new version of the TACACS protocol referenced by RFC 1492. It is currently studied by the IETF in order to become an RFC. It is based on TCP as opposed to UDP to increase security and reliability. We describe here the potential of this protocol. This does not imply that every implementation is using all those functions; in particular, the 8235 currently uses the authentication part only. This may change, once an RFC exists.

TACACS+ General Description: TACACS+ has three major components: the protocol support within the access servers and routers, the protocol specification, and the centralized security database. Similar to an internal security database, TACACS+ supports the following three required features of a security system, which are three separate protocol components, each of which can be implemented on separate servers:

- Authentication
  - Login and password query
  - Challenge/response (CHAP)
  - Messaging support (any)
  - Encrypted in MD5
  - Replaceable with Kerberos 5
- Authorization
  - One authentication
  - Authorization for each service
  - Per-user access list and user profile
  - Users can belong to groups
  - IP and Telnet support (IPX, ARA future)
  - Any access or command and permission or restrictions
- Accounting

  TACACS+ provides accounting information to a database through TCP to ensure a more secure and complete accounting log. The accounting portion of the TACACS+ protocol contains the network address of the user, the user name, the service attempted, protocol used, time and date, and the packet-filter module originating the log. For Telnet connections, it also contains source and destination port, action carried (communication accepted, rejected), log, and alert type. Formats are open and configurable.

  The billing information includes connect time, user ID, location connected from, start time, and stop time. It identifies the protocol that the user is using and may contain commands being run.

TACACS+ and the 8235: The following features are supported for TACACS+ servers:

- Authentication through the TACACS+ server when a user logs in to an 8235.
- Challenge/Response dialogs are transmitted to the TACACS+ server by the 8235 if the TACACS+ server is configured for challenge/response.
- Data encryption of TACACS+ packets sent over the network.

Note: Since the authorization capabilities of TACACS+ are not used currently, all users are given the same user privileges. These privileges can be modified through a generic user profile TACACS or through the Additional Configuration page. See “Changing the User Profile for TACACS Users” on page 238 for more information. There is only one generic user ID TACACS that applies to both TACACS and TACACS+.

Configure TACACS+ on the 8235: Select **TACACS+** from the User Authentication group. The TACACS+ dialog box appears.

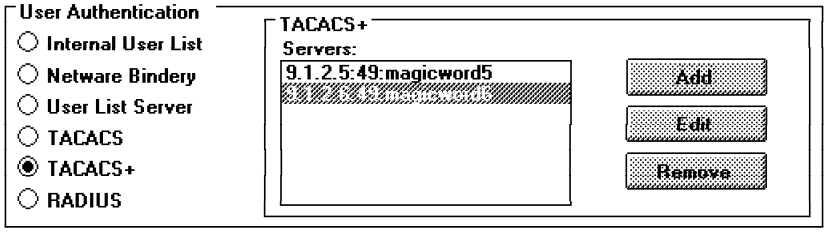


Figure 162. TACACS+ Configuration Area

Click on **Add** to enter the address, port, and security information. The Add a TACACS+ Server dialog box appears.

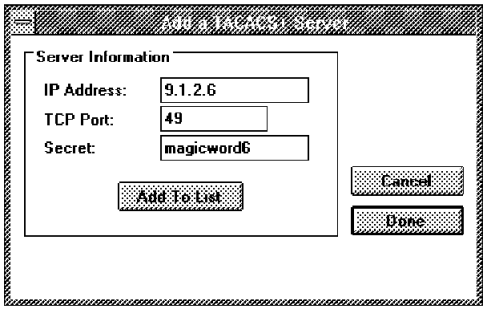


Figure 163. Add a TACACS+ Server Dialog Box

Enter the IP address of your TACACS+ server and the TCP port number, or accept the default of port 49. This is the port that the TACACS+ server uses to communicate. Enter the secret key (1 to 10 alphanumeric characters) in the Secret field. This is the key that the TACACS+ server and the 8235 use to encrypt data packets. This must match the key that was configured in the TACACS+ server. Click on **Add to List** to add the information to the TACACS Plus area of the Security page. You can define a list of TACACS+ servers, currently up to three.

A Sample TACACS+ Server: Blockade: An example for a TACACS+ server that has been tested with the 8235 is “Blockade for IBM 8235.” There are four systems along with their respective components involved in the authentication (currently authentication is the only supported feature):

1. The DIALs client, attempting to log in.
2. The 8235, configured with TACACS+ as external security device.
3. An OS/2 system, having IP connectivity with the 8235, running the Blockade for IBM 8235 software. This is the TACACS+ server to be specified in the 8235. Within the Blockade terminology this is a called a Distributed Third-party Authentication Server (DAS).
4. An MVS system with RACF (other supported options: ACF2, Top Secret), running the Blockade Enterprise Security Server (ESS), which acts as a link between RACF and the DAS. Note that the VM platform is not supported by this product.

Blockade for IBM 8235 enhances the functionality of the IBM remote access server by providing centralized administration, extended user authentication and enhanced logging and auditability. All security management is centralized on the MVS platform using RACF. Blockade for IBM 8235 operates as a DAS that communicates with the IBM 8235. The Blockade for IBM 8235 DAS in turn communicates with the Blockade ESS residing on the MVS platform. When a user attempts to connect to the LAN using the IBM 8235, the Blockade DAS collects the necessary identification information (this may be user ID and password, user ID/password/dynamic token information, etc.). It then passes the information to the ESS for authentication against user profile information stored in the RACF database.

There is no technical limit to the number of 8235s supported by one DAS.

Blockade for IBM 8235 supports all leading token devices for extended user authentication. All support is provided by the ESS without requiring any additional hardware or software. Token device manufacturers explicitly listed by Blockade are Security Dynamics, Digital Pathways and CRYPTOCard. For more details on token devices, see 10.3.2, “Two-Factor Authentication-Only Solutions” on page 249.

The bottom line is that control of remote LAN access is centralized around an existing mainframe security product. As an additional benefit, you get remote LAN access audit records written to SMF.

