Columbus Client

Remote Workstation Access to
distant LANs via ISDN

Version 3.40

December 98

Digi International Inc.
Joseph-von-Fraunhofer-Str. 23
D-44204 Dortmund
E-Mail: support@itk.de
WWW: http://www.itk.com

Contents

Preface

Congratulations! In purchasing **Columbus Client** you have selected a truly high-performance product. It will allow you to access a remote LAN or the Internet from an individual PC (Laptop) via ISDN, Modem or GSM connections.

If you have ever used a PC to connect to a remote LAN via a modem or an X.25 connection, then you certainly know how slowly data move between the systems. At data transfer rates of from 2.4 to 33.6 kbit/sec, you simply cannot work efficiently in such an environment.

With ISDN transfer technology you will get significantly faster response—even with only one “B channel.” B channels are the digital paths used in an ISDN connection to carry *user data*—in other words voice, data or video information—at a rate of 64 kbit/sec.

With many applications, you can therefore use Columbus Client and only a single B channel to work at speeds that are completely acceptable to a PC user who is accustomed to LAN environments.

Connecting a remote PC to a LAN involves a technically sophisticated process. We want to make using Columbus Client as easy as possible for you. As soon as you have installed Columbus Client, you can use your PC to access a remote LAN just as easily as you would if your PC was directly connected to the LAN.

“Dynamic line management” with “Short Hold” mode will reduce your transmission costs in the public ISDN dial-up network. Only if you have ISDN leased lines or if you exclusively use the lines in your ISDN telephone system for LAN access you will be able to avoid additional transmission costs, regardless of how much you use your LAN connection.

We wish you the *best of success* in using Columbus Client!

Digi International Inc.

Important Notice:
By purchasing *Columbus Client*, you have acquired the right to use the software for **only one** installation! You may make a backup copy of the software you purchased, but if you wish to make several installations, you must **purchase a separate license** for each one. Violation of the rules governing the use of the Columbus Client software is subject to criminal prosecution.

1 Before you begin

This chapter offers a **basic overview** of Columbus Client. It explains how the manual is organized and what it contains, and helps you to find your way about the manual in an efficient manner. Finally, it contains information on the Columbus Client environment.

In this chapter you will find:

- a description of the **manual elements** and how they facilitate using the manual
- a **product overview** for Columbus Client
- the **requirements for installing** Columbus Client
- **examples of how to use Columbus Client** (Remote access and Internet access)

1.1 How to use this manual ...

This manual is intended for the *basic* PC user who, for example, wants to connect his workstation at home to a LAN for the very first time but has no special LAN know-how. All that is needed to understand this manual is familiarity with Windows 95/NT 4.0 and a basic understanding of how to use a PC.

Structure and Organization of this Manual

- **Chapter 1** provides an **overview** of the product functionality, the installation requirements, and how a PC is connected to a corporate LAN and to the Internet.
- **Chapter 2** describes **operation under Windows 95**. You will learn how to start your remote PC, log into the remote server, and how to check the ISDN connection. You will use the new ISDN Connection Manager to establish and de-establish the ISDN connection, add and remove channels, and check the various operating modes.
- **Chapter 3** describes **operation under Windows NT 4.0**.
- **Chapter 4** describes the organization of and all the **functions available in the ISDN Connection Manager** in tabular form. This chapter is especially useful if you need to look something up.
- **Chapter 5** describes how to **test** your **remote PC** by logging in to the Digi_TEST router in Dortmund, Germany. The chapter will also tell you what you can find on the Digi_TEST server.
- **Chapter 6** describes **how to correct frequently occurring errors:** when connections are established, when accessing the LAN, and with the *Short Hold* feature.
- **Appendix A** contains **detailed error messages** and explains how you can correct errors when they occur.
- **Appendix B** contains a **brief description of the filters** and emulations for extremely experienced users.
- **Appendix C** contains **Information** about the **SecurID (ACE) Client**.
- The **glossary** contains the most important **technical terms** briefly explained.

- The extensive **index** will help you locate the information you need quickly to answer questions in advance or explore areas which may come up during setup or operation.

In any event, you must be certain to contact the appropriate network administrator for the remote LAN you will be using to obtain the telephone number(s), connection parameters, and access authorizations needed to access the remote LAN.

The following features are employed consistently throughout the manual to facilitate its use.

Header

The header on each page also contains the page numbers ("1-2" for example means: Chapter 1, page 2). The current chapter and section number are indicated on left-hand (even-numbered) pages. On the right-hand (odd-numbered) pages of text you will find the *title of the current chapter* to guide you when you want to leaf through the manual.

On the even-numbered pages you will see the *version number* of Columbus Client on the right side of the header.

Note

Especially important information is shown with a gray background:

The gray background indicates an important point that you should not skip over.

Special Note

Particularly important information that, if ignored, could easily lead to problems is also indicated by an exclamation mark symbol:

This item is especially important. Ignoring this information may very quickly lead to problems or cause the product to malfunction!

Bold or Italic Print

Bold or italic print are used in this manual to **highlight information** or *emphasize* it.

Expressions in Angle Brackets <>

Expressions in angle brackets refer to keys on your computer keyboard, for example: <Insert> refers to the Insert key.

If keys and letter combinations are connected with a plus sign, for example <Ctrl>+<N>, these keys must be pressed **simultaneously**. <Ctrl>+<N> means that the <Ctrl> key and the <N> key must be pressed at the same time.

Expressions in angle brackets can also be used for the contents of variables, for example: <name of the primary server>.

General Operating Steps

Operating steps are presented as follows:

(1) Turn on your PC.

(2) [next operating step]

(3) [... additional operating steps]

(4) …

1.2 Columbus Client: Product Information

This section describes the various properties of Columbus Client.

The Columbus Client software has the following individual components, which are contained on the CD supplied with the product:

- README files contain the very latest information on the product.
- Installation files for Windows 95 and Windows NT 4.0

Important:

Current information which could not be included in the manual may be found in the README.TXT file.

1.2.1 Properties of Columbus Client

Columbus Client was developed especially for Windows 95 and Windows NT 4.0, which means that it is easy to install and operate. Here is a brief list of the Columbus Client properties:

Integration in Windows 95 / NT 4.0

Columbus Client is a totally new product. Since it supports Microsoft's preferred interface NDIS 3.1, it offers seamless integration in Windows 95 / NT 4.0. Full integration in Windows 95 / NT 4.0 assures a simple installation. When you install Columbus Client for Windows 95, you will be accompanied by a so-called *guide*, which explains every step of the installation in a separate window. In addition, you can configure your setup in a user-friendly manner to simplify future work. For example, you can place connections that you use often right on the desktop, so that you can activate them by simply double-clicking on them.

ISDN Connection Manager

The ISDN Connection Manager works like a *control panel* for Columbus Client. It allows you to check current connection data, the connection status, and current configuration whenever you wish. Extensive statistics allow you to optimize your ISDN environment and therefore cut costs. In addition, the ISDN Connection Manager generates detailed journals so that you can check ISDN charges whenever you want. These journals are stored in a file named *journal.txt*, which can be evaluated at a later time.

CAPI 2.0

Columbus Client is based on the CAPI 2.0 standard. Because of this, you can use Columbus Client in parallel with other CAPI 2.0 applications. Thus, you can set up your PC to run as a multifunctional workstation:

- Fax G3 and G4
- Voice mailbox
- Euro-Filetransfer
- Telephony support
- Access to online services

PPP Support

PPP has established itself in the ISDN world as the standard used for connectivity products produced by numerous manufacturers. Columbus Client offers extensive PPP support with the following options:

- IPX protocol
- TCP/IP protocol
- Bridging
- PAP
- CHAP and MS CHAP
- IP address negotiation
- PPP Multilink, PPP Callback, PPP Compression

Columbus Client is compatible with the following third-party remote access servers:

- Cisco 1000, 2000, 4000, 7000, ...
- 3COM Access Builder
- etc.

Short Hold (Inactivity timeout)

Columbus Client offers a special mechanism called *Short Hold* or inactivity timeout. If you have activated this mechanism on your remote PC, the *physical* ISDN connection between your remote PC and the remote LAN is automatically de-established if it was not used to transfer data for a given length of time. Meanwhile, the *logical connection* to your server remains intact: The connection is *sleeping*.

As soon as you request new data from the remote LAN or try to send data to the LAN, the sleeping physical connection of the logical connection is re-established, and you simply continue working without having to log in again. You will barely notice the brief delay (1 to 1.5 seconds).

Basic Security Service (BSS)

Columbus Client supports BSS on the Digi ISDN boards as a default setting. You can use a subscriber authentication to determine which destinations will be allowed to access the ISDN dial-up network. Incoming calls are identified by the calling party number, which is indicated by the ISDN network.

If an incoming call is coming from an ISDN dial number that is not found in the authentication table, the connection is disconnected immediately.

CHAP, Microsoft CHAP and PAP Authentication Protocols

CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol), MS CHAP (Microsoft CHAP) and PAP (**P**assword **A**uthentication **P**rotocol) are password-based authentications between the remote PC and the ISDN router. The following parameters are required by the communicating partners for the authentication to be successful:

Parameter	Explanation
User name	Name of the remote PC
Partner	Name of the connection partner (router)
Password	Password for the connection
Direction	Direction of the authentication

An authentication request is sent to the connection partner as the connection is being established. The connection partner transmits the parameters *user name* and *password*; these parameters are compared with the actual entries. If they match, the connection is established; the connection is de-established immediately if they do not match. The authentication may be conducted in one direction or (for greater security) also in both directions. The difference between PAP and CHAP is that with CHAP the password must always be transmitted in encrypted form over the ISDN line. If you have the option to use either PAP or CHAP, you should always use CHAP.

Windows NT or Windows 95 remote partners use besides PAP a variant of CHAP, the Microsoft CHAP, which applies a different encryption. With MS CHAP it is only possible to use „allow own authentication“ as direction.

Callback

In the case of callback, the remote PC tries to establish a connection to the ISDN router. The router checks the dial number communicated in the D channel and, based on its connection partner entry, the router determines that it must call this connection partner back. It then rejects the call and immediately establishes a connection to this connection partner. The remote PC recognizes the incoming call from the router and accepts it.

This callback is performed for security reasons and to ensure that costs are only charged to a single location (reverse charging). Callback is configured solely at the router. With this type of callback, the remote PC does not incur any communications charges whatsoever.

Another form of callback is the PPP callback. This type of callback is an option provided by PPP. When this option is used, a complete B channel connection is established, and after authentication the remote PC signals a request for a callback. Based on its partner configuration, the router then decides whether the connection will be de-established and a callback performed.

CAPI Modem Driver

Columbus Client supports analog and GSM-modem connections via PPP (**P**oint-to-**P**oint **P**rotocol).

This feature is realized by a **CAPI Modem Driver**: a CAPI interface for using the installed standard modem drivers of the appropriate operating system. It enables Columbus Client to support incoming and outgoing connections via CAPI 2.0 compatible ISDN adapters and any standard modem drivers.

1.3 Requirements for the Remote PC

Using Columbus Client turns your PC into a LAN remote PC. To accomplish this, however, the following requirements must be met:

- You will need an **Digi ISDN board** and driver software (this driver software may also have to be installed during the installation of Columbus Client) or an ISDN board which has CAPI 2.0 support, or an ISDN board with a CAPI subsystem installed.

A version of the CAPI subsystem is contained on the original Microsoft Windows 95 CD (German version). This version is defective and therefore cannot be used with Columbus Client. A newer, executable version of the CAPI subsystem is available from Acotec, Berlin (Germany).

- An ISDN line on the public ISDN system or on an ISDN PBX system must be **cleared** for *data transfer services*.
- An ISDN **socket** must be located within reach of the ISDN cable supplied with the Digi ISDN board.
- The **CD** for **Columbus Client** must be on hand.
- The **CD** for **Windows 95 / NT 4.0** must be on hand.

Furthermore your PC has to run under Windows 95 or Windows NT 4.0 and your PC has to fulfill the usual requirements for these operating systems.

In order for you to be able to access the remote LAN with your remote PC, an ISDN router must be installed in this LAN.

Please note:

In purchasing Columbus Client you have obtained the license rights for **a single** remote PC installation **only**! However, you are permitted to make a copy of the software for backup purposes.

If you want to operate more than one remote PC, you will need to purchase **a separate license for each PC**. Any illegal use of Columbus Client software may result in criminal prosecution.

1.4 Hotline

Please contact your local distributor.

1.5 Examples of Applications

Two of the most important applications for Columbus Client are discussed below:

- access to a remote LAN via ISDN (remote access)
- access to the Internet via ISDN (Internet access)

1.5.1 Connection to a Corporate LAN

You can use Columbus Client to connect to a corporate network via ISDN. It makes no difference whether you are working at your workstation at home or are on the road with your laptop. The corporate network must have an ITK NetBlazer or some other PPP-compatible router.

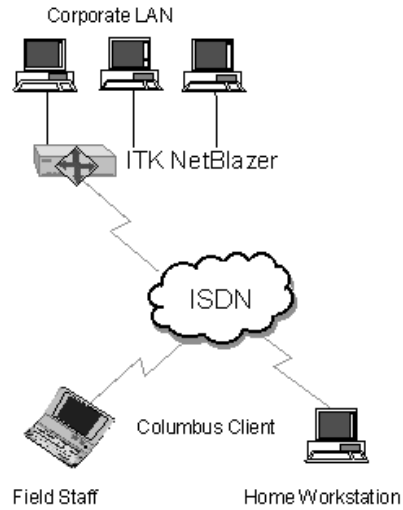


Fig. 1-1 Typical configuration for two remote PCs which access a corporate network via ISDN.

An ISDN board which supports CAPI 2.0 must be installed in the remote PC itself. The NDIS 3.1 driver for Columbus Client uses an ISDN connection as the communications medium, and it works together with the corresponding router in the corporate network.

The remote PC on which Columbus Client is installed therefore has the same Desktop as a PC which is connected directly to the LAN.

1.5.2 Connection to the Internet

You can use Columbus Client to establish a connection to the Internet via ISDN. To do this you will need an active or a passive ISDN board and a standard TCP/IP application (for example: Netscape Navigator or the Microsoft Internet Explorer). This permits you to use the popular WWW, E-Mail and FTP.

Columbus Client supports the 32-bit WINSOCK.DLL for Windows.

