BRICKware for Windows

for all BinTec Products

Version 3.5

Document #71030A

August 2000

Purpose This manual provides a description of the BRICKware for Windows utility programs for the BinTec product range. The information included in this manual is compatible with software version 5.2.1.

Liability While every effort has been made to ensure the accuracy of all information in this manual, BinTec Communications AG assumes no liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document. BinTec Communications AG is only liable within the scope of its terms of sales and delivery.

The information in this manual is subject to change without notice. Additional information, including changes and Release Notes, can be retrieved from www.bintec.de.

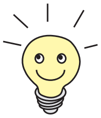
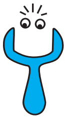
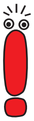
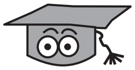
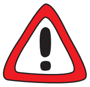
As an ISDN multiprotocol router, a BinTec router establishes ISDN connections in accordance with the system´s configuration. To prevent unintentional charges accumulating, a BinTec router should be carefully monitored. BinTec Communications AG accepts no liability for incidental or consequential loss of data, unintentional connection costs and damages resulting from the unsupervised operation of the product.

Trademark BinTec and the BinTec logo are registered trademarks of BinTec Communications AG.

All other product names and trademarks are the property of their respective companies.

Icons used in this guide

To help you locate and interpret information easily, all BinTec manuals use the following visual aids:

Symbol	Meaning
	Points out useful and relevant tips and tricks
	Predicts potential pitfalls and explains how to avoid them
	Brings to your attention general and important points
	Explains required fundamental information
	Brings your attention to important safety precautions. Levels of danger are in accordance with ANSI: ■ Caution (indicates possible danger that, if unheeded, could cause material damage) ■ Warning (indicates possible danger that, if unheeded, could cause bodily harm) ■ Danger (indicates danger that, if unheeded, could lead to serious bodily harm or death)

Typographical conventions

In order to help you find and interpret the information in all BinTec manuals, the following typographical elements are used:

Typography	Meaning
➤	Here you are requested to do something
■ –	Lists including two levels
MENU ➧ ***SUBMENU***	Indicates menus and submenus in Setup Tool.

`Non-proportional (Courier), e. g.`
`ping 192.168.1.254`
	■ Indicates commands (e. g. in the SNMP shell) that you must enter as shown
	■ Used for drawings of the Setup Tool

`<IP address>`	Indicates commands (e. g. in the SNMP shell). Enter the value of the term in brackets. Do not enter the corner brackets.
bold, italics, e. g. ***BigBoss***	Indicates example terms
bold, e. g. ➤➤ **MIB**	Indicates terms that you can find in the glossary. (For online texts, click the double arrow)
bold, e. g. **biboAdmLoginTable,** **Windows Start menu**	■ Indicates fields in Setup Tool and MIB tables/variables ■ Indicates keys/key combinations and Windows terms
italics, e. g. *none*	Indicates values that can be entered or set in Setup Tool or MIB variables
Online: underlined	Indicates links

Version 3.5
Document #71030A
August 2000

1 Overview

BRICKware for Windows is a software package containing programs to help you install, configure and maintain your BinTec products.

BRICKware for Windows consists of two main parts.

- Firstly, the Desktop Internetworking Management Environment, DIME for short, is a suite of utilities for administrating and tracing BinTec routers from your PC.
- And secondly, Remote Access Drivers – Remote CAPI and Remote TAPI – which provide your PC with standardized software interfaces, such as CAPI 1.1 and CAPI 2.0 for communications applications, or TAPI 1.4 and TAPI 2.0 for telephony applications. In addition to this, there is the TAF (Token Authentication Firewall) Login program that can be used to authenticate users in connection with the tried and trusted Token-Card–ACE/Server solution provided by Security Dynamics.

Configuration Wizard

The Configuration Wizard can be used for a basic initial configuration of your router. For a step-by-step description of how to install your product and configure it with the Configuration Wizard, see the Quick Install Guide. The Guide is enclosed with your product or can be retrieved from BinTec's file server at http://www.bintec.de in PDF format.

TCP/IP stack

BRICKware for Windows has been successfully tested with the TCP/IP stack software Microsoft TCP and OnNet PC/TCP. BRICKware for Windows is also compatible with other TCP/IP stacks, such as Sun PC/NFS and Chameleon TCP.

RVS-COM Lite

Also included is the general-purpose communications software package RVS-COM Lite for Windows 95/98 and Windows NT 4.0. RVS-COM Lite utilizes your BinTec router via the CAPI interface, and allows you to access T-Online (formerly known as Datex-J or BTX), send and receive fax messages, voice mail, etc. For information on installing and using RVS-COM Lite, please refer to its online manuals on the BinTec ISDN Companion CD.