Configuring and Using Blockade Authentication

1. On the DIALs Client, you have two different scenarios:
   a. The DIALs Client 4.0 and higher is capable of extracting the user ID and password information from the respective fields in the Connect dialog box. To enable this, do *not* enable **Third party security device installed**. Enter your host user ID and password as if they were in the 8235 user list. Make all other selections as usual and click on **Connect**. If the authentication is successful, there will not be any other dialog steps. You will get the following message box:

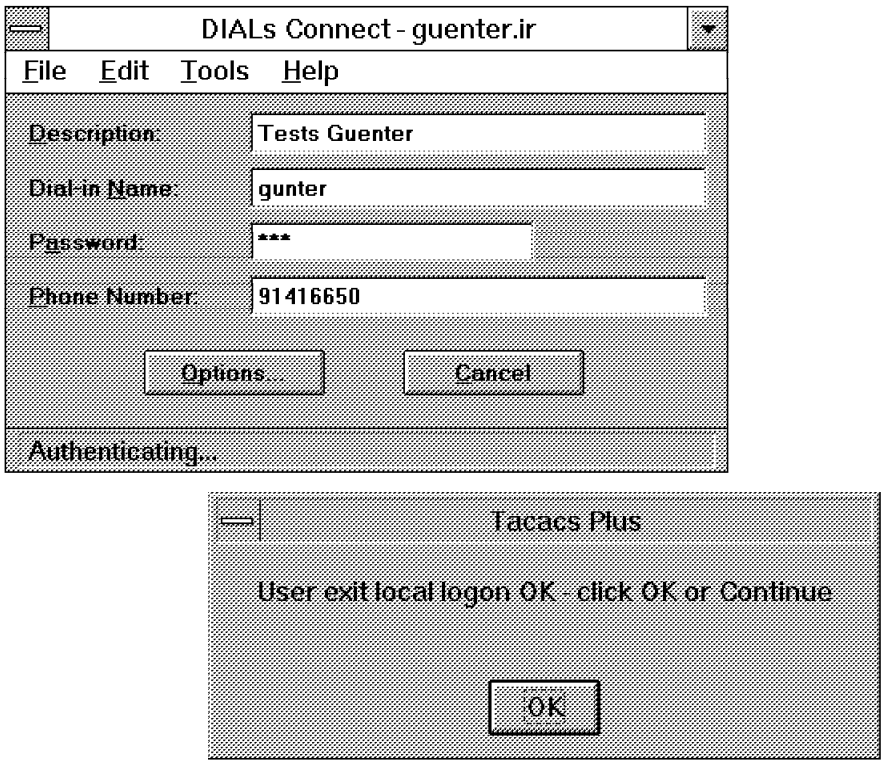


Figure 164. Blockade Dial-In with DIALs for Windows

If the authentication fails, you will get the following message box, no matter whether it was the user ID or password that failed.

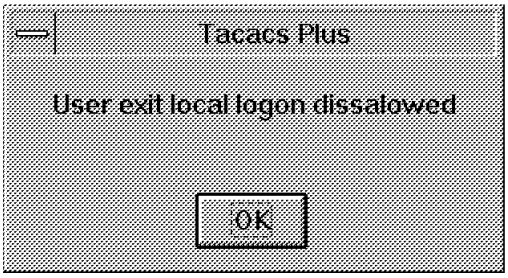


Figure 165. Blockade Dial-In Not Successful

This advanced third-party security device support is supposed to work both for OS/2 and Windows; however, our test with Blockade was only successful when using the Windows version.

b. *Clients* that do not support the advanced third-party security dialog (including all clients at Release 3.5 and earlier) require the following method. We used the OS/2 DIALs Client as an example.

   Enable the **Third-party security device installed** check box; do *not* enable **Echo characters locally**.

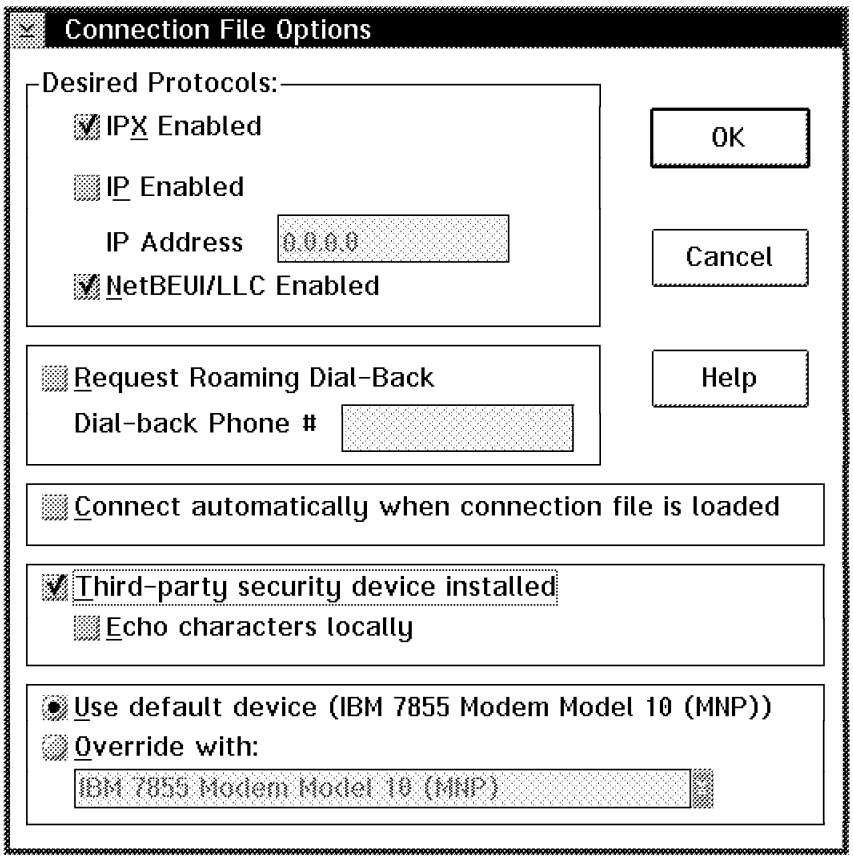


Figure 166. Blockade Dial-In with DIALs for OS/2

When the connection is made, the Third-Party Security window will appear and will be empty. Press Enter twice to get the prompt for your user ID and password. This prompt comes from the Blockade DAS and is passed through by the 8235. If the authentication is successful, you will get the following:

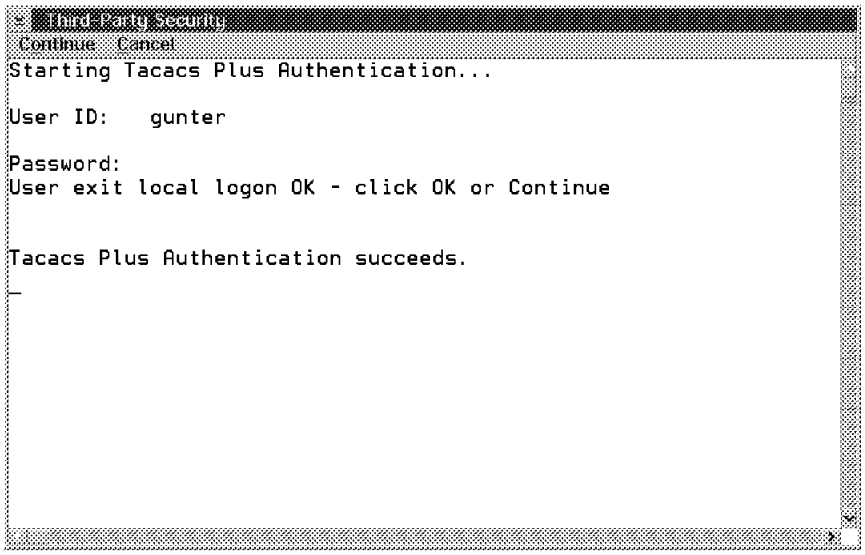


Figure 167. Blockade Dial-In Successful

Click on **Continue**.