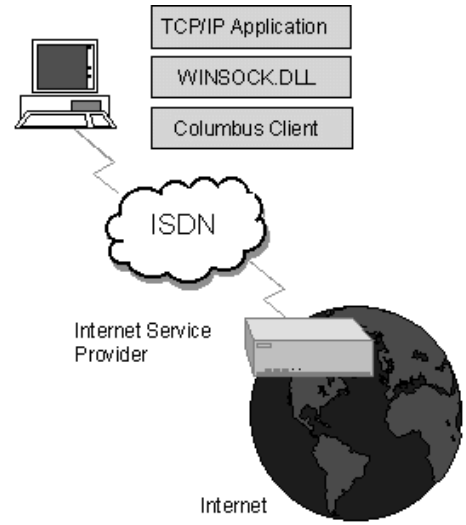


Fig. 1-2 Typical configuration for connecting to the Internet via ISDN

Advantages of this solution:

- The full ISDN 64-kbit/sec bandwidth is used.
- The extensive PPP support makes it possible to connect to any desired Internet provider.

2 Operation under Windows 95

In this chapter you will learn how to use Columbus Client on your PC operating under Windows 95.

You will learn how to:

- set up a new destination (Chapter 2.1.1, *Creating a New Destination* (page 2-3))
- establish and de-establish an ISDN connection (Chapter 2.1.2, *Connection Management* (page 2-5))
- check the status of the ISDN connection and display the journal (Chapter 2.1.3, *Checking the Status of an ISDN Connection* (page 2-11) and Chapter 2.1.4, *Journal* (page 2-14))
- logon to and off from a remote network server (Chapter 2.2, *Connecting Columbus Client to a Network* (page 2-20))
- start these functions from the ISDN Connection Manager.

Open the individual functions from the menu bar, the toolbar and the tabs (with command buttons).

In Chapter 2.1, *Using the ISDN Connection Manager* (page 2-2) you will learn, step by step, how to use the ISDN Connection Manager.

In Chapter 2.2, *Connecting Columbus Client to a Network* (page 2-20) you will learn how to establish a connection to a network using Columbus Client.

Chapter 4.1, *Organization of the ISDN Connection Manager* (page 4-2) provides a systematic description of how the ISDN Connection Manager is organized.

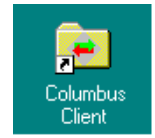
Chapter 4.2, *Summary of Functions* (page 4-30) lists all the functions in the form of a table. The table contains detailed explanations of the various functions.

2.1 Using the ISDN Connection Manager

The ISDN Connection Manager provides a convenient way to view all the data needed to establish a connection and to change any parameters as needed.

Open the ISDN Connection Manager:

(1) Double-click on the *Columbus Client* folder:



(2) Use the right mouse button to click on the icon for the destination which you wish to connect to.

The following context-sensitive menu will appear:

(3) Click on *Open*.

The ISDN Connection Manager is opened without establishing a connection to the destination you wish to connect to. All the parameters for this destination are set. You can now check and also edit these parameters.

Refer to Chapter 2.1.1, *Creating a New Destination* (page 2-3) to learn how to set up a new destination.

You can read about how to establish and de-establish a connection in Chapter 2.1.2, *Connection Management* (page 2-5)

Explanations of statistical data are provided in Chapter 2.1.3, *Checking the Status of an ISDN Connection* (page 2-11)

Data on connections which were established and de-established in the past are stored in the so-called Journal. Chapter 2.1.4, *Journal* (page 2-14) contains information on the Journal.

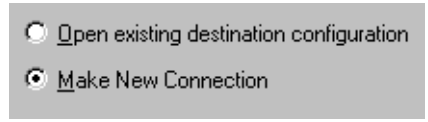
2.1.1 Creating a New Destination

You must first set up a destination before trying to establish a connection to this partner.

To accomplish this, perform the following steps:

(1) Double-click on this icon

The following dialog box will appear:



(2) Choose *Make New Connection*, then click on *Next >*.

The remaining procedure is the same as that described for the first-time installation. For detailed information, please refer to your *Installation Manual*, Chapter 2.2.1, *Installing Columbus Client under Windows 95,* section *Wizard: Create New Destination*.

(3) Check the parameters that are set on the *Destination* tab. You can read about this in Chapter 4.1, section *Destination Tab* (page 4-19).

Note that the tab will differ in appearance depending on which dial number scheme is being used (Fig. 2-1, *Destination tab with full dial number scheme* and Fig. 2-2, *Destination tab for Use of straight dial numbers*.)

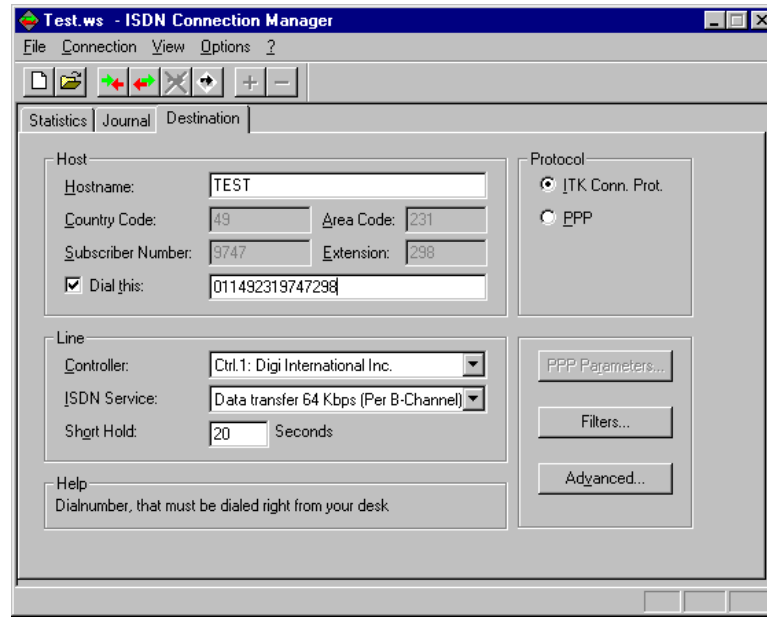


Fig. 2-1 *Destination* tab with **full dial number scheme**

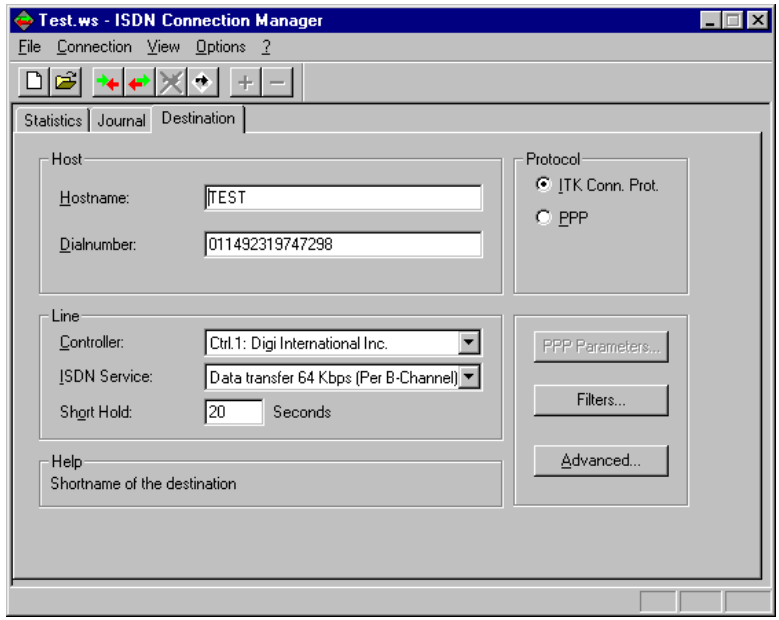


Fig. 2-2 *Destination* tab for **Use of straight dial numbers**

Any changes can be made in these tabs. The meanings of the individual parameters are explained in Chapter 4.1, section *Destination Tab* (page 4-19). The changes do not take effect until after a connection has been established manually (click the  icon in the toolbar).

2.1.2 Connection Management

In this chapter, you will learn how

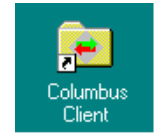
- to establish an ISDN connection to a destination
- to add and remove a B channel manually
- to manually teardown an ISDN connection (Short Hold feature)
- to terminate the ISDN connection.

Establishing an ISDN Connection to a Destination

If the destination has not yet been created, please read Chapter 2.1.1, *Creating a New Destination* (page 2-3) first.

To establish an ISDN connection to a **destination that has** already **been set up,** perform the following steps:

(1) Double-click on the *Columbus Client* folder.



(2) Double-click on the icon for the destination you wish to connect to.

The connection to the desired destination is now established.

(3) If you are already in the ISDN Connection Manager, establish the connection by clicking on  or on *Establish* in the Connection menu.

If you have activated the Short Hold mode for your PC (default setting), then you will not need to worry about de-establishing the connection.

As soon as the connection is not used during the previously set Short Hold time, the ISDN Connection Manager will automatically terminate only the physical connection to avoid connection charges. The ISDN Connection Manager will re-establish the physical connection as soon as it is needed again.

If you have not activated the Short Hold mode for your PC or the destination, you will be connected to the destination from this point in time on. ISDN charges will be incurred until you terminate again this physical connection.

Adding and Removing a B channel

These functions are available with PPP, but not with the ITK Connectivity Protocol.

In order to be able to operate a multiple-channel connection, the PPP Multilink Protocol must always be active.

Proceed as follows:

(1) Click on the *Destination* tab.

(2) Click on the command button *PPP Parameters*.

(3) Select one of the following 3 options under *Multilink*:

Entry	Meaning
Inactive	One and **only one** B channel is always used.
Static	If two free B channels are available, **two** B channels are always used.
Dynamic	**One or two** B channels are used (depending on the data flow requirements). This mode is optimized for using Columbus Client to make connections to other networks.

In the case of the *static* and *dynamic* settings, the PPP Multilink Protocol is used to negotiate connections to the destination. A multichannel connection is not possible unless both partners support this protocol.

If you use channel bundling, your connection charges will definitely increase. However, it is not always possible to fully exploit the resulting transfer performance gain.

When you use the ISDN Connection Manager, you can add and remove a B channel manually.

Function	Meaning	Click on Icon	Open Menü → Submenu
Add B channel	Add B channel to an existing logical connection		**Connection → Add Channel**
Remove B channel	Remove B channel from an existing logical connection		**Connection → Remove Channel**

Assigning an IP address to your TCP/IP protocol

You can also specify a static IP address within a *.ws file. This IP address is valid for only this particular ISDN destination. It is forwarded to your TCP/IP protocol via the DHCP emulation.

The main advantage of this method is that you don't need to reboot Windows after changing to another ISDN destination if you just want to run IP traffic.

In order to use this feature follow these instructions: Configure your TCP/IP protocol in the Windows network configuration to *Obtain an IP address from a DHCP server.* Now add for instance the following lines to the [Partner] section of the *.ws file

```
OwnIpAddress = 192.109.96.30
PeerIpAddress = 192.109.96.32
```

The "OwnIpAddress" specifies the IP address that will be assigned to your station whenever you communicate with this ISDN destination.

The "PeerIpAddress" is the IP address of the destination itself; this value is used as gateway address in subsequent operation.

Only for Windows NT 4.0:

During the installation of TCP/IP the protocol "WINS-Client (TCP/IP)" is activated automatically. It shows up within the binding list of the network configuration and must not be deactivated manually. Otherwise the use of DHCP is impossible.

Manually de-establishing an ISDN Connection

Even if you are using the Columbus Client Short Hold mode, it can sometimes make sense to manually drop the ISDN connection. This is the case if you have completed your work on the network and are certain that you will not have to use any network resources in the immediate future. In this case, you would not wait for the Short Hold time to de-establish the connection, since a new billing interval might begin during this time; instead, initiate the transparent de-establishment manually.

Another reason for de-establishing manually is to help your destination be accessible to other PCs who might be trying to connect to the remote LAN through the destination's limited number of B channels.

To manually de-establish the ISDN connection, click on the  icon on the toolbar. The physical connection has now been de-established, but the logical connection remains intact.

Terminating an ISDN Connection

If you are running your remote PC in the Short Hold mode, you will not need to make a special effort to terminate ISDN connections to cut costs since Columbus Client automatically shuts down physical connections that are not in use. Once you have finished working in the remote LAN, you can log out. See Chapter 2.2, section *Connecting Columbus Client to a Network* (page 2-20). Shut down the ISDN connection (Click on ).

The following warning message (see Fig. 2-3) will appear if

- you shut down the ISDN connection without having logged out from the server and
- the option *Require user confirmation to disable* is activated (see Chapter 2.2.4, *Prompting on Connection Disable* (page 2-23).

This warning message will only appear if you have mapped network drives or are using the ITK Connectivity Protocol.

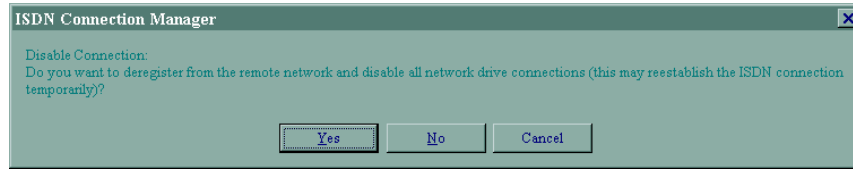


Fig. 2-3 This warning message will appear if you try to shut down an ISDN connection without first logging out.

- Click on *Yes* to automatically release all network drive mappings and shut down the ISDN connection.
- Click on *No* if you are certain that you will not want to re-establish the ISDN connection. In this case, the network drives are not released. This can subsequently result in slower response times since the system will look for network drives.
- Click on *Cancel* to cancel the procedure and not shut down the ISDN connection.

If you have not mapped any network drives and are using PPP (with Internet applications, for example), the following warning message will appear (see Fig. 2-4).

Fig. 2-4 This warning message will appear if you try to shut down an ISDN connection without first logging out.

- Click on *Yes* to shut down the ISDN connection when you will not be establishing the ISDN connection again (with Short Hold).

- Click on *No* if you do **not** want to shut down the ISDN connection.

2.1.3 Checking the Status of an ISDN Connection

The ISDN Connection Manager keeps extensive statistics on each connection when it is in progress and displays them online.

To obtain statistics on individual connections, click on the *Statistics* tab.