1.1 DIME

DIME comprises the following programs:

- DIME Tools – a suite of utilities for administrating and monitoring BinTec routers from your PC. You need Windows 3.1, Windows 95/98 or Windows NT 4.0 to run DIME Tools.
  - BootP Server – enables your PC to act as a Bootstrap Protocol server (BootP server for short) for one or more BinTec routers. Basic configuration information (i.e. IP address, network mask, name server, etc.) can be initially and remotely loaded over the LAN.
  - ISDN and CAPI Trace Utility – allows you to run an ISDN or CAPI tracer to a BinTec router to examine and analyze the byte streams being sent over the B or D-channel.
  - TFTP Server – manages the transfer of configuration files between the BinTec router and your PC via TFTP. You can, for example, use the TFTP Server to store different versions of your BinTec router's configuration, or to update its system software as described in the **User's Guide**.
  - Syslog Daemon – actively displays system messages received from the BinTec router and stores them in various files for future reference.
  - Time Server – enables your PC to supply your BinTec router with the current time.
- Configuration Manager – this SNMP Manager provides easy access to all the BinTec router's SNMP tables and variables via a graphical user interface.
  You can use Configuration Manager for all configuration and administration purposes, provided you know which values need to be changed to achieve your goal. If you are new to the administration of BinTec routers, the menu-driven Setup Tool (explained in your **User's Guide**) might be the better choice of tools. For an initial configuration of your product, we recommend using the BinTec Configuration Wizard.

1.2 Remote CAPI Client and Remote TAPI Client

- Remote CAPI Client – provides the CAPI 1.1 and CAPI 2.0 interfaces for all Windows systems. With the Remote CAPI Client installed, you can use the ISDN interface of your BinTec router from all PCs in your LAN as if it was locally installed in the PC.
  From the range of communications programs available for Windows which use the CAPI interface, RVS-COM Lite for Windows 95/98 and Windows NT 4.0, a general-purpose communication package, is included on your BinTec ISDN Companion CD.
- Remote TAPI Client – provides TAPI telephony services on your PC. You can use a number of Windows applications—e.g. the MS Dialer, or MS Outlook—to initiate calls which use the analog devices connected to the POTS ports of your BinTec router from your PC, or to display information about the caller from a database to help you decide whether to take the call.
- Remote Multi CAPI Client (RMCC) – provides a CAPI 2.0 interface for multiple BinTec routers for Windows NT 4.0 systems. With RMCC installed, you can use the ISDN interfaces of all BinTec routers available on your network for CAPI connections from one PC.
- Remote Clients Configuration – is a setup utility for Remote CAPI and Remote TAPI.

1.3 Configuration Wizard

Basic configuration

With the Configuration Wizard included in the BRICKware for Windows, you can start running your BinTec product easily and quickly. You can perform a basic initial configuration via the serial connection from your Windows PC. The Configuration Wizard is one of several possibilities to configure your router. Other methods to configure your router and fine-tune your configuration are described in your **User's Guide**.

Quick Install Guide

For a step-by-step description of how to install your BinTec product and configuring it with the Configuration Wizard, see the **Quick Install Guide**, which is enclosed with your product or can be retrieved from BinTec's file server at http://www.bintec.de in PDF format.

1.4 Device at COM1 and Device at COM2

Terminal program

Device at COM1 and Device at COM2 are preconfigured links to Windows' terminal program for accessing a BinTec router connected to COM1 or COM2 with a serial interface cable. You can then easily login to your BinTec router and configure it, e.g. by using the built-in Setup Tool (see **User's Guide**).

1.5 Token Authentication Firewall (TAF) Login Program

Access security

Token Authentication Firewall, TAF, is an advanced means of controlling access to central site computing resources. It goes beyond the theoretical limitations of existing security mechanisms like Access Lists and Network Address Translation.

These features control access to routing services based on the contents of incoming/outgoing IP packets (IP address, TCP port number, interface, etc.). In contrast, TAF is user oriented; meaning that IP connections are managed based upon authentication of the actual user at the remote host. This solves such security problems involving:

- unauthorized access to company resources by family members using teleworkers' home equipment
- stolen equipment (laptops) and the loss of sensitive configuration information (login IDs and password)

Token Card

TAF Login user verification is based on the tried and trusted Token-Card–ACE/Server solution provided by Security Dynamics.