The Windows client's Third-Party Security window looks slightly different. The upper three lines of text appear immediately when the window opens because they are of local origin. Again, you have to press Enter twice; the remainder of the dialog is identical.

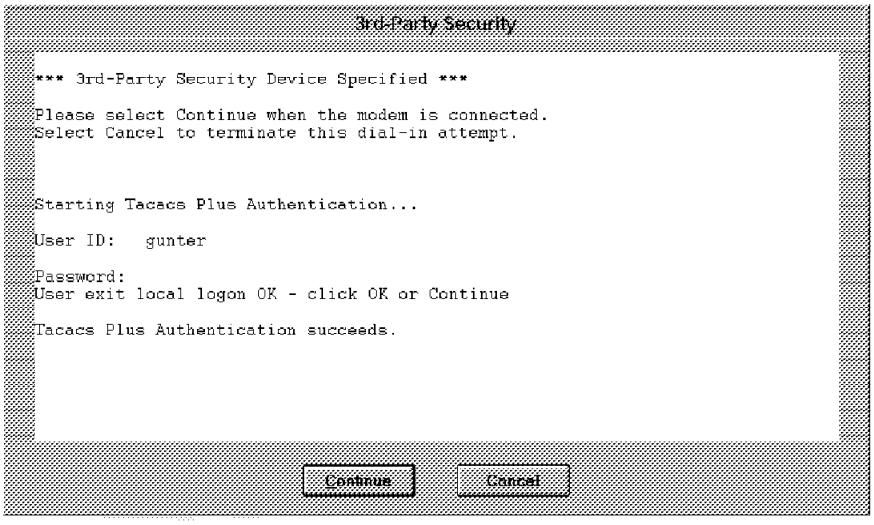


Figure 168. Manual Authentication with Windows Client

2. Configure your 8235 as described in "TACACS+ and the 8235" on page 240. For TCP port number and secret, configure the same values that are used on the Blockade DAS.

   Note: The secret corresponds to the shared key described in the Blockade implementation manual.

3. Configure the *Blockade for IBM 8235 DAS* using the implementation manual that comes with the product.

4. Administration of *Blockade ESS* on the host mimics that of RACF. The following commands illustrate how to alter global Blockade settings (SETBOPTS), how to define the 8235 to Blockade (RBDEFINE) and how to associate a token with a user (ABU). Token support is an optional component of the Blockade implementation.

```
SETBOPTS BLKAPPC(abcname) MODE(BLK) SMF(213)
                         1
RBDEFINE $BSERVE BLKNET.SER8235 TYPE(8235) MODE(BLK)   2

ABU      userid TOKEN(SECURID) SER(12345678)           3
```

Notes:

1 Name corresponds to VTAM definition

2 One statement per DAS

3 One statement per user. Note that SecurID token is handled by Blockade in this example. SecurID must not be enabled by 8235, since there is no separate SecurID server.

Figure 169. Blockade Definitions on Host

10.3.1.4 RADIUS

Remote Authentication Dial In User Service (RADIUS) is another distributed security solution to centralize authentication for multiple, distributed communication servers like the 8235. It has a feature important for service providers: it is capable of providing accounting and billing information.

RADIUS includes two pieces: an authentication server and client protocols.

The server is a UNIX software product developed by Livingston Enterprises (see Appendix A, “Related Terminology” on page 253). It is being shipped in source code format and can be adapted to work with systems and protocols already in use. Ports have been reported to the following platforms:

- AIX
- HP/UX
- SunOS
- Solaris
- Ultrix
- Alpha OSF/1
- BSDI BSD/386
- Linux
- SCO
- UnixWare
- Windows NT
- Windows 95

The RADIUS protocol defines how authentication and authorization information of users is sent between the server and the 8235 that acts as a client. The full protocol specification is available as an RFC (RFC 2058) form in the Internet Engineering Task Force (IETF).

This communication is conducted using UDP. The packets traveling between the 8235 and the RADIUS server are encrypted with a method that uses a 64-byte key.

The authentication request is sent over the network from the 8235 to the RADIUS server. This communication can be done over a local or wide area network, allowing network managers to locate RADIUS clients like the 8235 remotely from the RADIUS server. If the server cannot be reached, the client can route the request to an alternate server.

Note: This enables global enterprises to offer their users a dial-in service with a unique login user ID for corporate-wide access, no matter what access point is being used.

When an authentication request is received, the server validates the request, then decrypts the data packet to access the user name and password information. This information is passed on to the appropriate security system being supported. This could be UNIX password files, Kerberos, a commercially available security system or even a custom developed security system.

If the user name and password are correct, the server sends an authentication acknowledgment. If at any point in this log-in process conditions are not met, the RADIUS server sends an authentication reject to the 8235 and the user is denied access to the network.

A single RADIUS server can support hundreds of communication servers and tens of thousands of users.

The RADIUS architecture supports third-party security enhancements, similar to the 8235 itself. So it allows centralization and unification of enhanced, tokenized authentication even if a mix of different communication servers is used, including some that cannot invoke tokenized authentication servers themselves. This is not the case with the 8235, which supports SecurID and Digital Pathways Defender of its own. However, if a method not supported by the 8235 is preferred, it can be integrated via RADIUS.

RADIUS Accounting is a recent enhancement. It uses the RADIUS protocol for its packet format and adds attributes to handle the additional information needed for accounting. The accounting server listens for UDP packets at port 1646, and is not required to run on the same host as the RADIUS server, although that can be done and is often convenient. A backup accounting server is supported.

Note: The current Release 4.0 of the 8235 only supports RADIUS authentication.

The 8235-I40 supports RADIUS Accounting. To configure these parameters, choose the **Accounting** selection in the configuration drop down menu. Check the **Save to RADIUS Server** box and then press **Add...**. Enter the IP address and secret for the RADIUS server, changing the UDP port if necessary.

Note: RADIUS Accounting is normally on port 1646.

Configure RADIUS Security on the 8235: Select **RADIUS** from the User Authentication group on the Security configuration page. The RADIUS dialog box appears.