The *Statistics* tab might look something like this:

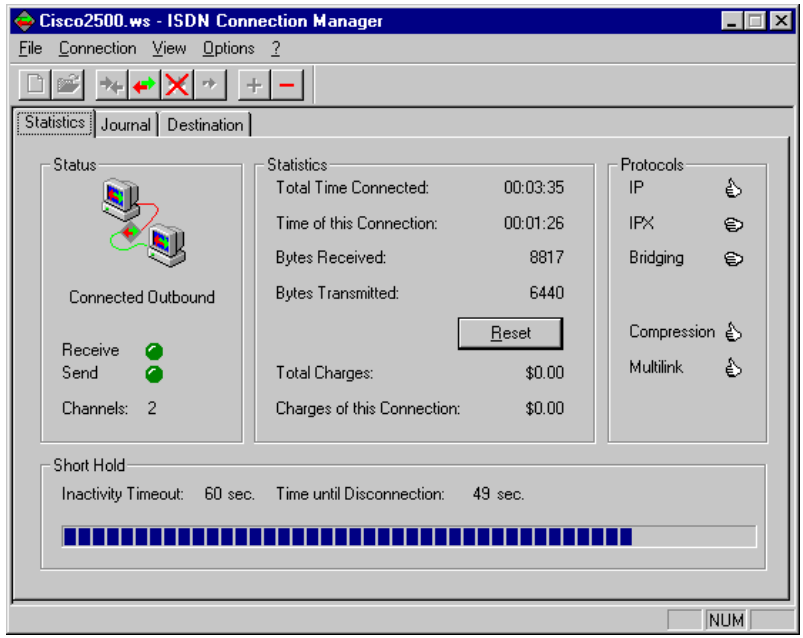
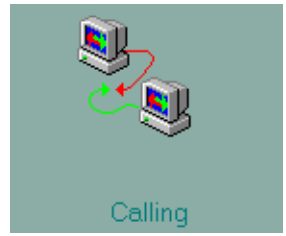
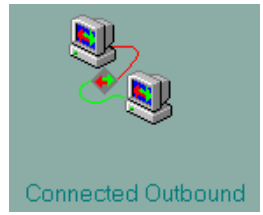
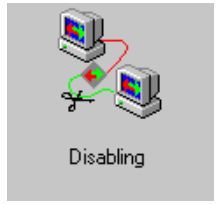
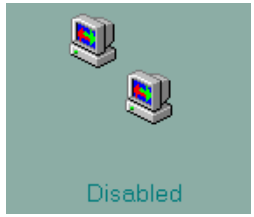


Fig. 2-5 *Statistics* tab

Each time the connection status changes, the graphic on the *Statistics* tab will change accordingly.

The meanings of the various graphics are indicated in the following table:

Entry/Graphic	Meaning
	The ISDN Connection Manager is attempting to establish an ISDN connection to the destination.
	A physical connection to the destination is already present. The two stations are exchanging identification or handshaking data in order to establish a logical connection.
	A physical and logical connection to the destination is present. The physical connection may sometimes consist of a number of bundled B channels.

Entry/Graphic	Meaning
	No ISDN connection is present; a connection can be established automatically (Short Hold).
	The physical and logical connection is currently being de-established. The next status should be *Disabled*.
	**Neither a** physical connection **nor a** logical connection to the destination are present. The connection cannot be established automatically (neither actively nor passively). To establish a connection, click on  .
	No ISDN connection is present. As soon as a call is received from the outside, a connection will be established.

Checking Data Traffic

You can check the data traffic by looking at the *Statistics* tab. The green light will tell you whether data are being sent or received. The number of data sent and received will also be indicated. The meanings of the functions are explained in the following table:

Entry/Graphic	Meaning
	If the green *Receive* lamp is lit, Columbus Client is **receiving** data.
	If the green *Send* lamp is lit, Columbus Client is **sending** data.
	Displays the number of bytes **received** for the entire logical connection.
	Displays the number of bytes **transmitted** for the entire logical connection.
	Sets the *Received Bytes* and *Sent Bytes* displays back to zero.

2.1.4 Journal

Information on earlier and ongoing connections is collected in the so-called *Journal*. This information is simultaneously saved in the *Journal.txt* file (located on the same directory in which the ISDN Connection Manager was installed).

To go to the Journal, click on the *Journal* tab.

Journal Tab

Here is an example of what the *Journal* tab might look like:

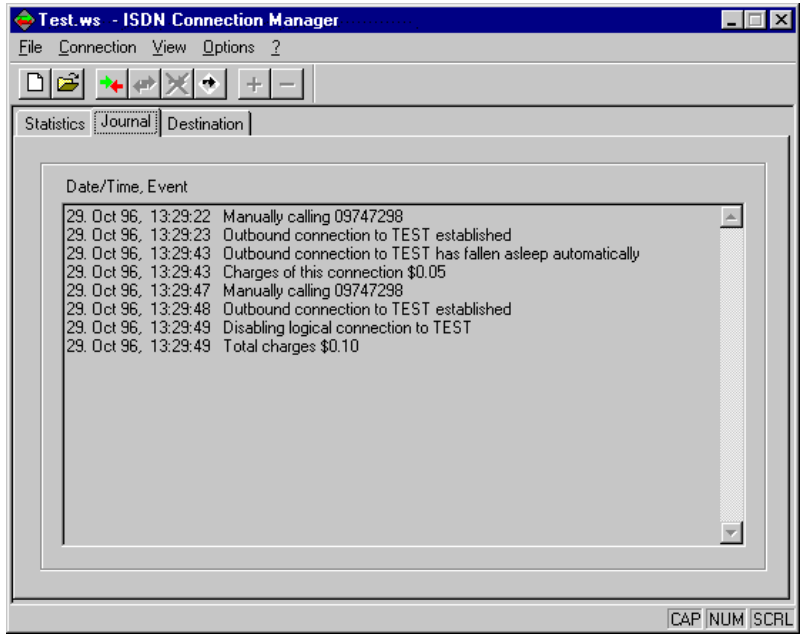


Fig. 2-6 Journal tab

The individual entries have the following meanings:

Entry	Meaning
Date/Time	The date and time of the event are displayed here.
Event	Here you will also find detailed information on: • The type of connection (outgoing connection established, outgoing connection sleeping, call to ... etc.) • Name of the destination • Charges incurred • Error messages

2.1.5 Establishing a Connection upon the Start of Windows 95 and Initial Short Hold

Establishing a Connection upon the Start of Windows 95

If you activated the function *Establish connection at Windows startup* in the *ISDN Service and Short Hold* dialog box during installation, a connection to the specified destination will be established automatically after Windows 95 is started.

> In order to gain full access to NetWare networks we recommend to use the "Establish connection at Windows startup" feature.

If you did not choose this function during installation but want to use it later, then perform the following steps:

(1) Click on the *Options* menu and then on *ISDN Connection Manager ...*

(2) Click on the *Browse...* command button.

The dialog box *Select Destination* will appear.

(3) Select the partner you wish to connect to and then click on *Open*.

The destination you wish to connect to is now entered. When Windows 95 starts, a connection to this destination will be established automatically.

When Windows 95 starts, wait until the connection has been established before entering your Windows password.

(4) If you want the ISDN Connection Manager to be minimized when it runs during the automatic establishment of a connection, click on *Launch Minimized*.

(5) If you no longer want to have an automatic connection to a destination established upon the start of Windows 95, click on the command button *Clear*.

Using the option *Establish connection at Windows startup* results in a permanent logical connection until you as user manually force Columbus Client to disable the connection. Even if you log off from Windows a logically established connection will not be cut and remain *connected* or in Short Hold mode. Please note that this may cause additional charges. If you shut down Windows having an established logical connection you may observe fairly long shut down times. This can be prevented by disabling the logical connection before actually shutting down.

Always use a Windows password, since otherwise Windows 95 will have security gaps.

Setting up Windows password

To set up a Windows password, perform the following steps:

(1) First, click on the *Start* button.

(2) Point to *Settings* and then click on *Control Panel*.

The *Control Panel* will appear.

(3) Double-click on the *Passwords* icon:

(4) On the tab *Change Passwords* click on the *Change Windows Password* command button.

(5) Enter a new password under *Password*.

(6) Re-enter the same password under *Confirm Password*.

(7) Confirm by choosing *OK*.

Initial Short Hold

This feature allows to switch to the sleeping state without establishing an initial connection.

In order to establish a connection to an Internet Service Provider (e.g. isp.ws) automatically, you have to create a Desktop-shortcut with the following command line:

```
"c:\columbus client 95\program\ixconf95.exe c:\columbus
client 95\destination\isp.ws /S"
```

For Windows NT 4.0:

```
"c:\columbus client nt\program\ixconfnt.exe c:\columbus
client NT\destination\isp.ws /S"
```

After running the shortcut the connection will now be established automatically if you launch e.g. a Web-Browser.

If the Columbus Client is disabled or waiting for an incoming call, you may switch to the sleeping mode by the menu option *Short Hold*.

For using this feature under Windows 95 you should bind only the *TCP/IP-Protocol* to the Columbus Client.

For using this feature under Windows NT 4.0 you should bind only the *TCP/IP-Protocol* and the *WINS-Client (TCP/IP)* to the network adapter *Columbus Client*. You may check this on the *Bindings* tab in the network configuration window of Windows NT.

The initial Short Hold can be selected for a connection establishment at Windows startup in the ISDN Connection Manager's *Destination* tab. The Windows RAS service should be disabled.

In order to ease dynamic assignment of IP addresses Columbus Client retains the IP address that was assigned during the last session. In case of trouble with IP address assignment (DHCP) you may disable this property. Just add the following line to the [Partner] section of the *.ws file by using, for example, the Notepad:

```
UseLastIpAddrForInitialSleep=0
```

2.1.6 Activating Acoustic Signals

Sound files are copied into your Windows 95 directory upon installation. If you have installed a sound card in your PC, you will be able to hear a specific sound whenever the status changes (ringing telephone, busy signal, etc.).

Complete the following steps if you want to hear these sounds:

(1) Click on *Options* in the menu bar of the ISDN Connection Manager, and then click on *ISDN Connection Manager*.

The *Options* menu will appear.

(2) Click on the check box *Enable sounds on connection events* to activate the acoustic signals.

(3) Confirm by choosing *OK*.

You can also configure the acoustic signals individually by clicking on the *Sounds* icon in the *Control Panel*:

2.2 Connecting Columbus Client to a Network

One of the most important applications of Columbus Client is connecting to a remote LAN. For this reason, we shall now briefly describe how to log in or out from a remote LAN using Columbus Client.

2.2.1 Logging In

Perform the following steps to connect Columbus Client to a remote LAN:

(1) Establish a connection to the destination you wish to connect to. Refer to Chapter 2.1.2, *Connection Management* (page 2-5) to find out how to do this.

(2) Double-click on the *Network Neighborhood* icon on your Windows 95 Desktop.

The *Network Neighborhood* window will appear; the destination's various servers are listed in it.

(3) Double click on the server which you want to log in to.

The *Enter Network Password* window will now appear:

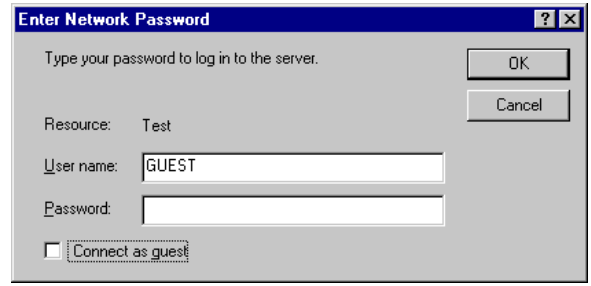


Fig. 2-7 *Enter Network Password* window

(4) Enter your user name and password and confirm by choosing *OK*.

You will now be logged in to this server.

If a password is stored in the password register for the chosen server, Windows will automatically log in without prompting for a password.

2.2.2 Logging Out

Once you have finished your work on the server, you will need to log out. Proceed as follows:

(1) Double-click on the *Network Neighborhood* icon on your Windows 95 Desktop.

The *Network Neighborhood* window will appear; the destination's various servers are listed in it.

(2) Mark the server from which you want to log out.

(3) Press the right mouse button.

The following context-sensitive menu will appear:

(4) Click on *Who Am I* to find out where you are logged in and from which server you will have to log out.

(5) Click on *Detach* to log out from this server.

(6) Now continue as described in Chapter 2.1, section *Terminating an ISDN Connection* (page 2-9).

2.2.3 Restoration of network drives

Mapped network drives will be saved and restored for each destination automatically. Also the ISDN Connection Manager will restore on termination all network mappings that had been assigned before Columbus Client was started.

This functionality can be disabled as follows:

(1) Under *Options* choose *ISDN Connection Manager*.

(2) Click on the option *Save and restore mapped network drives automatically.*

This option will be disabled by using the *Establish connection at Windows startup* feature. For Windows 95 please refer to Chapter 2.1.5, *Establishing a Connection upon the Start of Windows 95 and Initial Short Hold* (page 2-16) and for Windows NT 4.0 refer to Chapter 3.1, *Establishing a Connection upon the Start of Windows NT* (page 3-2).

The following figure shows the *Options* dialog box with the disabled option *Establish connection at Windows startup*:

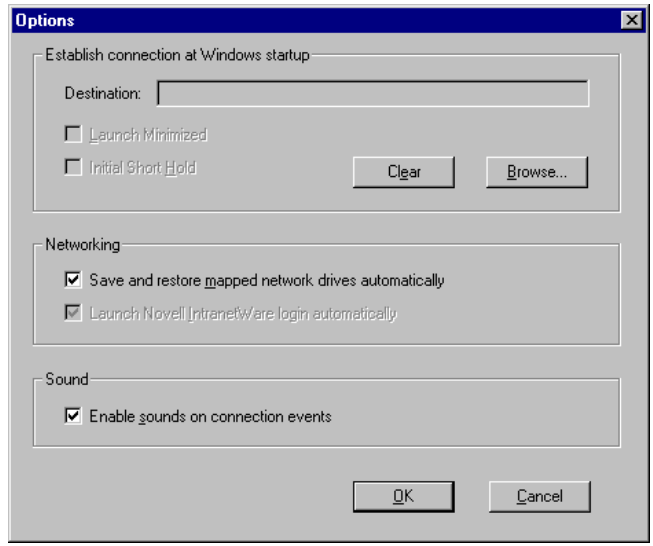


Fig. 2-8 *Options* dialog box

2.2.4 Prompting on Connection Disable

Upon connection de-establishment a confirmation dialog appears by default.

This behavior can be enabled/disabled.

(1) Click on the *Options* menu and then on *ISDN Connection Manager...*.

(2) Click on the option *Require user confirmation to disable*.

A hook in the option field shows that disabling must be confirmed.

2.2.5 Using the Novell Client 32 for Windows 95

Working with the Novell NetWare Client 32 for Windows and Columbus Client is now possible. In the network configuration, both *IPX/SPX compatible protocol* of Microsoft and *IPX 32 Bit Protocol for Novell NetWare Client 32* of Novell must be installed. For each protocol, the frame type must be set to Ethernet_II.