You will need a special TAF license to use TAF on your BinTec router. Along with this license, you will get 10 TAF Login licenses for PCs you wish to use as TAF clients.

A security solution using TAF is made up of four components:

- a Remote Access Server by BinTec
- an ACE Server by Security Dynamics
- a Token Card by Security Dynamics
- a Windows application for the client PC by BinTec

1.6 Windows Activity Monitor

The included Windows program Activity Monitor allows you to monitor as well as manipulate the states of interfaces of a BinTec router via windows and icons on the desktop of your PC. You can open a window and an icon for every interface and so the state of a BinTec router is visible at a glance.

Information monitored covers among other things

- the transmission rate performed on a channel
- the state of a channel
- the number of open channels
- the state of the BinTec router's WAN partners

From BRICKware version 5.2.1, an online Help is available with the Activity Monitor program. There you will find the complete documentation for this application.

2 Installation

This chapter includes the required steps for installing and deinstalling BRICKware for Windows.

You will learn:

- How to install the TCP/IP Protocol
- How to install BRICKware for Windows
- How to uninstall BRICKware

2.1 Checking and Installing the TCP/IP Protocol

The TCP/IP protocol is the “language” PCs use to communicate over the network and to connect to the Internet. All components of BRICKware for Windows need TCP/IP. Make sure that the TCP/IP protocol is installed before you start installing BRICKware.

To check the installation of the TCP/IP protocol, proceed as follows:

- In the **Start** menu click **Settings**, in the submenu click **Control Panel**. Double-click **Network**.
- Windows 95/98: search the networks components list for **TCP/IP**.
- Windows NT: click the tab **Protocols**. Search the network protocol list for the **TCP/IP Protocol**.
- If you can’t find this entry, install the TCP/IP protocol as described below. Otherwise, close the dialog box and start the installation of BRICKware as described in figure 2.2, page 17.

To install the TCP/IP protocol:

- Windows 95/98: in the dialog box **Network** click **Add**. In the network components list, select **protocol** and click **Add**. In the manufacturers column, click **Microsoft** and then click **Microsoft TCP/IP**. Click **OK**. In an existing network, you might have to configure additional settings. Ask your system administrator.
- Windows NT: in the **Network** dialog box, click the tab **Protocols** and click **Add**. In the network components list, click **TCP/IP Protocol** and click **OK**: confirm the questions with **Yes** to set up a new network. In an existing network, ask your system administrator.
- Follow the instruction on the screen and finally restart your PC.

2.2 Installing BRICKware

From release 5.2.1, Windows 3.x. and Windows NT 3.x. are no longer supported. All programs belonging to the BRICKware suite are 32-bit applications.

It is reasonable to install Configuration Manager, Configuration Wizard and DIME Tools on the administrator's computer only.

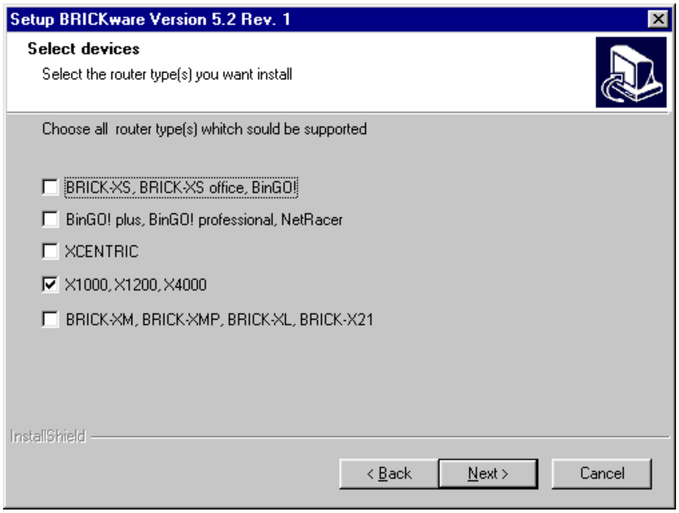
The Remote CAPI and Remote TAPI Clients, on the other hand, must be installed on each computer on which you wish to use the BinTec router's Remote CAPI or Remote TAPI feature. You can only make use of the TAPI if your BinTec router has a POTS module (CM-AB) built in.

On the BinTec Companion CD in the folder BRICKware, you can also find the Administrator and Client Edition of the BRICKware separate in the subfolders Admin and Clients. This is also useful for a system administrator, for example, who wants to prepare floppy disks for the installation of the Client Edition.