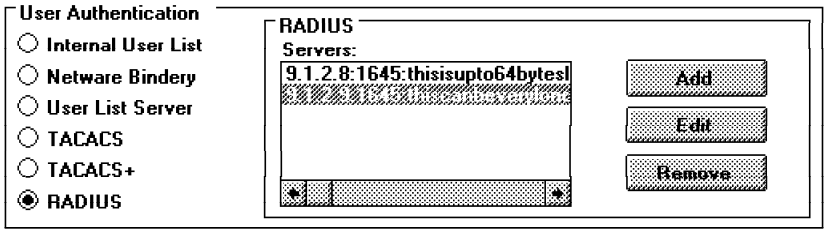


Figure 170. RADIUS Configuration Area Dialog Box

Click on **Add** to enter the address, port, and security information. The Add a RADIUS Server dialog box appears.

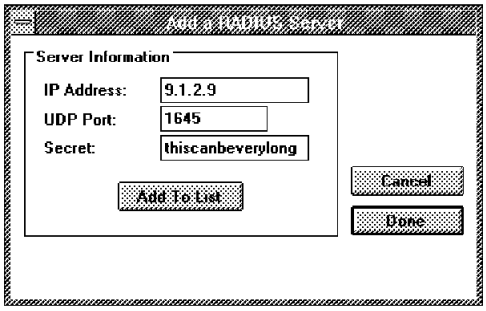


Figure 171. Add a RADIUS Server Dialog Box

Enter the IP address of your RADIUS server. This is the IP address of the workstation on which the RADIUS server software is running. Enter the UDP port number or accept the default of port 1645. This is the port that the RADIUS server uses to communicate. Enter the secret key in the Secret field. It can be up to 64 characters long. This is the key that the RADIUS server and the 8235 use to encrypt data packets. This must be the same key that is configured in the RADIUS server. Click on **Add to List** to add the information to the RADIUS area of the Security page. You can define a list of RADIUS servers, currently up to three.

Configuring a RADIUS Server, User Attributes: The protocol allows for authenticating a user based on a user name/password pair, a challenge/response pair, or both. Lists of user attributes can be configured on the RADIUS server on a per-user basis. The protocol also provides a means for the RADIUS server to return to the 8235, in the authentication reply, the list of user attributes configured for the specific user. Authentication is performed by the RADIUS server; authorization is performed on the 8235 using the user′s authorization information returned from the RADIUS server.

Configuration of a RADIUS server varies depending on the implementation of the server. This section describes how a RADIUS server is configured if the server is built using RADIUS implementations such as Livingston or Merit. If the server is not built with these implementations, the configuration may be different. Always refer to the documentation included with your implementation of RADIUS server software. There are three files read by the RADIUS server:

- The USERS file contains authentication and authorization information for each user.
- The CLIENTS file contains information to authenticate RADIUS clients (8235 remote access server).
- The DICTIONARY file tells the server how to read the user attributes out of the USERS file.

The rest of this section describes the configuration files in more detail.

Users Configuration: The RADIUS server reads a USERS file to get user configuration information. This file contains a list of:

- Users
- Attributes associated with each user

The user attributes are returned to the RADIUS client upon successful completion of authentication. The following example shows part of a USERS file. Note the format of the file:

```
testuser password="testpassword"
     DialBack-Number=16175551234
     DialBack-Number=16175555678
     Shiva-User-Attributes="/di/do/sh/fd/max=5"
     Framed-Address=123.456.789.012
```

Refer to the documentation that is included with your implementation of RADIUS server software for any special format or configuration issues.

Clients Configuration: The RADIUS server reads a CLIENTS file to get client and client secrets information. The CLIENTS file consists of a list of client (device) names and a secret associated with each client. The following example shows a CLIENTS file:

```
Device1    Secret1
Device2    Secret2
```

The device name can be either an IP address or the name of the device, provided that the name exists in the /etc/hosts file. Note that the secret must match the secret configured on the device for this server. Refer to the documentation included with your implementation of RADIUS server software for any special format or configuration issues.

Dictionary Configuration: RADIUS server software assumes that a *dictionary* file exists on the system. The dictionary file tells the server how to read the user attributes out to the USERS file. This file contains a list of attributes that are associated with each user. It assigns an attribute code with each attribute, and indicates what the attribute type is (such as string, integer, and IP address). This file must be modified to include 8235-specific user attributes. Depending upon whether you want to use unassigned attribute values or use vendor-specific attributes, review the information in the following list:

- *Unassigned Attribute Values*

  If the 8235 attributes are going to be added using unassigned attribute code values not currently assigned in the RADIUS RFC, the following line must be added to the end of the dictionary file:

  ```
  ATTRIBUTE    Shiva-User-Attributes      51    string
  ```

  The actual attribute code values depend upon what attribute codes are unassigned in the dictionary file used on the RADIUS server. If the RADIUS server is only talking to a 8235 client device, all attribute values except 1-49 will probably be available. If the RADIUS server is also talking to client devices from other vendors, some of the attribute values above 49 may already be assigned. In the Additional Configuration page under the [Security] section, set the following, where 51 is the starting value of the 8235 user attributes:

  ```
  UseExtendedAttributes=1
  ExtendedAttributeBase=51
  ```

- *Vendor-Specific Attributes*

  If the RADIUS server supports the Tagged Length Value (TLV) format for vendor-specific attributes, the RADIUS client will look for 8235-specific attributes in the Vendor-Specific attribute field. In this case, the following lines should be added to the end of the dictionary field:

  ```
  ATTRIBUTE    Shiva-User-Attributes      1     string     Shiva
  VENDOR               Shiva                    166
  ```

  In this example, note that Shiva in the first line refers to Shiva in the second line. This format can only be used if the RADIUS server software is able to read dictionary file entries in this format. Because different implementations of RADIUS server software might call for different formats, it is necessary that the information appear in the appropriate format. Refer to the documentation included with your implementation of RADIUS server software for dictionary format and configuration issues. In the Additional Configuration page under the [Security] section, set:

  ```
  UseExtendedAttributes=0
  ```

10.3.2 Two-Factor Authentication-Only Solutions

For a sophisticated hacker or a determined insider it is relatively easy to compromise a user's password and gain access to valuable information resources. Single-factor identification (a static password) may hence be considered insecure. Many people choose poor passwords or store them in unsecure places; they attach them to their keyboard, PC or monitor, for example. A high percentage of successful break-ins into networks are due to guessed or stolen passwords.