For smooth working with Novell Client 32, consider some differences to the *Client for NetWare networks* included in Windows 95:

- After establishing a logical connection, Columbus Client tries to attach to the default server entered in the network configuration. If this fails, the Novell login program is invoked where you must enter a valid server name!
- The (de-)establishment of logical connections takes slightly more time, especially if one is logged in to an NDS tree. It is recommended to wait 1-2 sec after physical connection establishment before browsing the network neighborhood.
- With Novell NetWare Client 32 for Windows it is not possible to establish ISDN connections to different destinations subsequently. Before connecting to the second destination, Windows 95 needs to be rebooted.
- Shutdown of Windows 95: If the system seems to hang after the message screen *Please wait while your system shuts down* is shown, press <*Enter*> to proceed.

2.3 Using the CAPI Modem Driver

During the installation of Columbus Client you may have chosen to install the CAPI Modem Driver. This piece of software enables you to utilize Columbus Client together with your modem(s) to establish PPP connections over analog lines. You simply have to install the modem under Windows 95 or Windows NT due to your modem's installation description. Please refer to your modem manual and the Windows manual.

Once the modem is installed and you have rebooted your system, it will automatically be recognized by the CAPI Modem Driver and offered as a *Controller* within the Columbus Client configuration.

To establish a dial-up PPP connection with Columbus Client using your modem please refer to Chapter 2.1.1, *Creating a New Destination* (page 2-3). When prompted to select a Controller simply choose your modem from the drop down list.

Please consider following items when working with modem connections:

- Only PPP connections are supported (no ITK Connectivity Protocol)
- Short Hold is supported, but consider that the connection establishment may take a fairly large period of time (caused by modem training)
- The timeout for the modem training is set to 60sec.
- Since on incoming modem calls, the caller's dialnumber is not provided by the network the calling line identification (CLI) is not possible.
- After adding/removing a modem to/from your windows environment you have to reboot to make the CAPI Modem recognize this configuration change.
- CAPI Modem Drivers use the regular Windows TAPI interface to establish the modem connections. Therefore all modem specific configuration items like *AT init* commands that are configured within the Windows environment also apply to CAPI Modem connections.
- Following special characters are supported within the Columbus Client's dialnumbers in order to ease modem connectivity:

  W wait for dialtone
  P pulse dialing
  T tone dialing (DTMF)
  , pause of 2 seconds

- If you want to use callback please ensure that your modem correctly reports incoming calls and busy conditions. Some modems, e.g. the Microsoft standard modem drivers, have been observed that do not behave this way and thus prevent Columbus Client from accepting calls correctly.

3 Operation under Windows NT 4.0

The content of Chapter 2, *Operation under Windows 95* is also valid for the operation under Windows NT 4.0.

Please note that under Windows NT 4.0 Columbus Client offers a security option, which exploits the extended security options of Windows NT. This security option is activated once during the installation by the administrator and can be deactivated only by reinstalling or installing an update of Columbus Client. If this security option had been chosen, users **without administrator rights** can only establish and de-establish connections. All other user interface items are locked.

The following information are referring to an installation with administrator rights.

Read what's different under Windows NT 4.0 in Chapter 3.1, *Establishing a Connection upon the Start of Windows NT* and Chapter 3.2, *Working with Network Clients*.

3.1 Establishing a Connection upon the Start of Windows NT

In order to gain full access to NetWare networks with Windows NT we recommend to use the *Establish connection at Windows startup* feature.

To activate this feature proceed as follows:

In order to be able to activate this feature you have to be logged in as administrator!

To activate this feature, proceed as follows:

(1) In the *ISDN Connection Manager* click on *Options* and choose *ISDN Connection Manager ...* .

(2) Click on the *Browse* button.

(3) Select the *Destination* to which a connection has already been established at Windows startup.

The following figure shows the *Options* dialog box with the option *Establish connection at Windows startup.*

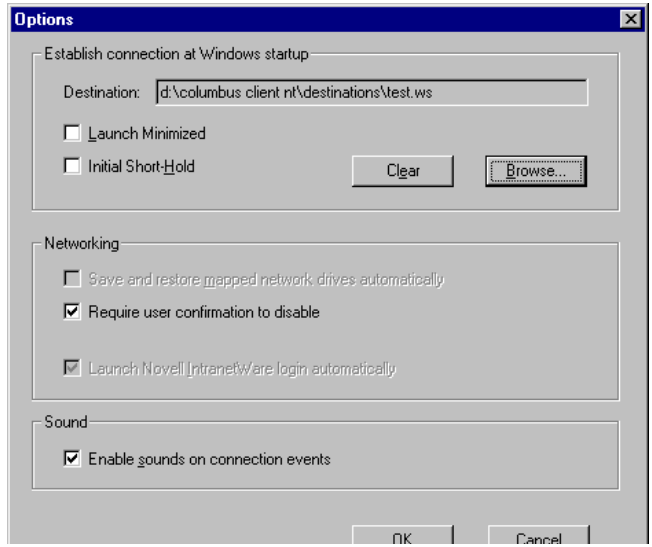


Fig. 3-1 *Options* dialog box

Using this option, please wait with logging on to Windows with the Windows NT 4.0-login until a connection is established:

When the **connection is going up** the **mouse pointer will change to an Columbus Client icon**. As soon as the connection is established the mouse pointer changes to an arrow with a **smaller Columbus Client icon**.

Since the network drivers will be loaded while the login screen shows up, please be patient.

3.2 Working with Network Clients

3.2.1 Microsoft Client Service for NetWare

Using this client, network mappings on bindery servers can be re-established automatically.

> Please ensure that your Windows user name and password are identical with your NetWare login.

If you are not willing to use the option *Establish connection at Windows startup*, in the configuration do not enter a preferred server nor a preferred tree.

Access to NDS volumes is not possible in this case.

Please ensure that your NetWare server is operating in bindery emulation mode.

If you definitely need NDS access please use the *Establish connection at Windows startup* feature.

> If you have activated the *Establish connection at Windows startup* feature, please wait for the connection being established before logging on to Windows. Then you will be able to logon to the network.

3.2.2 Novell IntranetWare Client

When using this client the Novell Login user interface will show up after booting Windows.

> If you have activated the *Establish connection at Windows startup* feature please wait for the connection being established before logging on to Windows. Then you will be able to logon to the network.

If you have not enabled this option, proceed as follows:

(1) In the login choose the *Windows NT* tab.

Enable the option *Windows NT login only*.

The Novell Login will be launched again automatically after establishing a logical connection to a destination (each first connect). As soon as the user has done the Login, the ISDN Connection Manager will re-establish the mapped network drives on all attached servers. If there is any drive mapping on a server that is not attached by the login procedure, the restoration of the drives will stop. Alternatively you may use a NetWare login script.

> Please note that it may take some time (up to 60 sec.) until the Novell Login will show up after establishing the connection.

Perform the following steps to disable the automatic launch of the Login:

(1) In the *ISDN Connection Manager* choose the *Options* menu.

(2) Click on the option *Launch Novell IntranetWare login automatically*.

4 Functions of the ISDN Connection Manager

The ISDN Connection Manager is the core component of Columbus Client.

It is the starting point for all actions that you will take and for all information on previous and current connections.

The ISDN Connection Manager looks like this on your screen:

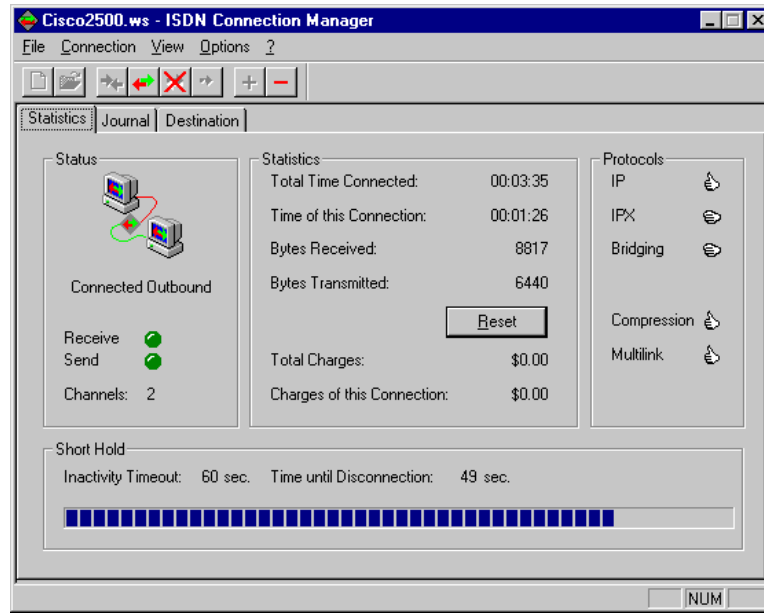


Fig. 4-1 The ISDN Connection Manager

4.1 Organization of the ISDN Connection Manager

The ISDN Connection Manager is divided into four areas:

① Menu Bar

② Toolbar

③ Tabs (Statistics, Journal, Destination)

④ Status Bar

These 4 areas are described in detail below.

4.1.1 Menu Bar

The *File* Menu

Menu Option	Meaning
Make New Connection	This option is used to create a new destination with the aid of dialog boxes.
Open	Use this option to open a destination.
[Created Destination: WS file]	The most recently used destination will be displayed.
Exit	Use this item to exit Columbus Client.

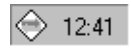
The *Connection* Menu

Menu Option	Meaning
Establish	Establish a connection to the selected destination.
Short Hold	Inactivity Timeout.
Disable	Terminate a connection both logically and physically.
Wait for Call	Use this option to prepare your PC to accept a call from a destination. Once a connection has been established from the *Wait for Call* state, and subsequently went into *Short Hold*, your PC might now establish connections in the outgoing direction, too.
Add Channel (only PPP with Multilink)	Add a B channel.
Remove Channel (only PPP with Multilink)	Remove a B channel.

The *View* Menu

Menu Option	Meaning
Toolbar	Display/hide toolbar
Status Bar	Display/hide Status Bar
Minimize Window	Use this option to hide the ISDN Connection manager. When the ISDN Connection Manager is hidden, the connection status is displayed as an icon in the Windows Task Bar (next to the clock).

The following icons can be displayed:

Task Bar Display Area	Meaning
	Short Hold
	Physical connection is established. The arrows will blink when data are sent or received.
	Connection is disabled.

If you point the mouse cursor on the Columbus Client logo, the destination, the status and the charges (if incurred) will be displayed:

Miller, Short Hold

You can redisplay the ISDN Connection Manager in two different ways:

1st Option

(1) Double-click on the Columbus Client logo in the Task Bar.

2nd Option

(1) Click the right mouse button on the Columbus Client logo in the Task Bar.

The following context-sensitive menu will appear:

(2) Click on *Show* to display the ISDN Connection Manager again.

The *Options* Menu

Menu Option	Meaning
Own station	Use this option to change the parameters of your own station (dial number, product key, ...) (see page 4-8)
ISDN Connection Manager	Here you can set the destination with which a connection is to be established automatically when Windows boots. Use this option also to deactivate and activate the acoustic signals.

Menu Option	Meaning
Regional Settings	This option will take you to the corresponding Windows dialog. There, you will set the date and time and the currency symbol which is to be used, and you will also set the date and time formats.
Network	This option will take you to the corresponding Windows dialog. You can view your network settings and change them as needed.

If you choose the menu option Own Station, the following dialog box will appear:

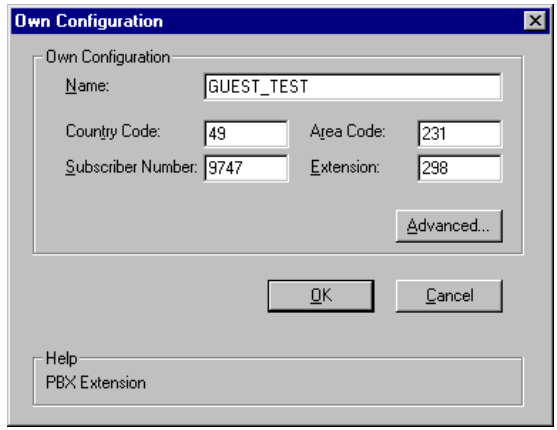


Fig. 4-2 Dialog box *Own Station Properties*

In the dialog box *Own Station Properties* click on *Advanced*.

The *Advanced* dialog box will appear:

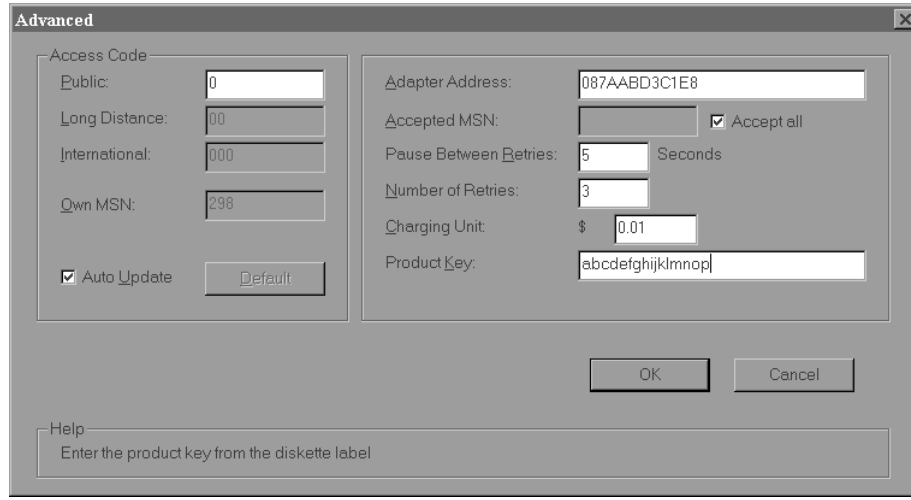


Fig. 4-3 *Advanced* dialog box

The parameters have the following meanings:

Entry	Meaning
Public	The number you need to dial to get the public telephone system dial tone from a PBX system. In some PBX systems this number can be 0, in others it can be 9.
Long Distance	The sequence of numbers you need to dial to make a long-distance call. In Germany, this is the 0, in the USA, 1 (from a public line).

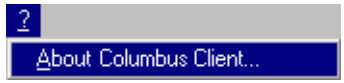
Entry	Meaning
International	The sequence of numbers you need to dial to make an international call. In Germany, this is the 00, in the USA, 011 (from a public line).
Own MSN	This parameter is only meaningful with some PBX systems. With these systems it is important for *outgoing* calls. Your user MSN indicates which Multiple Subscriber Number initiates a call. In the USA MSN resembles DN.
Auto Update	If *Auto Update* is activated, the values for the dial number are entered automatically. If this field is not activated, you can change the values yourself or you can click on *Default* o accept the preset values.
Default	Click this command button to apply the preset values.
Adapter Address	You do not need to change this parameter.