Installation procedure

Installing BRICKware:

- Quit all Windows-based programs on your PC. Note that also CAPI applications which are only signalled by an icon in the status area of the taskbar should be closed.
- Put the BinTec Companion CD into the CD-ROM drive of your PC. After a few seconds the start window appears. If the start window does not appear automatically, click the CD-ROM drive in your Windows Explorer and double-click setup.exe.
- Select the language version.
- Click BRICKware to start the setup program.
- Specify the directory BRICKware shall be installed to. We recommend accepting the default path settings.
- Select one or more types of BinTec routers:



Setup BRICKware Version 5.2 Rev. 1

Select devices

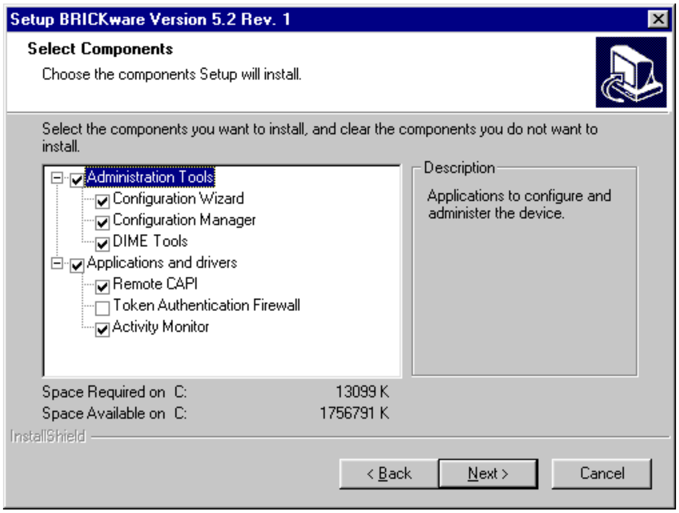
Select the router type(s) you want install

Choose all router type(s) whitch sould be supported

- □ BRICK-XS, BRICK-XS office, BinGO!
- □ BinGO! plus, BinGO! professional, NetRacer
- □ XCENTRIC
- ☑ X1000, X1200, X4000
- □ BRICK-XM, BRICK-XMP, BRICK-XL, BRICK-X21

Figure 2-1:   Custom Installation - BinTec devices

➤ Select the software components you want to be installed (see chapter 1, page 7 for explanation of the components):



Setup BRICKware Version 5.2 Rev. 1

Select Components

Choose the components Setup will install.

Select the components you want to install, and clear the components you do not want to install.

- ☑ Administration Tools
  - ☑ Configuration Wizard
  - ☑ Configuration Manager
  - ☑ DIME Tools
- ☑ Applications and drivers
  - ☑ Remote CAPI
  - □ Token Authentication Firewall
  - ☑ Activity Monitor

Description

Applications to configure and administer the device.

Space Required on C: 13099 K

Space Available on C: 1756791 K

Figure 2-2:   Custom Installation - Options

➤ Confirm the settings you have selected in the following dialog box and the installation begins.

Autostart

If the Activity Monitor and TAF were selected, they are automatically included in the Autostart group. If you want to add Dime Tools to the Autostart group, this must be done by hand. This is especially useful when you want to use BootP Server (see chapter 3.3, page 31), TFTP Server (see chapter 3.5, page 42), Syslog Daemon (see chapter 3.6, page 44) or Time Server (see chapter 3.7, page 48). For the basic functions of your router, it is not necessary to start DIME Tools automatically together with Windows.

At the end of the installation, you can continue with the configuration of your device.

BRICK.INI and Registry

BRICKware adds a new file BRICK.INI to your Windows directory. This file contains the required configuration information for the programs to work properly. If this file is removed, the configuration will be lost. In general, BRICKware also makes entries to the Windows Registry.

Initial configuration

For BinTec´s Personal Access products, we recommend using the BinTec Configuration Wizard for an initial configuration.

An alternative for more advanced users is configuration via the serial interface of your PC using the Setup Tool (see chapter 7, page 81).

To use Setup Tool via telnet (see **User’s Guide**) or the Configuration Manager (see chapter 4, page 51) for a configuration of your BinTec router, first a name, IP address and netmask must be assigned to the BinTec router with the help of the BootP Server.

As soon as the BootP Server receives a BootP request from your new BinTec router, it opens the BootP Server Configuration window (see chapter 3.3, page 31). Here you can enter the name, IP address and netmask for your BinTec router.