Before any other security measure is meaningful, authorized system users should be reliably identified, while all unauthorized users must be locked out. The method discussed in this section is a two-factor authentication. It consists of:

- Something secret that a person *knows*, such as a memorized password or personal identification number (PIN)
- Something unique that a person *owns*, such as a smart card that generates a random token

The 8235 supports two external two-factor authorization methods:

- Security Dynamics' SecurID ACE Server
- Digital Pathways Defender Server

10.3.2.1 SecurID

There are four components of a full implementation of SecurID:

- *ACE/Server*

  This component, which uses the UDP Protocol to communicate with an 8235, runs on a UNIX machine. Supported platforms listed by Security Dynamics Inc. are IBM AIX, Sun Microsystems' SunOS/Solaris, Hewlett Packard's HP-UX. (The 8235 is compatible with any ACE/Server Version 1.1 or later.) You must purchase this server software from Security Dynamics, Inc.

  The 8235 supports the use of secondary ACE/Servers. A secondary ACE server is a backup to the primary server. When the primary server is down, the secondary server authenticates user logins and maintains an audit trail.

- *SecurID client*

  This component runs on the 8235 and communicates with the SecurID server via UDP. It is enabled when you configure the 8235 for SecurID.

- *SecurID token*

  The SecurID token is an access control security token that is used to positively identify users of computer systems and networks. It automatically generates a unique, unpredictable access code every 60 seconds. This access code, in combination with the user's PIN, is typed by the user at login time. The SecurID client function within the 8235 passes this on to the SecurID server. Relying on a correct system clock, the server is synchronized with the token and thus either permits or denies access for this user.

  Security Dynamics lists two types of token devices:

  1. The SecurID card with a 6-digit display.

2. The SecurID PINPAD card that requires the PIN to be entered before a token is displayed. This is so the secret PIN is not transmitted over any line and is not exposed to eavesdropping.

- *Dial-in client software*

  This component is the DIALs Client program for PC users or the ARA program for Macintosh users.

Enabling SecurID ACE/Server Support: To enable SecurID ACE/Server support:

1. Enable the **3rd-Party Authentication** check box on the Security configuration page.
2. Select the **SecurID** authentication radio button. The area to the right turns into the SecurID configuration area.

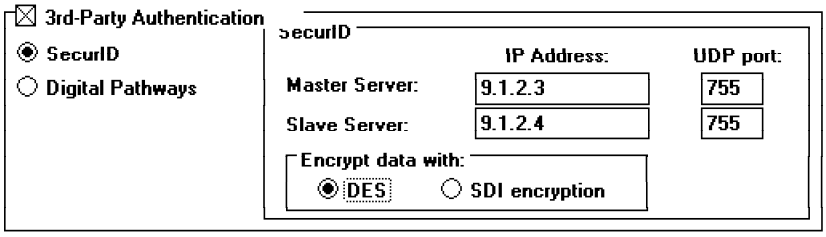


Figure 172. SecurID Configuration Area

3. Type the IP address for the master (or primary) SecurID server.

   Note: The SecurID server can be located on an IP network different from the 8235's IP network.

4. If required, change the default UDP port number of 755.
5. Follow the same steps for the slave (or secondary) server (if any) to be used in the event that the master server is unavailable.
6. Select the data encryption method that is used by your ACE/Server using the Encrypt data with buttons. There are two methods to choose from:
   - Data Encryption Standard (DES)
   - SDI encryption - a Security Dynamics proprietary method

On the SecurID server, follow the instructions given by the Security Dynamics ACE/Server documentation to define the 8235's IP address and name in the appropriate network database and use the SecurID administration software to enable the 8235 as a SecurID client. Then, enable the SecurID cards of any user dialing in to the 8235 and activate these cards for the 8235.

Note: The 8235 must have the IP protocol enabled and have an IP address to interact with the ACE/Server.

For versions 4.0 and higher (DOS not included), the dial-in clients will display dialog boxes for information needed to authenticate. Other versions of dial-in clients must check the **Third Party Security Device Installed**. See Figure 166 on page 243.

10.3.2.2 Digital Pathways Defender Security Server

There are four components involved in this two-factor authorization:

- *Defender Security Server*

  This software component, which must be purchased from Digital Pathways, Inc., runs either on NetWare (as an NLM), Windows NT or UNIX. It provides the centralized authentication database. It supports multiple servers. Currently the 8235 supports two of them.

- *Communication server as agent*

  This is the 8235 configured as the Defender Security Server agent. When the 8235 starts up, it uses IP (in case of Windows NT or UNIX) or IPX (in case of NetWare as the server platform) to connect to the primary Digital Pathways server. The Digital Pathways server authenticates the 8235 using the agent ID and agent key. These need to be configured identically on both machines. If the authentication is successful, the connection remains active.

- *SecureNet Key token*

  SecureNet Key token devices must be purchased from Digital Pathways, Inc. They use a challenge/response process with the Defender server. The server sends an 8-digit *challenge*. The user enters this and the PIN into SecureNet Key. SecureNet Key then displays an 8-digit *response* which, in turn is typed in by the user and is used to either accept or deny this login. With this method, only one-time information gets transmitted over the line; no PIN or password can be overheard by an eavesdropper.

- *Dial-in client software*

  This component is the DIALs Client program for PC users, having the Third-Party Security feature enabled. After modem negotiation, a TTY window appears and displays the challenge prompt coming from the Defender server. This is how the user carries out the challenge/response dialog imbedded in the 8235 dial-in procedure.

Note: An 8235 configured to use Digital Pathways authentication can answer LAN-to-LAN connections, but the LAN-to-LAN connection establishment will not use Digital Pathways authentication; the connection will be made using only the primary authentication method.

Configure Digital Pathways Defender Server: To enable Digital Pathways support:

1. Enable the **3rd-Party Authentication** check box on the Security configuration page.
2. Select the **Digital Pathways Authentication** radio button. The area to the right turns into the Digital Pathways configuration area.

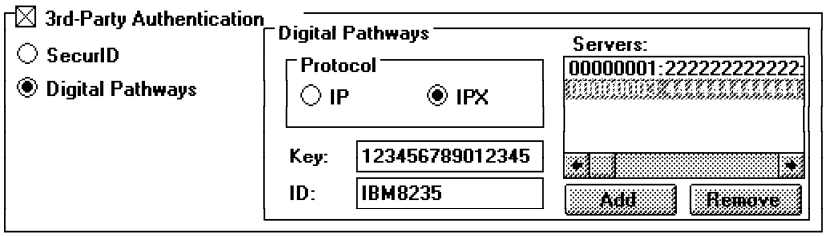


Figure 173. Digital Pathways Configuration Area

3. Select **IP** or **IPX** in the Protocol group.
4. Type the key (up to 16-digit hexadecimal value) and ID (a case-sensitive, alphanumeric value) of the agent. The default agent ID is IBM8235.
5. In the Servers area, use the **Add** and **Remove** buttons to define the Digital Pathways Server and one backup server (if any). Depending on the protocol selected you will get a dialog box, either like Figure 174 (IPX) or like Figure 175 (IP).