Entry	Meaning
Accepted MSN	This parameter is needed for *incoming* calls. This number determines which Multiple Subscriber Number of an ISDN line (with Euro-ISDN) or which terminal selection digit (with 1TR6) will have to be called from outside: in order to make Columbus Client accept the call. Activate *Accept all* to cause your PC to physically accept **all** (authorized) incoming calls with the proper service code. Please use the following settings if you have a number of devices which use *data services* and are attached to a *single* ISDN line: • When Euro-ISDN (DSS-1) is being used: Enter the MSN for your PC here. • When the 1TR6 protocol with a terminal selection digit is being used: Enter your PC's terminal selection digit here. The default setting is *Accept all*. In the USA MSN resembles DN.
Pause between Retries	Use this parameter to enter the minimum time in seconds which Columbus Client must wait between two retries to establish a connection. This time is important if the system tries to re-establish the ISDN connection after a Short Hold period and the first attempt was not successful.
Number of Retries	Number of dialing attempts This value indicates the number of dialing attempts which the system will make in trying to establish a connection. If these dialing attempts are not successful, you will have to establish the connection manually. Default value: 3

Entry	Meaning
Charging Unit	In this parameter you enter the charges for one billing increment. Set the currency under: *Options* → *Regional Settings*.
Product Key	The product key is displayed. You also find the product key on the label of the Columbus Client CD jacket.

The "?" Menu

Open the following menu:



It displays the version number and version date of Columbus Client.

4.1.2 Toolbar

If you place the mouse cursor on one of these icons, a window displaying the name of the command button will appear on your screen.

The table below lists the various icons that appear on the toolbar:

Icon	Meaning
	Make new connection
	Select destination
	Establish ISDN connection

Icon	Meaning
	Short Hold
	Disable ISDN connection
	Wait for incoming call
	Add a B channel (only with PPP Multilink)
	Remove a B channel (only with PPP Multilink)

4.1.3 Tabs (Statistics, Journal, Destination)

Statistics Tab

Click on the *Statistics* tab.

> You will find the status information in *Chapter* *2.1.3, Checking the Status of an ISDN Connection* (page 2-11).

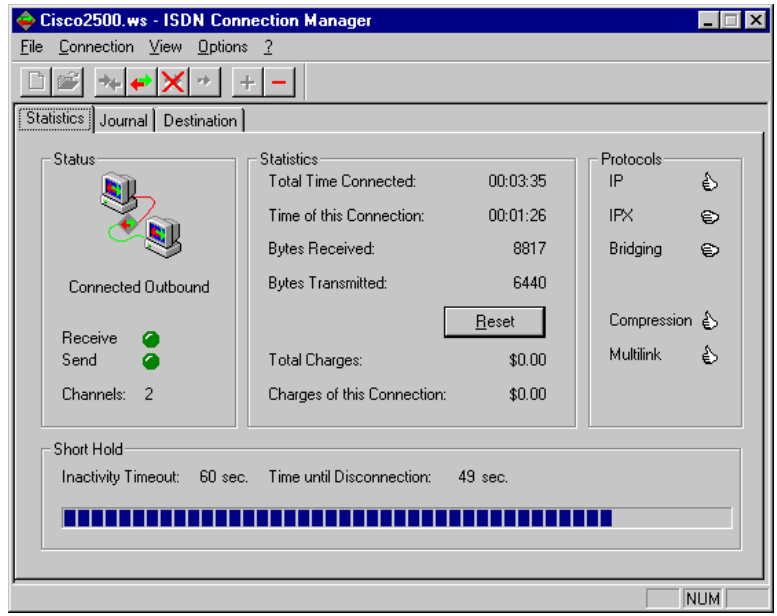


Fig. 4-4 *Statistic* Tab

The following connection information is displayed:

Status	Meaning
Receive	If the green *Receive* lamp is lit, Columbus Client is **receiving** data.
Send	If the green lamp is lit, Columbus Client is **sending** data.
Channels	The number of B channels currently established—i.e. which can be incurring charges at this time. If the value 0 appears, no B channels are established at this time.
Short Hold	Wait time is the time in seconds after which the ISDN connection will be torn down if no data is exchanged between the PC and the partner during this time interval (inactivity timeout). Only with ITK Connectivity Protocol: This value is the result of the matching procedure between the destination and your PC at the beginning of the communication. If both stations have different values for the Short Hold parameter, the lesser of the two is automatically used and displayed here. If the Short Hold mode is deactivated on *one* end, the Short Hold mode set on the other end is nevertheless used! Time remaining to connection de-establishment: Here, the time in seconds remaining until the connection will be torn down is displayed.
Total Time Connected	Total of all times over which an ISDN connection was established. Format: hours:minutes:seconds

Status	Meaning
Time of this Connection	Time during which the current ISDN connection has been active. Format hours:minutes:seconds
Bytes Received	Displays the number of bytes **received** for the entire logical connection.
Bytes Transmitted	Displays the number of bytes **transmitted** for the entire logical connection.
Reset	Sets the *Bytes Received* and *Bytes Transmitted* displays back to zero.
Total Charges (not in USA)	Charges for all connections up to now. This entry is not displayed with ISDN connections that do not have this capability—for example, with 5ESS/NI-1.
Charges of this Connection (not in USA)	Charges incurred so far for the current physical connection. If you have an Euro-ISDN connection (DSS-1), ask your telephone company or your network administrator to have charges information displayed. Find out whether your ISDN board reports charges to the PC application. **Important:** With PBX systems it may occur that the charges information is not passed all the way through to the ISDN board. In this case, the value will be 0, even though charges have been incurred. This entry is not displayed with ISDN connections that do not have this capability—for example, with 5ESS/NI-1.

In the protocol area the hand icon will tell you whether the protocol:

- is available 
- is **not** available 
- is **not** active 
- is currently being negotiated 

The individual entries have the following meanings:

Entry	Meaning
IP	IP protocol (Internet)
IPX	IPX protocol (Novell)
Bridging	Mac Layer Bridging (MLB): for transferring other protocols
Compression (Only with PPP)	 Transfer compressed  Do not transfer compressed  Not active
Multilink (Only with PPP)	 Channel bundling possible  Channel bundling not possible  Not active

Compression and Multilink are only displayed with the protocols if you have set PPP.

Journal Tab

Click on the *Journal* tab.

A *Journal* tab can, for instance, contain the following entries:

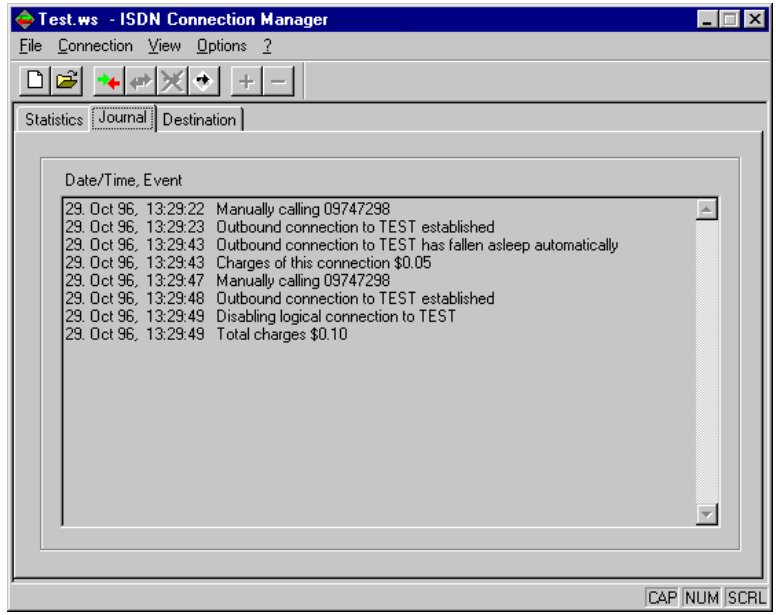


Fig. 4-5 *Journal* Tab

The individual entries have the following meaning:

Entry	Meaning
Date/Time	The date and time of the event are displayed here.
Event	Here you will find detailed information on: • The type of connection (outgoing connection established, outgoing connection torn down, call to…, error message, etc.) • Name of the destination • Charges incurred

Destination Tab

Click on the *Destination* tab.

This tab contains all the parameters for the destination. You can set and save these parameters for each destination.

You can change these parameters at any time. The changes do not take effect until the next **manual connection establishment**.

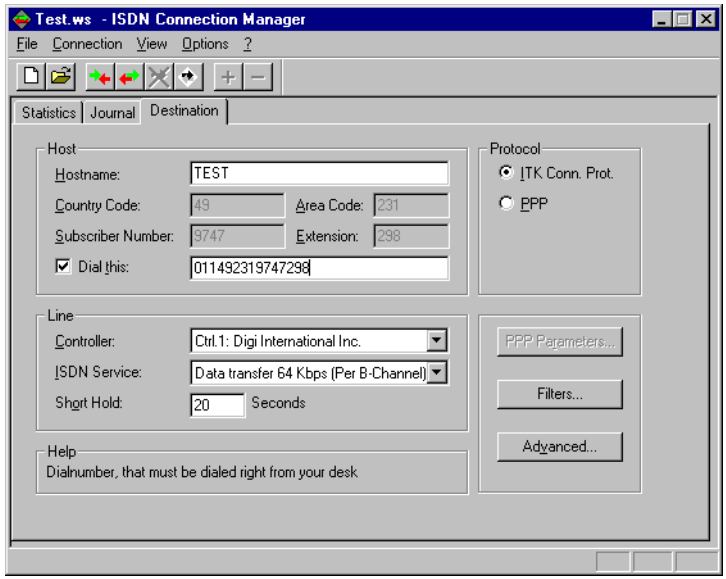


Fig. 4-6 *Destination* Tab

The entries have the following meaning:

Entry	Meaning
Hostname	Name of destination (maximum length 80 characters)

Entry	Meaning
Country Code Area Code Subscriber Number Extension	For detailed information, please refer to your *Installation Manual*, Chapter 2.2.1, *Installing Columbus Client under Windows 95,* section *Full Dial Number Scheme*. If you decided to *Use straight dial numbers* when you installed the software, only the *dial number* entry will appear here.
Dial this	This entry only appears with the full dial number scheme. If you have activated this box, please enter the dial number as a sequence of digits only.
Controller	This item can be used to select a particular ISDN or modem device (if used in conjuction with the CAPI Modem) to call this destination.

Entry	Meaning
ISDN Service	*Analog modem* *Rate adaption V.110 (GSM)* *Rate adaption V.120* *Data transfer rate 64 kbit/sec* (default value) *Data transfer rate 56 kbit/sec* (connections in the USA: depending on the destination) *X.75 with 64 kbit/s* *X.75 with 56 kbit/s* The *56 kbit/sec* data transfer rate is of importance only in the USA. Find out from your destination in the USA which data transfer rate to use, since both *64 kbit/s* and 5*6 kbit/s* are common. *X.75 (56/64 kbit/s)* may be used for connections to destinations supporting PPP over X.75 (e.g. ITK NetBlazer 5100, Compuserve, AOL). It provides reliable connections using the X.75 protocol. If the CAPI driver does not offer the choosen ISDN Service (e.g. CAPI modem driver only offers analog modem connections), an error message will be displayed at connection establishment.
Short Hold	The Short Hold is the time in seconds after which a connection is torn down if no user data were transmitted (inactivity timeout). Select a value which is somewhat less than the billing increment used for this line. Default value: 60 seconds
Help	Help information is provided on the boxes in which the mouse cursor is located.

Entry	Meaning
ITK Conn. Prot.	Activate *ITK Conn. Prot.* (ITK Connectivity Protocol) if Columbus Client or ITK NetBlazer 4400 is installed on the destination.
PPP	In all other cases, set PPP.

Clicking on the following command buttons will take you to the expansions listed in the tabs. There you can examine and edit additional parameters.

Command Button	Meaning
PPP Parameters	Click this command button to view and change the parameters for PPP.
Filters	Click this command button to check the filter/emulation settings. As a general rule, you should not change the default settings. Please note the warning message on page 4-27.
Advanced	Click this command button to enter or change advanced parameter or connection settings. The individual settings and their meanings are explained in Chapter 4.1, section *Advanced…* (page 4-28).

PPP Parameters

Click on the *PPP Parameters* command button.

The *PPP Parameters* dialog box will be displayed.

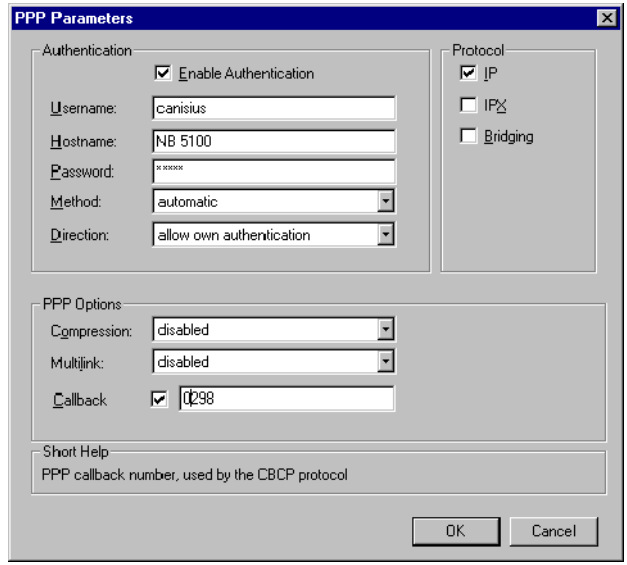


Fig. 4-7 PPP Parameters for the destination

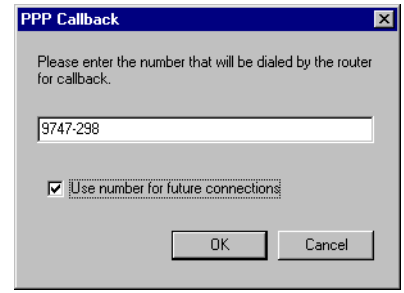
If you have set the destination as *PPP with Authentication* or *PPP without Authentication*, the default values will already be entered here. You can change them at any time.

The individual entries have the following meaning:

Entry	Meaning
Enable Authentication	By activating this box you can change the following five authentication parameters.
Username	Enter your own name for the authentication process (maximum 80 characters). You can enter a different name for each destination.