Another way to carry out remote configuration is to use the isdnlogin command from a remote BinTec router on the BinTec router and then to start the Setup Tool from the prompt (see your product’s **User’s Guide**).

BRICKware Program Group

After the installation is complete, you will find the utility programs in the BRICKware start menu group:

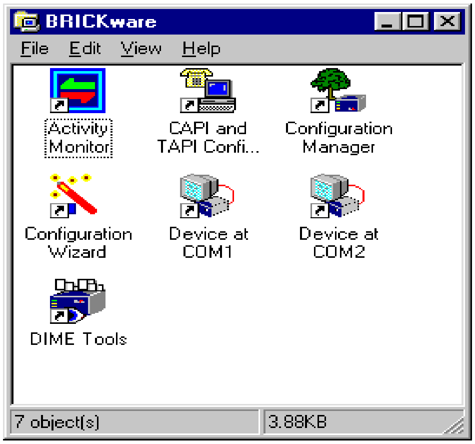
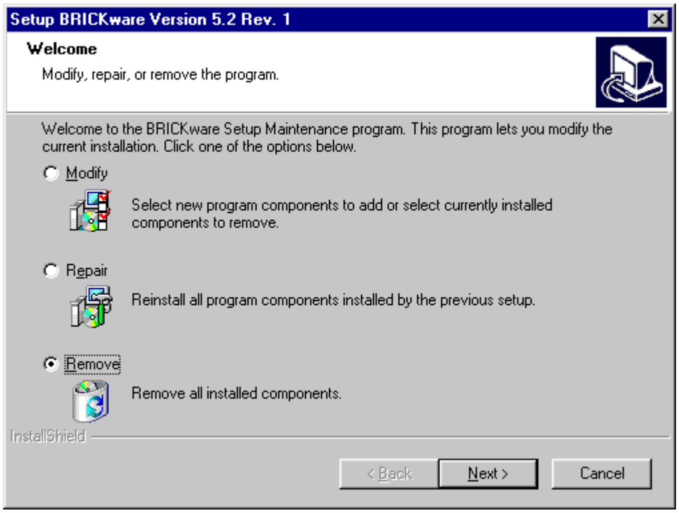


Figure 2-3: BRICKware Start Menu Group

2.3 Uninstalling / Maintaining BRICKware

To uninstall BRICKware, choose **Software** from the Windows **Control Panel** and there select **BRICKware** and uninstall it.

Alternatively, you can insert the BinTec Companion CD and select the **Remove** option button on the page which opens when existing BRICKware is detected on the system. Further options over this setup page include repairing as well as modifying existing installations.



Setup BRICKware Version 5.2 Rev. 1

Welcome

Modify, repair, or remove the program.

Welcome to the BRICKware Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

○ Modify

Select new program components to add or select currently installed components to remove.

○ Repair

Reinstall all program components installed by the previous setup.

● Remove

Remove all installed components.

Table 2-1: Uninstalling BRICKware

Your BRICK.INI configuration file in the Windows folder and registry entries will be kept, however, so you do not lose your configuration when uninstalling BRICKware. This is especially useful for software updates.

We recommend that you uninstall BRICKware prior to installing a BRICKware software update.

3 DIME Tools

DIME Tools consists of the following administration tools:

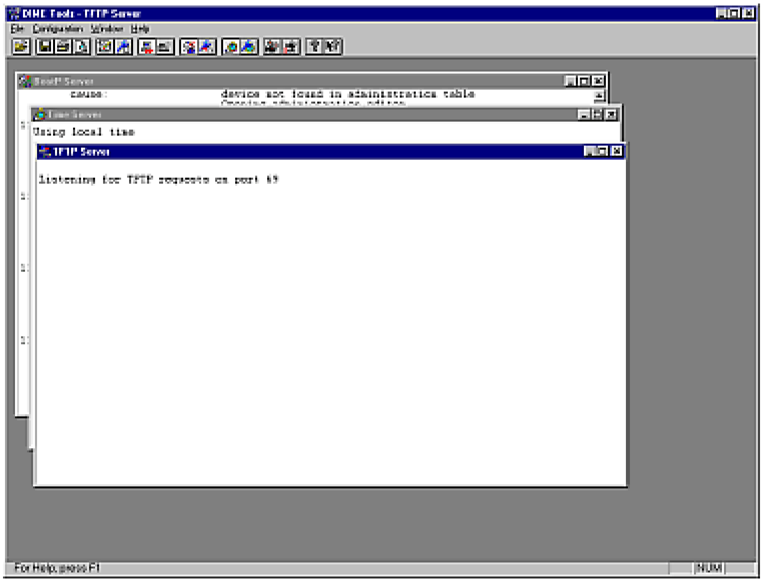
- BootP Server
- DIME Tracer
- TFTP Server
- Sysog Daemon
- Time Server

3.1 Starting up the Toolkit

After starting up DIME Tools for the first time, the TFTP Server window, Syslog Daemon, BootP Server and Time Server window will open automatically.