   To change a server information entry, double-click on the line that represents this server. The Edit window will be similar to the Add window; however, it will not have the **Add to List** button. Note that the box in Figure 174 is named Add rather than Edit erroneously.

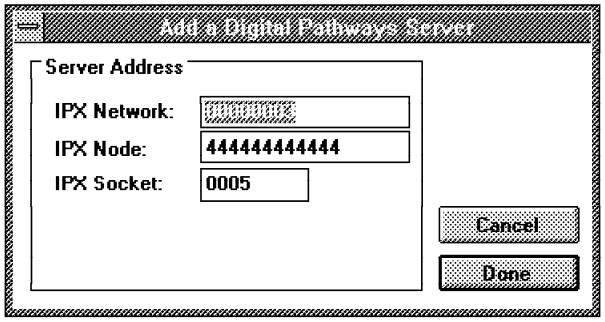


Figure 174. Edit a Digital Pathways Server (IPX)

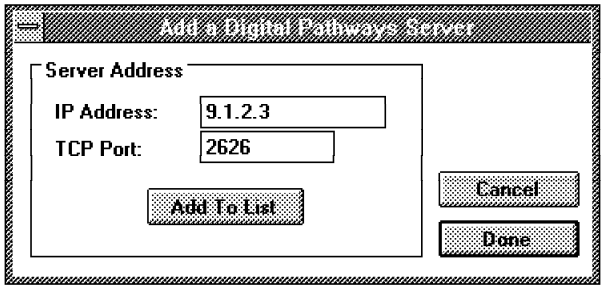


Figure 175. Add a Digital Pathways Server (IP)

6. For IP, type in the IP address and the UDP port of the Digital Pathways server. For IPX, type in the IPX network, node and socket number of the Digital Pathways server. Then, click **Add to List** or **Done**.

   The first Digital Pathways server in the list is the primary server; the second one is the backup server.

Appendix A. Related Terminology

Terminology	Definitions
Access lines	Lines used to access services within the network cloud (analog, BRI, PRI, T1/E1).
Access mode	In remote access, it refers to the three ways to access information (dial-in, LAN-to-LAN, and dial-out)
Aggregation (Bandwidth)	Bandwidth aggregation is the ability to combine multiple B channels into a single higher bandwidth communications channel per connection.
Analog	A continuous signal that can consume all of the values of the spectrum through which is passes.
Asynchronous	A method of data transmission that allows characters to be sent at non-predetermined intervals by preceding each character with a start bit and ending each character with a stop bit. These extra bits slow down data transmission, but also make communication more forgiving of errors because the bits help keep the transmission accurate even when poor line quality exists.
Augmentation (Bandwidth)	Bandwidth augmentation is the ability to add another communications channels to an already existing communications channel. (Augment = to add to)
Backbone	The part of the communications network designed to carry the bulk of traffic. Provides connectivity between subnetworks in an enterprise-wide network.
Bandwidth	A term defining the information-carrying capacity of a channel: its throughput. The greater the bandwidth, the more information that can be sent in a given amount of time.
B-channel	A ″bearer″ channel that carries voice or data at 64 kbps in either direction and is circuit-switched.
Bonding	A type of inverse multiplexing performed at the circuit level, where the data stream is sliced up into equal portions, regardless of the content of the data stream, and each portion is transmitted over an available circuit. At the receiving end the data stream is reassembled in the proper order.
BRI (Basic Rate Interface)	ISDN access method comprising two 64 kbps B-channel and one 16 kbps D-channel (2B+D).
Channel	A path for electrical transmission between two or more points. Also called a line, link, circuit or facility.
CHAP	Challenge Handshake Authorization Protocol. Protocol that describes how to authenticate incoming data calls using password from calling end. Password is encrypted over access line.
CODEC (Coder/Decoder)	A sophisticated digital signal processing unit that takes analog input and converts it to digital on the sending end. At the receiving end, the process is reversed to take the digital signal and reconvert it to analog.
Compression	Data compression increases the amount of data that can be carried across WAN connections in a given time. STAC compression can improve ISDN performance by as much as 400%.
CSU (Channel Service Unit)	A device used to connect a digital connection, such as a T1/E1 being delivered from the phone company, to network access equipment located on the customer premises. The CSU also regenerates the digital signal to boost clarity and remove background noise. Some devices include an integrated CSU/DSU.
D-channel	The out-of-band ″data″ channel of an ISDN interface. The D-channel operates at 16 kbps in the BRI and 64 kbps in the PRI.
DCE (Data Circuit Equipment)	A device which converts digital signals for asynchronous transmission over a phone line. Generally known as a modem.

Terminology	Definitions
DTE (Data Terminal Equipment)	A device transmitting data to, and/or receiving data from a piece of data communications equipment (such as a modem). Your computer, particularly the communications port, is a DTE device.
Dial-in	A mode for remote users to access information. To the user the network is remote.
Dial-out (shared)	A mode for locally connected LAN users to access shared communications equipment to dial up remote information.
Digital	A discrete digital that can assume only certain specific values within its range. The use of a series of binary codes (zeros and ones) to represent information.
Digital modem	A type of modem that allows analog calls to be received over a digital (ISDN) line. Converts incoming digital data stream containing PCM-encoded modem waveform into actual data contained in waveform at the data rate transmitted by the remote analog modem. Performs the inverse function for an outgoing data stream.
DS0	A 64 kbps unit of transmission bandwidth. A worldwide standard speed for digitizing one voice conversion. Twenty-four DS0s equal one DS1.
DS1	A 1.544 Mbps unit of transmission bandwidth in North America and 2.048 Mbps unit of transmission in Europe. A telephony term describing a 1.544 or 2.048 Mbps digital signal carried on a T1 line.
DSP	Digital Signal Processor. Another term for digital modems.
DSU (Data Service Unit)	A device used to connect a computing device (DTE) to a digital phone line to allow for fully digital communications.
E1	European equivalent of a T1 circuit. Transmission rate of 2.048 Mbps on E1 communications lines. An E1 facility carries a 2.048 Mbps digital signal over 32 channels (30 channels when the T1 is provisioned for ISDN PRI).
Fractional T1	Service offering data rates between 64 kbps (DSO rate) and 1.544 Mbps (DS1 rate) in specified intervals of 64 kbps. T1 service is ordered, but less than the full 24 channels is delivered.
Frame Relay Frame	A variable length unit of data in frame relay format that is transmitted through a frame relay network as pure data. Contrast with Packet.
Frame Relay Network	A network interface providing high speed frame or packet transmission with minimum delay. It has less protocol overhead than X.25.
Homologation	Conformity of a product or specification to international standards.
Hub	A central point of a network, usually providing some level of network-wide coordination. A hub can also be a single point of failure. Often, it is efficient to locate the fileserver or connection to a wider area network at the hub.
In-band signaling	Transmission within a frequency range normally used for information transmission.
ISDN (Integrated Services Digital Network)	A service that allows a variety of switched digital data and voice transmission to be accommodated simultaneously. It is a networking concept that provides subscribers with end to end fully digital communications.
ISDN multirate	A network-based ISDN service that allows users network access equipment to dial network channels of bandwidth increments of 64 kbps up to 1.536 Mbps. Access to ISDN multirate is obtained over ISDN PRI lines.
IEC	Interchange Carrier. Common carrier providing communications channels between local telephone companies. Also known as long-distance carriers such as AT&T, MCI, Sprint, WilTel, etc.
Internet	The global system of networks interconnected by TCP/IP (and IP related protocols) which include over 30 million users from the private sector, educational institutions, government, non-profits, and individuals. Internet users gain access to e-mail, file transfer, remote login, gopher news, World Wide Web and other related services.