Entry	Meaning
Hostname	Enter the destination name for the authentication process (maximum 80 characters).
Password	Enter your password here for the authentication process (maximum 32 characters).
Method	The ISDN Connection Manager will detect the destination's configuration. So normally you should leave the default setting (*Automatic*) as is. In special cases, you can set which authentication process is to be used: PAP, CHAP or Microsoft CHAP.
Direction	Here you will enter whether you want to have the authentication conducted in one or both directions: allow own authentication (Default setting) Your authentication data are not sent unless the destination requests an authentication. Your own station will not request authentication by the destination. peer must authenticate The destination must authenticate itself to you or the connection will be terminated. In addition, your station will authenticate itself to the destination if requested to do so.
IP, IPX, Bridging	Here you can activate or deactivate the desired data transfer protocol. IP for connections to the Internet IPX for connections to Novell networks Bridging for other protocols

Entry	Meaning
Compression	Click on *Compression* to select the PPP data compression: disabled For Destinations that don't support the built-in compressions, like Windos 95 / NT. automatic If the compression methods supported by the destination are unknown, select "automatic". The PPP will try to adapt to the compression method of the destination. The connection establishment can take slightly longer in some cases. Predictor For Destinations that support the "Predictor" compression, e.g. Unix and Cisco routers. STAC LZS For Destinations that support the compression of STAC Electronics, e.g. Cisco routers.
Multilink	Set how the channels are to be bundled here: dynamic The B channels are automatically bundled depending on the data load. static If 2 B channels are available, 2 B channels are always bundled together. disabled (Default value) One and only 1 B channel is always used. The Multilink Protocol is not negotiated. Therefore, you cannot add additional B channels during the rest of the connection.

Entry	Meaning
Callback	Click on *Callback* to activate or deactivate PPP security callback. In each case a brief charge-incurring connection is established. If you are using the Microsoft Callback Control Protocol (CBCP) you can enter here the callback number to be dialed by the server. This number may differ from the number you set up for Columbus Client as your own number. If the number is empty, then you will be asked for the callback number during connection establishment.  This callback number will then be valid for the current session. By activating the option *Use number for future connections*, the entered number will be permanentely saved and is therefore valid for future connections. Please note: The Microsoft Call Back Protocol (CBCP) is not supported by ITK NetBlazer 4400. If you want to use the ITK MPR for ISDN or ITK NetBlazer callback option, you must configure callback on the router only, but not in your remote PC. This PPP parameter is ignored in this case.
Short Help	Help information is provided on the boxes in which the mouse cursor is located.

Confirm your changes by clicking on *OK*.

If you want to discard your changes, click on *Cancel*.

Filters

When you click on *Filters* a menu of filter and emulation settings will appear. Default settings will already appear here.

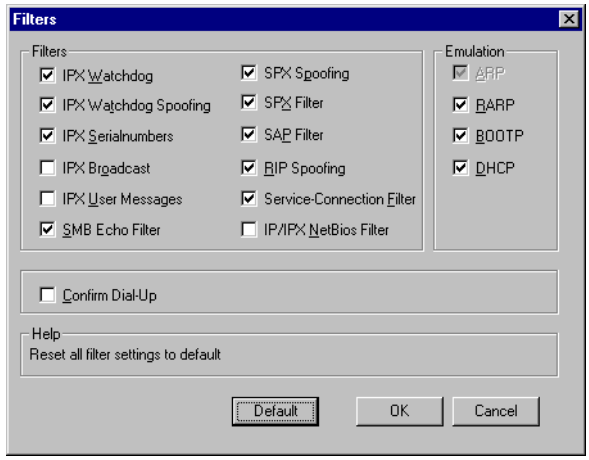


Fig. 4-8 Filter settings for the destination

Do not change the default settings. Only very experienced users should change them!

Improper settings can prevent the Short Hold feature from working properly, thereby resulting in unnecessary extra expenses.

Appendix B, *Filters*, provides explanations of the filters, spoofing and emulations.

Entry	Meaning
Confirm Dial-Up	If you activate this option, you will be prompted to confirm each dialing operation.
Help	Help information is provided on the boxes in which the mouse cursor is located.
Default	Click on this command button to return to the default settings.

Advanced...

When you click on *Advanced...* in the *Destination* tab, a menu containing advanced settings for the destination will appear.

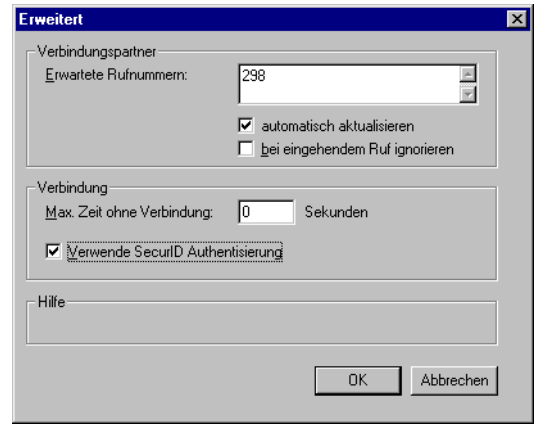


Fig. 4-9 Advanced settings for the destination

The individual entries have the following meaning:

Entry	Meaning
Expected Dial Numbers	Here you will enter the destination's permissible dial numbers. These are the numbers at which incomming calls will be accepted.
Auto Update	Only with full dial number scheme: When this function is active, the list of expected dial numbers is updated automatically.
Ignore Dialnumber at incoming call	When this function is active, the dial number of the incoming call is always accepted.
Maximum pause between connection	Enter the maximum Short Hold time in seconds here.
Use SecurID Authentication	If this option is enabled the support of Security Dynamics´ACE server is activated (see Appendix C, *SecurID (ACE) Client*)

4.1.4 Status Bar

If the mouse pointer is located on a menu command, a brief explanation of this menu command appears on the Status Bar. Error messages also appear in the Status Bar.
NUM means that the numerical keypad on your keyboard is active.

4.2 Summary of Functions

There are two ways to invoke a function:

1st Option

Click on the corresponding icon in the toolbar.

2nd Option

Open the desired menu and submenu in the Menu Bar.
Format: **Menu → Submenu**

Some of the functions can be opened by using keyboard shortcuts.

For example, <Ctrl>+<N> means:

Press the <Ctrl> key and the <N> key simultaneously.

The following table describes the functions of the ISDN Connection Manager that you can call up from the **menu** or **toolbar.**

Function	Meaning	Click on Icon	Open Menu → Submenu
Make new connection	You can use this option to create a new connection with the aid of dialog boxes.		**File → Make new Connection ...** or **<Ctrl>+<N>**
Select destination	Select a destination that is already present.		**File → Open...** or **<Ctrl>+<O>**
Establish ISDN connection*	Establishes a connection to the currently selected destination (*Destination* tab)		**Connection → Establish** or **F5**
Short Hold	Manually teardown current connection.		**Connection → Short Hold** or **F6**
Disable ISDN connection	Terminates a connection logically.		**Connection → Disable** or **F7**

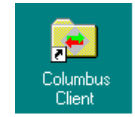
Function	Meaning	Click on Icon	Open Menu → Submenu
Waiting for incoming call	Use this option to prepare your PC to accept a call from a destination. Once a connection has been established from the *Waiting for incoming call* state, and subsequently went into *Short Hold*, your PC might now establish connections in the outgoing direction, too.		**Connection → Wait for Call** or **F8**
Add B channel (only PPP with Multilink)	Add B channels to an existing logical connection (only if the given destination is set up accordingly).		**Connection → Add Channel** or **Num+**
Remove B channel (only with PPP Multilink)	Remove B channels from an existing logical connection (only if the given destination is set up accordingly).		**Connection → Remove Channel** or **Num-**
Toolbar display/hide	Displays the toolbar, also hides it.		**View → Toolbar**
Status Bar display/ hide	Displays the Status Bar, also hides it.		**View → Status Bar**

Function	Meaning	Click on Icon	Open Menu → Submenu
Display ISDN Connection Manager as icon	Use this option to minimize the ISDN Connection Manager. The current connection state is merely displayed as an icon in the display area of the Windows Task Bar.		**View → Minimize Window**
Edit the parameters of your own station	Edit the following user parameters: Name, country code, area code, subscriber number, extension.		**Options → Own Station**
Edit advanced parameters	Edit advanced parameters. See the meanings of the advanced parameters on page 4-8.		**Options → Own Station → Advanced…**
Display information on Columbus Client	This menu displays the version number and version date of Columbus Client.		**? → About Columbus Client**

Tab. 4-1 Functions of the ISDN Connection Manager (menu and toolbar)

* To establish an ISDN connection to a **destination that has already been set up**, you can perform the following steps:

(1) Double-click on the *Columbus Client* folder.



(2) Use the right mouse button to click on the icon for the destination to which you wish to connect.

Click on the following in the context-sensitive menu: *Connect*

The connection to the destination you wish to connect to is now established.

Context-sensitive Menu

You can also use the context-sensitive menu to enter the settings for the destination.

Proceed as follows:

(1) Use the right mouse button to click on the icon for the destination which you wish to connect to.

The following context-sensitive menu will appear:

(2) Click on *Properties*.

The *General* and *Connecting Router* tabs will appear.

(3) Click on the *Connecting Router* tab.

Here you can set the same parameters as under the *Destination* tab in the ISDN Connection Manager.

5 Testing with the Digi_TEST Router

You now have the opportunity to test your installation by establishing a connection to the Digi_TEST Router in Dortmund, Germany. This is an especially good idea when you are not completely sure if your destination is already set up correctly.

It is assumed that you have installed the IPX protocol and that it has been bound to Columbus Client.

To establish a connection to the Digi_TEST Router in Dortmund (Germany), perform the following steps:

(1) Double-click on the *Columbus Client* folder.

(2) Double-click on the following icon:

The ISDN Connection Manager will be launched and will establish the connection to the Digi_TEST Router.

5.1 Login to Digi_TEST

We shall now briefly describe how to login or out from the Novell router Digi_TEST in Dortmund, Germany using Columbus Client.

Proceed as follows after you have established a connection to the Digi_TEST Router in Dortmund:

(1) Double-click on the *Network Neighborhood* icon on your Windows Desktop.

The *Network Neighborhood* window will appear; all the accessible Novell servers are listed.

(2) Double-click on Digi_TEST to login to the network.

The *Enter Network Password* window will now appear:

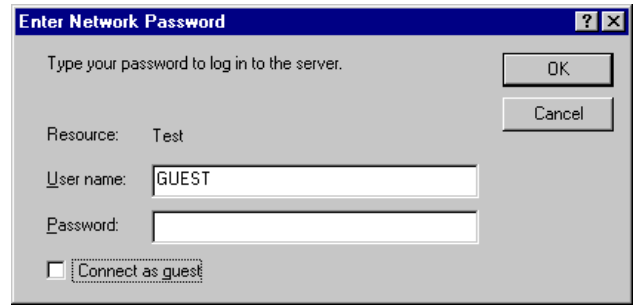


Fig. 5-1 *Enter Network Password* window for Windows 95

(3) Use the settings described above. You do not need to enter a password.

Confirm by pressing *OK*.

You are now logged into the Digi_TEST Router in Dortmund, Germany.

Please read Chapter 5.2, *What will I find on Digi_TEST? (page 5-4)* to learn about what you will find here.

If you are not able to access the Digi_TESTRouter, it is possible that all the B channels on the Digi_TEST Router happened to be busy at the time. In this case, you will have received an error message on the *Journal* tab. Please try again later.

Once this test is successful, perform the following steps before connecting to a different destination:

(1) Terminate the connection to the Digi_TEST Router by clicking on  .

(2) Restart Windows 95 / NT 4.0.

It is absolutely necessary that you **restartWindows 95 / NT 4.0** at this point since the Microsoft IPX protocol cannot handle a changing network address.

5.2 What will I find on Digi_TEST?

On the Digi_TEST Router you will find the current software for various products in the appropriate subdirectories:

```
\\Digi_test\ver\release\
```

If you have logged in as a GUEST, you can download the current update of your software without needing a password.

In case you want to send us E-Mail messages, here is our E-Mail address:

```
support@itk.de
```

You can also find current information and the latest software versions on the Internet:

www.itk.com

6 Troubleshooting

The most commonly occurring problems encountered with Columbus Client are described in the next few pages. Possible causes of each problem and strategies for correcting the problems are explained here.

6.1 Connection Establishment

If a connection to a destination is not established, perform the following **standard checks**:

1. Try to establish the connection at least one more time. Perhaps all the B channels on your destination were busy.
2. Check the journal to see which dial number was actually dialed. The journal will contain an entry like *Manual connection establishment to 02319747298*.
3. Check the settings on your ISDN board. Have you selected the correct D channel protocol?
4. Check whether the ISDN service *data transfer rate 64 kbit/sec* or *56 kbit/sec* offered by your ISDN service provider (e.g. Deutsche Telekom AG) is properly set for your line and whether the correct ISDN service is set in the configuration of the destination. You can read about this in Chapter 4.1, section *Destination Tab* (page 4-19).
5. For the USA only:

   Check whether your SPIDs and DNs have been entered correctly in your ISDN Adapter Network Property tabs and whether the correct services have been assigned to the respective SPID (for Columbus Client at least one *data SPID* must have been assigned). Your phone company provides you with one or more SPIDs upon subscription.
6. Check whether the call is reaching the proper ISDN line by using the debugging properties provided on this line. Make sure that the destination is correctly configured for accepting calls.

7. Check whether other ISDN devices are connected to your destination. These devices could be taking over the incoming call. The first test to be performed is to disconnect all other ISDN devices from your line and from your destination.
8. Check whether your ISDN connection has the specified standard configuration—for example: point-to-multipoint configuration (bus configuration).

Callback (not PPP Callback!)

If your destination is set to callback, your call is rejected immediately and your destination calls you back so that no telephone charges are billed to your line. If this callback does not occur, there are a number of possible causes:

1. If an incoming call was rejected by the ISDN Connection Manager, this will be displayed in the Journal. If this is the case, check the following settings depending on which message is displayed:
   - Incoming call with wrong MSN (in the USA MSN resembles DN)
   - Select the menu command *Options* → *Own Station*... and click on *Advanced*

     The MSN which is accepted by the ISDN Connection Manager is displayed in the *Accepted MSN* box. Change the MSN as needed, or click on *Accept all*.
   - Incoming call with illegal dial number

     Check the dial number that is displayed to be sure it matched the destination configuration.

     Select the *Destination* tab and click on *Advanced*. The numbers which are accepted by the ISDN Connection Manager are displayed in the *Incoming Dial Numbers* box.

     Click on *Ignore Dialnumber at incoming calls* if each incoming call should be accepted.
   - Incoming call with incompatible ISDN service

     If the incoming call is set to the ISDN service *data transfer rate 56 kbit/sec* and a *data transfer rate 64 kbit/sec* is set in the configuration for your destination, the ISDN Connection Manager will not be able to accept the call. Change the setting of the destination on the *Destination* tab as needed.

2. Check the destination settings. The destination must be configured for callback and must identify your station based on the dial number communicated. First, check the dial number communicated to the destination by Columbus Client. To accomplish this, select the menu command *Options* → *Own Station* and click on *Advanced*. The MSN of your station that is communicated to your destination appears in the box *Own MSN*. You should also look at your destination's corresponding properties to check which dial number your destination is expecting to receive from your station.