If these windows get closed at any time they can be reopened from the **File** menu or by clicking on the appropriate icon on the toolbar.

The DIME Tracer functions are available by selecting **File** ➧ **New ISDN Trace** or **File** ➧ **New CAPI Trace** from the main menu or from the toolbar.



```
cause:                    device not found in administration table
Using local time
listening for TFTP requests on port 69
```

Figure 3-1: DIME Tools - Main window

We will now give you a short explanation of all the icons in the toolbar, followed by a rundown of all available menu items.

The different parts of DIME Tools are then described in detail separately.

Note that activated DNS Name Resolution for Syslog Daemon can lead to unwanted ISDN connections if WAN connections have to be established for DNS requests. So check the entry in **Configuration** ➧ **Options...**.

As DIME Tools is a 32-bit application, it is possible to use long path settings and file names in all of the Dime Tools.

3.2 Menu Structure

DIME Tools has the following menu structure:

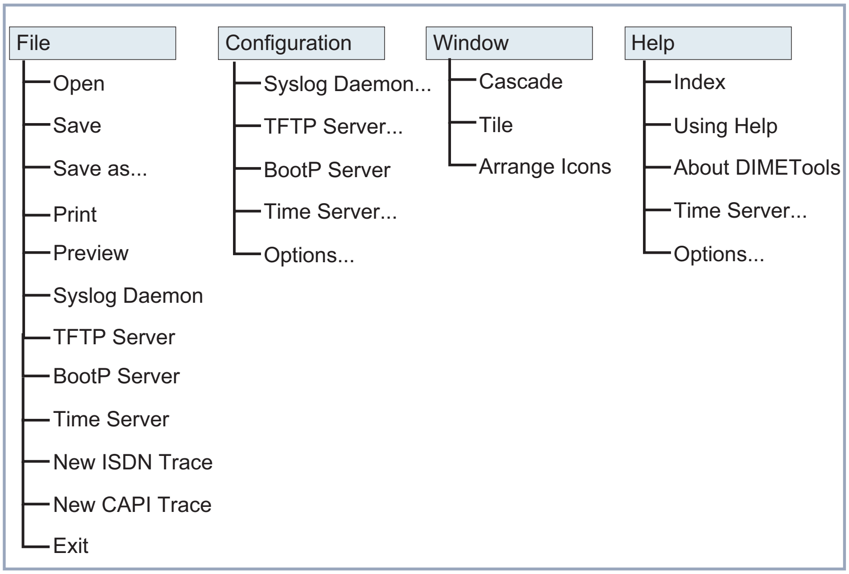


Figure 3-2: DIME Tools – Menu Structure

The important menu items can also be accessed by clicking on the appropriate icon on the toolbar:

Icon	Menu	Command
📂	File	Open - Open a file for viewing
💾	File	Save - Save text contents of active window to file
🖨	File	Print - Print contents of active window
🔍	File	Preview - Preview contents of active window
	File	Syslog Daemon - Open the Syslog Daemon window
	Configuration	Syslog Daemon - Configure Syslog Daemon
	File	TFTP Server - Open the TFTP Server window
	Configuration	TFTP Server - Configure TFTP Server
	File	BootP Server - Open the BootP Server window
	Configuration	BootP Server - Configure BootP Server
	File	Time Server - Open the Time Server window
	Configuration	Time Server - Configure Time Server
	File	New ISDN Trace - Open a new DIME Tracer window

Icon	Menu	Command
CAPI	File	New CAPI Trace - Open a new DIME Tracer window
?	Help	About DIME Tools - Display a short copyright message
↖?		Activate context-sensitive help

Table 3-1: DIME Tools – Icons on the Toolbar

The following is a short run through all menu items:

Menu	Command	Meaning
File	**Open**	Opens a configuration, syslog or trace file of a BinTec router for viewing or editing. This function can also be activated by clicking the 📂 icon.
File	**Save**	Creates a file with the text contents of the active window, including all text that is currently not visible on screen, but can be reached using the scrollbars. This function can also be activated by clicking the 💾 icon.
File	**Save as**	Save text contents of current window in the specified file.
File	**Print**	Prints the text contents of the active window. This function can also be activated by clicking the 🖨 icon.
File	**Preview**	Displays a print-preview of the text contents of the active window. This function can also be activated by clicking the 🔍 icon.
File	**Syslog Daemon**	Opens the Syslog Daemon window (if not already open). This function can also be activated by clicking the 📝 icon.