Terminology	Definitions
Internet Service Provider (ISP)	An organization that offers access to the internet through dial-up or dedicated lines. Supports customers to various degrees in the areas of special services, such as domain name registration, listservers, FTP site creation and maintenance, and Web page creation and maintenance.
Inverse multiplexing	Inverse multiplexing equipment receives high-speed input and breaks it up for the network into multiple 56 or 64 kbps signals so that it can be carried over switched digital services. It also provides the synchronization necessary to recombine the multiple channels into a single integrated transmission at the receiving end.
Leased lines	A circuit rented for exclusive use 24 hours a day, seven days a week from a telephone company. The connection exists between two predetermined points and cannot be switched to other locations.
Local Exchange Carrier (LEC) Lines	Local Exchange Carrier or local phone company telephone lines used to supply telephone service to a location. LEC lines are needed by all organizations to handle local telephone traffic.
Local loop	A transmission path between users and the central office. The connections between the local telephone company′s network and the customer premises equipment is formally called the network interface or the point of termination.
MIB	Management Information Base. A directory listing the logical names of all information resources residing in a network and pertinent to the network′s management. A key element of SNMP management systems.
Modem	Acronym for modulator/demodulator. A device that converts digital signals into a form suitable for transmission over analog facilities and vice versa.
Modulation	The alteration of a carrier wave in relation to the value or samples of the data being transferred.
Multilink PPP or MLP or MP	A standard method for splitting, recombining and sequencing packets across multiple data links to form a single aggregate channel. Originally developed to exploit multiple ISDN B-channels, but equally applicable to asynch links. Also referred to as packet inverse multiplexing. Officially termed MP in the RFC, but generally known as MLP.
Networking termination equipment	The part of the digital communications circuit that completes the final leg of the circuit to the data terminal equipment on the customer side of the connection.
NT1	The first customer premises device on a two-wire ISDN circuit coming in from the telephone company. Among other things, it converts the two-wire signal called a ″U″ interface to four wires, so multiple devices can be attached to the ISDN circuit.
NT2	Network Termination Type 2 equipment are those devices providing customer site switching, multiplexing, and concentration (PBXs, computers, terminal controllers).
Out-of-band signaling	Transmission outside the frequency range normally used for information transmission.
Packet	A group of fixed-length binary digits, including the data and call control signals, that are transmitted through an X.25 packet switching network as a composite whole. The data, call control signals, and possible error control information are arranged in a predetermined format. Packets do not always travels the same pathway, but are arranged in proper sequence at the destination side before forwarding the complete message to an addressee.
Packet fragmentation	The ability to configure a default packet size over which packets will be fragmented for more efficient distribution over aggregated communications links.
Packet switching network	A telecommunications network based on packet switching technology, wherein a transmission channel is occupied only for the duration of the transmission of the packet. Contrast with Frame Relay Network.
PAP	Password Authentication Protocol. Protocol that describes how to authenticate incoming data calls using a password from the calling end. The password is not encrypted over the access line.

Terminology	Definitions
PBX (Private Broadcast Exchange)	Any privately owned switching system. In contrast to a switch, which is run by the local telephone company. The telephone lines are still supplied by the telephone company, but line consolidation and routing is performed by the PBX.
Permanent Virtual Circuit (PVC)	A frame relay logical link, whose endpoints and class of service are determined by network management. Analogous to an X.25 permanent virtual circuit, a PVC consist of the originating frame relay network element address, originating data link control identifier, terminating frame relay network element address, and terminating data link control identifier. Originating refers to the access interface from which the PVC stops. Many network customers require a PVC between two points.
POP	Point of presence. A central office or service access point for a network service provider's services (such as an Internet Service Provider).
POTS (Plain Old Telephone Service)	The standard telephone service that we are all familiar with. The service is provided on two wires and uses analog signaling to provide single line telephone service. No additional features such as call waiting, call forwarding, conference calling, voice mail etc. All you can do is make or receive calls.
PPP Protocol	A protocol that allows a computer to use TCP/IP over a standard telephone line with a high speed modem to become a fully participating member of the internet. PPP is favored as a replacement for SLIP, an older protocol that accomplished the same function.
PRI (Primary Rate Interface)	An US and Japan 1.544 Mbps ISDN access method comprising 23 (64 kbps) B-channels and one (64 kbps) D-channel (23B+D) or an International 2.048 ISDN access method comprising 30 (64 kbps) B-channels, one (64 kbps)D-channel (30B+D), and one (64 kbps) channel used by the carrier.
Proxy	An entity that, in the interest of efficiency, essentially stands in for another entity.
PSTN (Public Switched Telephone Network)	The telecommunications network commonly accessed by all of us virtually every day when we make a telephone call. The PSTN is a gigantic maze of switching computers that can connect any two (sometimes more) telephony points in potentially hundreds of different ways.
RADIUS	Remote Access Dial-In User Security. A remote access dial-in security system administered by a centralized database that contains password and access information as well as user configuration profiles.
Rate Adaptation	Algorithms used to map a user's actual but transfer rate to the 64 kbps speed of the B-channel (9600 bps to 64 kbps).
Remote Adapted Routing	The adaptation of backbone routing techniques that take into account; slow-line communications links, intermittent connections, security, chatty routing protocols, management, and user ergonomics.
R interface	An ISDN reference point between non-ISDN terminal equipment (TE2) and a terminal adapter (TA).
RJ-11	Standard four-wire connector for phone lines.
RJ-45	A standard eight-wire keyed connector used in local area networks (LANs) and ISDN S/T interfaces.
Setup time	The time required to fully establish a WAN connector. Virtual connections work best over interfaces that support fast setup times (ISDN 1-3 seconds). Standard analog modems typically have a setup time of about 30 seconds.
Signaling	Transmission of information for the purpose of directing voice traffic over a telecommunications network.
SPAP	An authentication protocol developed by the Shiva Corporation which extends the functionality of dial-in users to allow for virtual connections, alert messages, and dialback.
SPID (Service Profile IDentifier)	A code used to identify a specific ISDN set on a given ISDN circuit when more than one ISDN device is attached to the same circuit.