Point-to-Point Protocol (PPP)

Make sure that the destination is communicating using PPP and that both sites are using the same network protocols.

When connections are being established, the *Statistics* tab displays the status of the protocols. During the *Identification* connection status, you can look at the *thumb* icons to ascertain which protocols have been deactivated, i.e.

- are not configured for this destination  ,
- which protocols are currently being negotiated 
- and which have already been negotiated  .

Modem Connection

In case you fail to establish a modem connection to your destination, the following messages may be shown in Columbus Client's journal:

1. *IXNDIS_LISTEN failed*

   This may be caused by a switched-off or misconfigured modem.

2. *Protocol Error Layer 2* or *Protocol Error Layer 3*

   This may be caused by a busy modem (modem resource is used by another windows application) or the called destination is busy.

6.2 Network Access

If you do not have access to the remote network, despite having successfully established a connection, this is generally due to an error in the network configuration of your destination or of your station.

Networks using the IPX Protocol (e.g. NetWare)

1. If you have set PPP, check in the *Statistics* tab whether the IPX protocol has been successfully negotiated with the destination  . If you see the symbol  in the IPX protocol, change to the *Destination* tab, click on *PPP Parameters*, and activate the IPX protocol.
2. In the network configuration in the IPX/SPX-compatible protocol, check whether the framing type is set to *Ethernet II*. To accomplish this, start the Control Panel and double-click on the *Network* icon.

Select the entry *IPX/SPX-compatible protocol* → *Columbus Client* and click on *Properties*. Select the *Advanced* tab, then click on the property *Frame Type* and set *Ethernet II* in the *Value* box.

3. If you have already established a connection with another destination and you accessed the network using the IPX protocol, you must reboot your computer. Windows 95 remembers the IPX network number used for the first IPX data traffic. No further changes can be made to this network number during the current Windows session. As a result, Windows 95 uses the wrong network number when connecting to another destination.

Networks using the TCP/IP Protocol

1. If you have set PPP, check in the *Statistics* tab whether the TCP/IP protocol has been successfully negotiated with the destination  . If you see the symbol  for the TCP/IP protocol, change to the *Destination* tab, click on *PPP Parameters* and activate the TCP/IP protocol.
2. If an error with IP address negotiation is displayed in the journal after a connection has been successfully established, check the configuration of the TCP/IP protocol. To accomplish this, start the Control Panel and double-click on the *Network* icon.

   Select the entry *TCP/IP* → *Columbus Client* and click on *Properties*.

   If your destination's administrator has given you an IP address and a subnet mask, these must be entered in the *IP address* tab. If you have not received an IP address and a subnet mask, select the setting *obtain IP address automatically*. Change to the *Gateway* tab.

   If your destination's administrator has given you a gateway address, enter this in the *New Gateway* box and click on *Add...*. This address should be the first entry in the *Installed Gateways* box. Change to the *DNS Configuration* tab. The *Enable DNS* setting must be selected, a name for your computer must be entered in the *Host* box, and at least one address must be entered in the *DNS Server Search Order* box. You will receive these from your destination's administrator.
3. If your destination is using the DHCP protocol to assign IP addresses, the DHCP emulation in the configuration of your destination (ISDN Connection Manager) must be deactivated. To accomplish this, select the *Destination* tab and click on *Filters*. Deactivate *DHCP* in the *Emulation* box 

   .

6.3 Short Hold

A de-established connection is re-established automatically when data are to be transferred. If this takes place even though you did not access any network resources, check the following settings:

1. Select the *Destination* tab and click on *Filters*. Click on *Default* to reset the filter settings to the default values. If the filters are set to values other than the default values, the ISDN Connection Manager can no longer distinguish reliably between genuine data traffic and data packets which are to be filtered out.
2. If you have activated *File and Printer Sharing* in the Windows 95 network configuration, Windows will have added the *File and Printer Sharing for NetWare Networks* service or the *File and Printer Sharing for Microsoft Networks* service to the network configuration. This service must be used if other users wish to access your computer via the network connection. If you do not need this service, remove it from the network configuration. Otherwise, click on *Properties* and check the following settings:

   If you are using *File and Printer Sharing for NetWare Networks* select ...

   - the entry *SAP Advertising* in the *Properties* box (*Workgroup display* must be disabled). The *Value* box should contain *Enabled, will not be master*.

   If you are using *File and Printer Sharing for Microsoft Networks*, select ...

   - the entry *LM Announce* in the *Property* box (the *Value* box should contain *No*).
   - and the entry *Browse Master* in the *Property* box (the *Value* box should contain *Disabled*).

The following situations also result in network traffic and therefore cause a connection establishment:

- When opening and closing an *MS-DOS Prompt*, Windows 95 checks all network drives to which a drive letter has been assigned. The same applies to many 16-bit applications.
- When accessing any folder (including the Windows Desktop), Windows checks all links in this folder. This means that tests are carried out as to whether the destination of a link is still present. If a link points to a network resource, this checking procedure generates data traffic.

  Accessing a folder means, for example, displaying the contents of the folder in Explorer or in the *File* → *Open* dialog of a program. You must therefore avoid using links to resources in the network.
- Programs which access network resources on a regular basis also result in a connection establishment. This includes, for example, mail programs which check whether any new mail has arrived.

A Messages

Various messages can appear in the Columbus Client Journal in addition to a log of connection establishment and de-establishment. Most of these messages are generated by the ISDN switch or the PBX system. They indicate errors which occur during initialization or connection establishment.

The most frequent errors are listed below, together with their causes and recommended ways of correcting the problem.

If other messages appear whose meanings are not obvious, please contact your dealer.

A.1 Messages generated upon Initialization

No CAPI driver "filename" present

Your ISDN board is not installed correctly, or it does not support CAPI 2.0.

What to do:

- For Windows 95: A file named VCAPID.VXD must be present in the system folder.
- For Windows NT 4.0: A file named IXCAPI.SYS must be present in the folder \SYSTEM32\DRIVERS\

No network protocol bound on Columbus Client

No network protocol is associated with Columbus Client.

What to do:

- Install a protocol using the menus *Control Panel* → *Network*. You will need to use the *IPX/SPX protocol* to access a Novell server. To access the Internet, use the *TCP/IP protocol*.

ixNdis.VxD not found (Windows 95)
ixNdis.Sys not found (Windows NT 4.0)

The ISDN Connection Manager could not find the file IXNDIS.VXD / IXNDIS.SYS.

What to do:

- Check whether the network configuration contains an entry called Columbus Client. If not, reinstall Columbus Client.
- Open the Control Panel and double-click on the *System* icon. Select the *Device Manager* tab. Under the heading *Network Adapters select Columbus Client* and click on *Properties*. Under the *Device Status* heading check whether Columbus Client is ready to use. Under Windows NT 4.0 further information can be found in the *Event Log*. For further hints refer to your Windows NT 4.0 documentation. If Columbus Client is not ready to use, check your ISDN card documentation.

A.2 Messages generated upon Connection Establishment

Messages from the ISDN Connection Manager generated upon Connection Establishment

`No ISDN route to specified transit network`
`No ISDN route to destination`

The ISDN connection could not be established since the destination address which was dialed is not valid.

What to do:

- Check the dial number for the given destination and repeat the dialing operation. The selected dial number is displayed in the Journal upon connection establishment.

`Destination busy`

The destination that you dialed is busy.

What to do:

- Make certain that the destination is activated and has at least one B channel available for data communication.

`Destination is not ready`

The destination that you dialed is not responding.

What to do:

- Make sure that your destination has its router switched on, or check the dial number of the destination that you are dialing. Make certain that the destination's router is configured properly so that your destination can accept the incoming call.

`Call rejected by destination`

The destination has rejected your call. If you are using callback, this message is normal.

What to do:

- Check the communication authorization used by your destination. It may be that your destination is using incorrect entries for its authorized destinations.

`Dial number has changed`

The dial number of your destination has changed.

What to do:

- Inquire about the new number.

`Requested ISDN service unavailable`

Your destination's terminal is not ready.

What to do:

- Retry the dialing operation. If the error persists, check whether your destination is in service.
- In the USA: check whether the DN is assigned to a SPID with data service

`Another CAPI application got that call`

The ISDN Connection Manager tried to accept an incoming call, but the other application in the same PC was faster and accepted the task instead.

What to do:

- Remove the other application from memory or make certain that the ISDN Connection Manager and the other application do not interfere with each other.

`Incoming call with incompatible ISDN service`

An incoming call is rejected since the services code is not supported. Columbus Client supports the ISDN services *data transfer 64 kbit/*sec and *56 kbit/sec, bit rate adaption V.110, bit rate adaption V.120* and *analog modem connection*.

What to do:

- Check whether the ISDN service that you have selected for your destination matches the ISDN service that your destination is actually using. To check the ISDN service of your destination, switch to the *Destination* tab. The ISDN service that is being used is entered in the *ISDN Service* box.

`Incoming call with restricted dial number`

Columbus Client has detected an incoming call whose dial number is not being accepted.

What to do:

- Switch to the *Destination* tab and click on *Advanced*. The numbers that are accepted by the ISDN Connection Manager are displayed in the *Incoming Dial Number* box.
- Activate *Ignore Dial number at incoming calls* if the ISDN Connection Manager is to accept all calls, or enter the dial number in the *Incoming Dial number* box.

Incoming call with wrong MSN

Columbus Client has detected an incoming call having the wrong MSN (respectively DN). In other words, the MSN (DN) which is determined for the incoming call does not match the MSN (DN) set in the ISDN Connection Manager.

What to do:

- Select the menu command *Options* → *Own Station* and click on *Advanced*. Enter the MSN (DN) which is to be accepted by the ISDN Connection Manager in the *Accepted MSN* box, or select *Accept all*.

Address negotiation failed: No IP address obtained
Address negotiation failed: No gateway address obtained

Your system's TCP/IP protocol expects that the ISDN Connection Manager will provide it with an IP address for your system and an IP address for your destination (default gateway). These addresses were not communicated when the connection was established.

What to do:

- Change the configuration of your destination so that the PPP option *IP Address Negotiation* is supported.
- For the TCP/IP protocol enter an IP address and a gateway address in the network configuration. You will receive these from your destination's system administrator.

Negotiated IP address differs from preconfigured address
Negotiated gateway address differs from preconfigured address

An IP address and a default gateway address are configured in your system's TCP/IP protocol. When the connection was established, other IP addresses were communicated by your destination. It is now possible that applications based on TCP/IP will not function properly.

What to do:

- If your destination's system administrator has given you an IP address and gateway address to use, check these addresses in the network configuration of the TCP/IP protocol, or
- In the Windows 95 network configuration set the TCP/IP protocol to *Obtain IP Address Automatically.* PPP must be set in the ISDN Connection Manager.

`Error D channel Layer 1 - Cable may be broken`

The communication between the ISDN board and the ISDN switch failed.

Possible Cause

- The cable leading to the ISDN network termination (NT) is not plugged in on one of its ends, or the cable itself is defective.
- The ISDN connection to the switch is not in operation or is defective.

What to do:

- Check the ISDN cable to be sure it is connected properly; also inspect it for mechanical damage. For example, use a different ISDN device on the same BRI bus to check whether the connection to the ISDN switch is working properly, and, as a last resort, try using a different ISDN cable between the ISDN NT and your PC board.

`Error D channel Layer 2 - possibly ISDN-line misconfigured`

A *D channel layer 2* connection could not be established between your ISDN board and the ISDN switch.

Possible Cause

- The ISDN board is configured incorrectly, or the ISDN line is configured incorrectly, especially in the case of PBX systems.

What to do:

- Check to be certain that the ISDN line configuration matches the terminal (ISDN board) configuration. Make certain that the point-to-point connection or the point-to-multipoint connection is set up properly.

`Error D channel Layer 3 - Possibly wrong protocol`

A *D channel layer 3* connection could not be established between your ISDN board and the ISDN exchange.

What to do:

- Check whether the correct protocol is set in your ISDN board's configuration.

For USA only:

- With NI-1 and 5ESS connections, check whether the DN is assigned to a SPID with data service

PPP Messages from the ISDN Connection Manager

`CHAP Auth. failed - remote not configured`

This problem is only encountered in conjunction with CHAP authentication. The destination is not configured for CHAP.

What to do:

- Do not use CHAP. Instead, set the authentication method to *Automatic* or *PAP* in the *PPP Parameters* in the ISDN Connection Manager.
- Change the configuration of your destination in such a way that CHAP can be used.

`PAP Auth. failed - remote not configured`

This problem is only encountered in conjunction with PAP authentication. The destination is not configured for PAP or does not support PAP.

What to do:

- Do not use PAP. Instead, set the authentication method to *Automatic* or *CHAP* in the PPP parameters in the ISDN Connection Manager.
- Change the configuration of your destination in such a way that PAP can be used.

`PAP Auth. failed - remote sent incorrect password or peer name`

The destination has sent an invalid password, or the name sent by the destination is incorrect.

What to do:

- Check whether the password for this connection was entered correctly on your destination's system.
- Also check the entries on your own system:
  - on the *Destination* tab: the name of the destination
  - in the PPP parameters under *Authentication*: the name and password of your destination

`PAP Auth. failed - password/peer name rejected by remote system`

Your system has sent an invalid password or the wrong name to the destination.

What to do:

- Check:
  - on the *Destination* tab: the name of the destination
  - in the PPP parameters under *Authentication*: your name and password
  - if you are using CHAP: the name of your destination must be correct and identical to the name sent by your remote partner.

Authentication failed - peer requested CHAP
Authentication failed - peer requested PAP

Your system and the destination are configured for different authentication procedures.

What to do:

- Under *Authentication* in the PPP parameters: check which method is set. Select that method that is set on your destination, or select *Automatic* to leave it up to the ISDN Connection Manager to select the method.

Authentication failed - peer is not able to authenticate himself

You have set the PPP *Direction* parameter to *peer must authenticate*, but your partner cannot authenticate itself to your system.

What to do:

- Change your destination's configuration so that it can authenticate itself on your system using the PAP or CHAP method.
- If the destination cannot authenticate itself on your system, in the PPP parameters change *Direction* to allow own authentication.

Waiting for PPP callback from destination

Columbus Client waits for callback from the destination after PPP callback was agreed-upon.

Timeout waiting for PPP callback from destination

You have set the callback option in the PPP parameters, but your destination did not call back within 10 seconds.

What to do:

- It is possible that all the B channels on your ISDN line are currently busy. Check whether you have a B channel free and try again.
- It is also possible that the destination does not have any B channels free for the callback. Try again.