Menu	Command	Meaning
File	**TFTP Server**	Opens the TFTP Server window (if not already open). This function can also be activated by clicking the icon.
File	**BootP Server**	Opens the BootP Server window (if not already open). This function can also be activated by clicking the icon.
File	**Time Server**	Opens the Time Server window (if not already open). This function can also be activated by clicking the icon.
File	**New ISDN Trace**	Opens a new DIME ISDN Tracer window. You can specify the kind of data to be traced in a dialog box (see chapter 3.4.1, page 36). This function can also be activated by clicking the icon.
File	**New CAPI Trace**	Opens a new DIME CAPI Tracer window. You can specify the kind of data to be traced in a dialog box (see chapter 3.4.2, page 40). This function can also be activated by clicking the CAPI icon.
File	**Exit**	Leave DIME Tools.
Configuration	**Syslog Daemon**	Here you can specify which syslog messages are saved to which file. This function can also be activated by clicking the icon.
Configuration	**TFTP Server**	Allows you to specify the TFTP path where all incoming and outgoing files are retrieved or stored respectively. This function can also be activated by clicking the icon.
Configuration	**BootP Server**	Calls the Administry Editor which lets you specify the devices to be configured by BootP Server. This function can also be activated by clicking the icon.

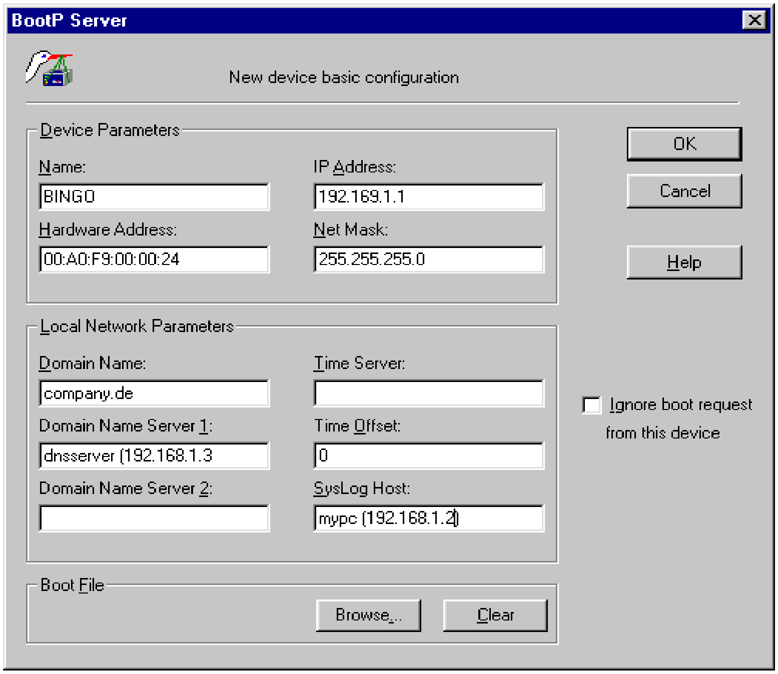
Menu	Command	Meaning
Configuration	**Time Server**	Opens a dialog box where you can select whether the PC’s local time or GMT shall be sent to the BinTec router. This function can also be activated by clicking the icon.
Configuration	**Options...**	Opens a dialog box from which you can change the IP broadcast behaviour of the BinTec router, the colours used for the output in all DIME Tools windows and activate or deactivate DNS Name Resolution for the Syslog Daemon. You can also restore the default colour settings. Note: Activated DNS Name Resolution for Syslog Daemon can lead to unwanted ISDN connections if WAN connections have to be established for DNS requests. So check the entry in **Configuration** ➧ **Options...**.
Window	**Cascade**	Cascade all open DIME Tools windows.
Window	**Tile**	Tile all open DIME Tools windows horizontally.
Window	**Arrange Icons**	Arranges all iconified DIME Tools windows at the bottom of the main window.
Help	**Index**	Lets you choose from an index of the available help topics.
Help	**Using Help**	Provides help on how to use the help function.
Help	**About DIME Tools**	Displays an information box and copyright notice for DIME Tools. This function can also be activated by clicking the ? icon.