Terminology	Definitions
S/T interface	The four-wire ISDN circuit between the customer's network termination equipment (NTI) and customer's data/voice equipment.
SNMP	Simple Network Management Protocol. A protocol governing network management and monitoring of network devices and their functions. Originally developed in the TCP/IP environment.
Spoofing	A method by which the client and/or router filters network traffic to keep unnecessary traffic from going over the WAN link.
Static route	A route that is manually entered into a routing table. Static routes take precedence over routes chosen by all dynamic routing protocols.
Synchronous	A transmission system in which characters are synchronized by the transmission of initial sync characters and a common clock signal.
Tariff	Documents filed by a regulated telephone company with a state public utility commission of the Federal Communications Commission. Documents details services, equipment, and pricing publicly offered by the telephone company. Also a general term for telephone line usage charges.
T1	A 1.544 Mbps 24 channel (23 when provisioned for ISDN PRI) digital line used for transmission of data though the telephone system. Used in the US and Japan.
TE1	Terminal Equipment type 1 (TE1) end-user ISDN devices that utilize ISDN protocols and support ISDN services (ISDN telephones and workstation).
TE2	Terminal Equipment type 2 (TE2) are non-ISDN compatible devices, such as analog telephones and personal computers.
Terminal Adapter (TA)	An ISDN phone or a PC card that emulates one. Devices at the end of basic-rate interfaces line are known as terminals.
Time division multiplexing (TDM)	The process of dividing the capacity of the transmission facility into discrete time slots, with each individual channel assigned a specific time slot.
Trunk	A single circuit between two points, both of which are switching centers or individual distribution points.
V.110	A rate adaptation scheme widely used outside of North America over ISDN lines.
V.120	A rate adaptation scheme used in North America over ISDN lines.
UART	Acronym for Universal Asynchronous Receiver-Transmitter.
U-Interface	The two-wire ISDN circuit between the customer's network termination equipment (NTI) and the telephone company's central office. It is capable of supporting the 2B+D signaling (144 kbps) and an additional 16 kbps for network signaling between the NTI or other customer premise device and the central office switching system.
Unified Access	A goal of IBM's to provide unified (transparent) access to networked information and processed regardless of access mode.
Virtual	Existing or resulting in essence or effect though not in actual fact. A term that refers to a "logical" entity that does not actually exist. (Examples: virtual circuit, company, connection, LAN, memory, office, terminal).
Virtual Circuit	A logical end-to-end connection between two points.
Virtual Connection (VC)	A connection set up between two points that appears to the user to be available as a dedicated connection. This "phantom" connection can be maintained indefinitely or can be ended at will. The three states of virtual connection are up, down, or suspended.
WAN	Wide area network. A data network typically extending a LAN outside a building or beyond a campus, over IXC or LEC lines to link to other LANs at remote sites. Typically created by using bridges or routers to connect geographically separated LANs.

Appendix B. Special Notices

This publication is intended to help Customers, IBM technical professionals, service specialists, marketing specialists, and marketing representatives to demonstrate, install, administer and support the IBM 8235 Access Switch. The information in this publication is not intended as the specification of any programming interfaces that are provided by the 8235-I40 Access Switch. See the PUBLICATIONS section of the IBM Programming Announcement for the 8235-I40 Access Switch for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these

names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX
AT
Client Access/400
IBM
OS/2
RACF
VTAM
WaveRunner
Workplace

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix C. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

C.1 IBM Publications

For information on ordering ITSO publications see “How to Get ITSO Redbooks” on page 263.

- IBM 8235 Model I40 Dial-In Access to LANs (DIALs) Switch Installation Map, GX27-4030
- IBM 8235 Dial-In Access to LANs Concept and Implementation, SG24-4816
- The 8235 LAN Connect Quick Reference, GX27-3985

C.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection	SBOF-7250	SK2T-8042

C.3 Other Publications

You may obtain further information about the 8235 and related products from the following sources:

- Request ns823540 from ssp at dalvmic1
- Tools sendto hqvmic1 toolslcl nsctools get netsows package
- IBM 8235 Forum
- Steven Zundel, RTPNOTES(zundel), IBM 8235 Forum
- http://www.raleigh.ibm.com
- http://www.networking.ibm.com/82s/82sprod.html
- http://www.networking.ibm.com/82s/82si40.html
- http://www.networking.ibm.com/nes/nes8235.htm
- ftp://lansupport.raleigh.ibm.com/pub/products/lanprods/hub
- Radius: http://nic.merit.edu/radius/installing.radius.html#SysReq
- Shiva: http://www.shiva.com
- Novell: http://www.novell.com
- Microsoft: http://www.microsoft.com

- Digital Pathways: http://www.digpath.com
- Blockade: http://www.blockade.com
- Synaptel: http://www.synaptel.fr
- Security Dynamics: http://www.securid.com
- Livingston: http://www.livingston.com
- ISDN*Tek: http://www.isdntek.com
- Funk Software: http://www.funk.com
- Remote Access Homeworld: http://www.geocities.com/SiliconValley/Peaks/2028/
- Dan Kegel's ISDN Page: http://alumni.caltech.edu/dank/isdn/

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at http://www.redbooks.ibm.com.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get BookManager BOOKs of redbooks, type the following command:

  ```
  TOOLCAT REDBOOKS
  ```

  To get lists of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO: type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Web Site on the World Wide Web**

  http://w3.itso.ibm.com/redbooks

- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

  IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (http://www.redbooks.ibm.com/redpieces.htm). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** — send orders to:

	IBMMAIL	**Internet**
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications	IBM Publications	IBM Direct Services
Publications Customer Support	144-4th Avenue, S.W.	Sortemosevej 21
P.O. Box 29570	Calgary, Alberta T2P 3N5	DK-3450 Allerød
Raleigh, NC 27626-0570	Canada	Denmark
USA		

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1)001-408-256-5422 (Outside USA)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services** - send note to softwareshop@vnet.ibm.com
- **On the World Wide Web**

Redbooks Web Site	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank).

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (http://www.redbooks.ibm.com/redpieces.htm). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

- Invoice to customer number
- Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

Numerics

A

B

C

D

E

R

S

T

U

V

W

X

Z

ITSO Redbook Evaluation

IBM 8235-I40 Access Switch Concepts and Implementation
SG24-2132-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@vnet.ibm.com

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes____ No____

If no, please explain:

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

_____

_____

_____

_____

_____

This soft copy for use by IBM employees only.

Printed in U.S.A.