B Filters

B.1 Overview

To prevent a connection that was torn down under Short Hold from being set up unnecessarily, Columbus Client must decide whether data packets are to be sent to the destination or filtered out, i.e. not transmitted.

There are three different procedures used by Columbus Client to ensure that the Short Hold feature operates properly.

- **Filters**

  recognize packages which do not absolutely need to be transmitted.

  For a connection which is torn down under Short Hold, these packets will be filtered out in order not to transmit them.

  Example: SAP packets are sent to all the computers in a LAN to report the user's own services.

  For an established connection the Short Hold timer is not reset for such packets.

  Normally, each packet received or sent causes the Short Hold time to be reset. In other words, the time until the connection is torn down is reset to the Short Hold time used in the configuration settings.

- **Spoofing mechanisms**

  Spoofing is an expansion to the filter functionality:Columbus Client generates local responses to data packets when the line is in Short Hold. These responses are the same as the responses which a remote computer sends when a connection is established.

- **Emulations**

  In an emulation, functions which are normally performed by a remote server in a network are simulated by the emulation—assigning IP addresses, for example.

B.2 Filter and Spoofing Mechanisms

The filters are described here briefly for experienced users. You can set which filters you want to use by clicking on the *Filters...* command button in the *Destination* tab.

IPX Watchdog (Filter)

Computers which provide NetWare file server functionality—in other words, NetWare servers or also Windows 95 computers using file and printer sharing for NetWare networks—regularly use *IPX watchdog packets* to check whether an already logged-in client is in fact still present on the network. These packets are sent when no data have been transferred for a given time.

IPX Watchdog Spoofing

In a Windows 95 / NT 4.0 system, file and printer sharing for NetWare networks can provide file server functionality for other NetWare clients or Windows 95 / NT 4.0 computers. In this case your system itself sends IPX watchdog packets to check whether already logged-in clients are still present. If the physical connection has been de-established, Columbus Client simulates (spoofs) the response to these packets.

IPX Serial Numbers (Filter)

NetWare servers regularly send packets containing their serial numbers to check whether the same software is being used on a number of servers.

IPX Broadcast (Filter)

If Columbus Client receives IPX broadcast packets, the Short Hold timer is not reset. IPX broadcasts that are sent when the physical connection is not established are discarded.

IPX User Messages (Filter)

If Columbus Client receives IPX user message packets, the Short Hold timer is not reset.

SMB Echo Filter

If the client for Microsoft networks is used, so-called *SMB echo packets* are sent out at regular intervals. These packets are discarded when the physical connection is not established.

SPX Spoofing

SPX connections are checked at regular intervals by corresponding polling packets. If the physical connection is de-established, these packets are answered locally (spoofed) to simulate an established connection when SPX is used on your system.

It is important that this option is supported by the destination, too.

SPX Filter

When a physical connection is present, SPX polling packets do not cause the Short Hold timer to be reset.

SAP Filter

Novell servers use the **S**ervice **A**dvertising **P**rotocol (SAP) to make their own services (file servers, etc.) known to the network. If a physical connection is not present, SAP packets are discarded. If the physical connection is present, the Short Hold timer is not reset for SAP packets.

RIP Spoofing

The **R**outing **I**nformation **P**rotocol (RIP) is used by NetWare servers to exchange routing information. The Windows 95 / NT 4.0 client for NetWare networks sends RIP requests from time to time. These requests are answered with default values if the physical connection is not established.

Service Connection Filter

The Windows 95 / NT 4.0 client for NetWare networks sends NCP Destroy Service Connection packets. This occurs some time after a service connection is no longer needed, and not immediately thereafter. If the physical connection is not established, these packets are discarded.

IP/IPX NetBIOS Filter

If the client for Microsoft networks is used via TCP/IP or IPX, NetBIOS name packets are sent at regular intervals. These packets are discarded when the physical connection is de-established.

B.3 Emulations

The emulations are described here briefly for experienced users. You can set which emulations you want to use by clicking on the *Filters*... command button in the *Destination* tab.

ARP Emulation

The **A**ddress **R**esolution **P**rotocol (ARP) is used to find out which physical network adapter address is used by a computer whose IP address is known.

Using PPP:
PPP is not able to transmit these packets. Thus, if your system attempts to resolve this address, the response is emulated by Columbus Client.

Using ICP:
Since the destination can detect and store the physical network address of the sender when an ARP request is received, no ARP emulation is performed in the ITK Connectivity Protocol. This ensures that the router will be able to correctly pass on IP packets for your system.

RARP Emulation

The **R**everse **A**ddress **R**esolution **P**rotocol (RARP) is used by your system to receive its own IP address in cases when only its own physical network adapter address is known. If your system sends an RARP request, Columbus Client emulates the response. In order to be able to do this, it must know your IP address. You have to use PPP or must have entered your address in the TCP/IP protocol in order for the IP addresses to be exchanged when the connection is established.

RARP is irrelevant if the Microsoft TCP/IP protocol is being used.

BOOTP Emulation

As with the RARP protocol, a system can get its own IP address from a BOOTP server by using the Bootstrap protocol (BOOTP). In this case, Columbus Client emulates the response to a BOOTP request. For this to happen, your computer's IP address as well as the IP address of the destination must be known.

You have to use PPP or must have entered your address in the TCP/IP protocol in order for the IP addresses to be exchanged when the connection is established.

BOOTP is irrelevant if the Microsoft TCP/IP protocol is being used.

DHCP Emulation

The Microsoft Windows 95 TCP/IP protocol uses DHCP to get an IP address for your own system and for the destination (default gateway). In this case Columbus Client emulates the response to DHCP packets and thereby reports the IP addresses to the TCP/IP protocol. For this to happen, your computer's IP address as well as the IP address of the destination must be known. You must use PPP in order for the IP addresses to be exchanged when the connection is established.

C SecurID (ACE) Client

The Security Dynamics ACE Server offers a safe method for user authentication via a special SecurID Login Procedure. This procedure can be started as described in the following.

Activating the SecurID Authentication

(1) Click on the *Destination* tab.

(2) Click on the button *Advanced....*

(3) Click on the option *Use SecurID Authentication.*

The check mark indicates that the SecurID method is used.

If the ACE server support is activated, it is automatically checked, if an ACE Server is the remote partner. If this is the case, the authentication procedure described below will be executed. Then the PPP connection will be established. In case of a PPP Multilink connection, an authentication for each B channel is required.

Effecting the SecurID Authentication

An authentication window for your Username and Passcode appears.

Fig. C-1 Dialog for Authentication

(1) Enter your Username and Passcode.

Detailed information about the composition of your Passcode can be found in the ACE documentation.

(2) If you want that your Username will be preset upon connection establishment, activate the option *Remember username*.

(3) Confirm with *OK*.

The ACE Server checks your values. If the authentication was successful, the PPP negotiation will proceed as usual.

ACE Authentication fails

If the authentication fails an error message window is displayed. The authentication can be retried 3 times before the ISDN connection will be dropped finally.

During the next connection establishment you will be asked for Username and Passcode again. As soon as the authentication is successful after the failed attempts, the following dialog is displayed.

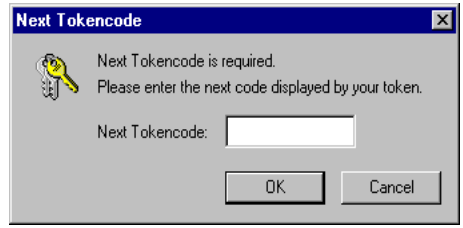


Fig. C-2 Dialog for next Tokencode

(1) Wait for the Tokencode to change on your ACE Token.

(2) Now enter the new Tokencode.

(3) Click on *OK*.

If no PIN has been assigned before you log in, the following dialog appears

Fig. C-3 Dialog for entering new PIN

(4) If you want the ACE Server to create the PIN, activate the appropriate option. Proceed with step **(6)**.

(5) If you want to enter the PIN, activate the option *I will create PIN*. Enter your PIN in the *PIN* and *Confirm* fields.

(6) Wait for the Tokencode to change on your ACE Token.

(7) Click on *OK.*

(8) Confirm the following step by clicking on *OK*

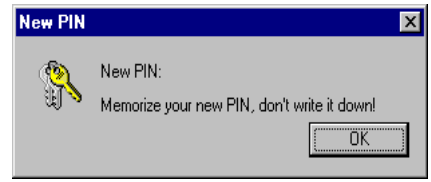


Fig. C-4 Dialog for memorizing new PIN

(9) Now pass through the authentication procedure with the newly defined PIN.

In case you are using channel bundling (PPP Multilink) please recognize that each channel needs to authenticate separately.

After the first authentication wait until the Tokencode changes for the second authentication.

Because of an error of the ACE Client on the RAS Server, it is possible that the second authentication fails and needs to be repeated. The repetition will be successful if entered correctly.

If you would like to use the callback option, only **one** authentication procedure needs to be performed. Outgoing calls from the server generally do NOT require an ACE authentication.

Glossary

This glossary contains brief explanations of key technical terms.

Active ISDN board	ISDN board with on-board processor
Analog mode connection	can be established using either CAPI modem driver or as emulation via ISDN (only in connection with the Columbus Card driver V2.30a or newer).
Apple Talk	Protocol used for connections between Apple computers.
B channel	An ISDN transmission channel used to transfer user data (voice, data, video)
BSS	**B**asic **S**ecurity **S**ervice A subscriber authentication is used for determining which destinations will be allowed to access the ISDN dial-up network. If an incoming call is coming from an ISDN dial number that is not found in the authentication table, the call is rejected immediately.

BRI

Basic **R**ate **I**nterface

Basic ISDN and basic Euro-ISDN line, also referred as S_0 line.

This is the most commonly used ISDN system offering one D channel and two B channels.

The two B channels can be used independently of one another to transmit voice, text, data and graphical information. The D channel is a control channel. It establishes and de-establishes the connection.

CAPI

Common ISDN **A**pplication **P**rogramming **I**nterface

A software interface which allows the ISDN board to communicate with applications and vice versa (for example: Columbus Client).

CAPI is an international standard: Version 2.0 is based on the European ISDN standard DSS-1.

CBCP

Microsoft **C**all**b**ack **C**ontrol **P**rotocol

Windows NT or Windows 95 Servers offer extended PPP callback features. Usually, the PPP callback server needs to know the Columbus Client callback number. With CBCP, the number can be specified by Columbus Client to the remote partner. This number can be entered in the PPP dialog, or, if the dialogfield is left blank, it can be specified during the connection setup in a separate dialogue.

Channel bundling

If needed, the B channels are bundled so that they can be used in parallel. With 2 B channels, the seeming result for the application software is a single transmission channel having a theoretical maximum speed of 2 x 64 kbit/sec (respectively 2 x 56 kbit/sec).

CHAP

Challenge-**H**andshake **A**uthentication **P**rotocol

An authentication method used within PPP in which passwords are transferred in encrypted form.

DN

Directory **N**umber

Resembles the MSN for US D channel protocols NI-1, 5ESS …

Each DN is assigned to a SPID therefore to a certain service (voice, data …)

EAZ

Endgeräte-**A**uswahl-**Z**iffer
(Terminal Selection Digit)

The EAZ is a feature of the German ISDN D channel protocol 1TR6. It is used to select terminals directly.

The terminal selection digit can be set from the application software (Columbus Client, for example).

E-Mail

Global electronic mail, mainly sent and received over the Internet.

ESS

Extended **S**ecurity **S**ervices

ESS is a security mechanism for data transmission (only with active ISDN boards).

FTP	**F**ile **T**ransfer **P**rotocol FTP is used to transmit data between a wide variety of systems. FTP is a very efficient application which only provides basic data transmission commands.
GSM	**G**lobal **S**ystem for **M**obile Communications Standard for mobile data communication (e.g. mobile phones)
Internet	A global computer network offering such services as WWW, E–Mail, FTP
IP	**I**nternet **P**rotocol The Internet Protocol transports individual data packages to a receiver across various networks.
IPX	**I**nternet **P**acket e**X**change A network protocol used by Novell.
ISDN	**I**ntegrated **S**ervices **D**igital **N**etwork A group of standards used to simultaneously transmit voice, data and video in digital form. The most frequently used ISDN system (in Germany: BRI) carries one D channel for signaling and two B channels for user data over the same copper wires. The transfer rate in Germany is 64 kbit/sec and in the USA 56 kbit/sec or 64 kbit/sec.
ITK Connectivity Protocol	An extremely efficient data transfer protocol.
ITK MPR for ISDN	**ITK M**ulti**P**rotocol **R**outer

ITK RAR 4000	**ITK** R**emote** A**ccess R**outer Now called ITK NetBlazer 4400
LAN	**L**ocal **A**rea **N**etwork A *local* computer network within a corporate site.
MLB	**M**ac **L**ayer **B**ridging A transfer protocol
MS CHAP	**M**icrosoft **C**hallenge-**H**andshake **A**uthentication **P**rotocol An authentication method used within PPP in which passwords are transferred in encrypted form.
Multilink Protocol	The Multilink Protocol is one of the PPP standards. It is needed to bundle B channels in the ISDN network.
NDIS	**N**etwork **D**evice **I**nterface **S**pecification Programming interface for network driver software
PAP	**P**assword **A**uthentication **P**rotocol An authentication method within PPP in which passwords are transferred in plain text form.
PPP	**P**oint-to-**P**oint **P**rotocol An internationally standardized transmission protocol that specifies how routable data packets are transferred over point-to-point links. PPP therefore allows the Internet to be accessed interactively via normal dial-up telephone lines or ISDN lines.

Router	A router is used as an interface between networks. If these networks use different protocols, then a multiprotocol router must be used.
SPID	**S**ervice **P**rofile **Id**entifier For US D channel protocols NI-1, 5ESS: at least one SPID is required per ISDN line. Each SPID is assigned to an ISDN service (e.g. voice, data …)
SPX	**S**equenced **P**acket e**X**change Connection-oriented network protocol in Novell networks
TCP/IP	**T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol Two frequently used protocols for data transmission and Internet connections.
V.110	Bit rate adaptation, defined up to 9600 Baud; available for most terminal adapters up to 38400, and for some also up to 57600 Baud. Each bit on the V24 or X.21bis page is mapped to a bit of the 64 kbit stream of the B channel. In some implementations slower speeds can be multiplexed, i.e. there are several valid mappings.
V.120	Similar to V.110, but additional removal of start and stop bits in the B channel data stream. The theoretically possible data speed (without compression) is therefore 76800 Baud.

WWW

World **W**ide **W**eb

An Internet service which uses graphically designed pages and *hyperlinks* (clicking on a hyperlink takes the user to other pages containing additional information).

Index

Bold page numbers contain detailed information.

C

D

E

F

G

H

I

N

O

P

R

S