Table 3-2: Menu items

In addition to the three help menu items, you can get help in context by clicking the ↖? icon. This lets you select the item you need help on with a mouse-click.

3.3 BootP Server

BootP Server is short for Bootstrap Protocol server for Windows. Using BootP Server, you can assign your BinTec router an IP address, network mask, and configuration file (optional) at boot time.



New device basic configuration

Device Parameters

Name: BINGO

IP Address: 192.169.1.1

Hardware Address: 00:A0:F9:00:00:24

Net Mask: 255.255.255.0

Local Network Parameters

Domain Name: company.de

Time Server:

Domain Name Server 1: dnsserver (192.168.1.3

Time Offset: 0

Domain Name Server 2:

SysLog Host: mypc (192.168.1.2)

Boot File

□ Ignore boot request from this device

Figure 3-3: BootP Server - Initial BinTec router Configuration

If you power up your BinTec router after having connected it to your network, but before supplying it with an IP address and network mask, it will start broadcasting BootP request messages over the ethernet.

When a BootP request from a new BinTec router is received by a PC running DIME Tools, the BootP Server Window opens a dialog box as shown in figure 3-3, page 31 above.

Here you can enter the most important network parameters.

BootP configuration

BinTec router parameters: The following parameters – which will be sent to the requesting BinTec router – are mandatory:

BinTec router Parameters	Meaning
Name	The host name for the BinTec router, as it should be used by a DNS server, for example.
IP Address	The IP address of the ethernet interface on the BinTec router.
Net Mask	The network mask to use. Note that this field is automatically filled when a new address is entered in the IP address field. If you are using subnets, you should change this field appropriately.
Ethernet Address	The hardware address for the BinTec router's ethernet interface (the hardware address is located on either the ethernet module or the underside of your BinTec router). This address is included in the BootP requests from a BinTec router. The field is automatically set to the address received.

Table 3-3: BinTec router parameters

Local Network Parameters: the following parameters are optional, are not required by the Bootstrap Protocol and can be changed later using the Setup Tool, for example:

Local Network Parameters	Meaning
Domain Name	Symbolic name of the LAN, e.g. the same as configured on your PC or the domain name provided by your Internet Service Provider.
Domain Name Server 1 and 2	IP addresses of the primary and secondary Name Servers on the LAN, which serve to resolve host names.
Time Server	IP address of the Time Server. You can enter the IP address of your PC here if you want to use it as a time server, or leave it empty if you want to collect time information from the ISDN, for example.
Time Offset	The time difference in hours between Universal Time Code UTC (previously known as GMT or Greenwich Mean Time) and local time. If you leave this item empty or enter 0, the local time is used.
Syslog Host	Host to send syslog messages to. You should enter the IP address of your PC here if you want to use the DIME Syslog Daemon for collecting syslog messages and you do not want to use another syslog host.
Boot File	Specifies a configuration file from the TFTP directory to send to the BinTec router. Please be aware that if a configuration file is specified, the settings stored in that file may overwrite the settings included in the previous fields. This item shall stay empty if you want to load the configuration from your BinTec router´s flash.

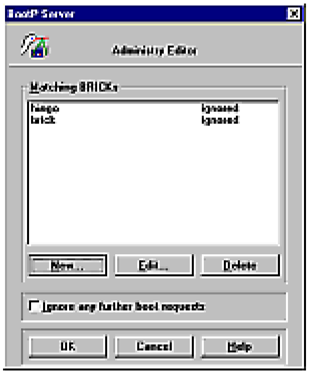
Local Network Parameters	Meaning
Ignore boot request of this BinTec router	If this box is checked, all subsequent BootP requests received from this hardware address will be ignored. This is useful if you want this device to be managed by another BootP server.

Table 3-4: Local Network Parameters

Administry Editor With the Administry Editor (available from **Configuration** ➧ **BootP Server**), you can specify any number of BinTec routers (devices) to manage BootP. The New, Edit, and Delete buttons, shown in figure 3-4, page 34 below, allow you to define which BinTec routers to manage from this PC.

Here you can also enter BinTec routers which are not directly connected to your LAN, but can be reached via TCP/IP.

The **Ignore any further boot requests** checkbox can be used to ignore all BootP requests originating from devices not specified in the list.



hugo ignored
brick ignored

□ Ignore any further boot requests

Figure 3-4: BootP Server - Administry Editor

Security considerations Since the BinTec router automatically sends BootP requests over the LAN (if no IP address or configuration file is present), each BootP Server set up on the LAN is capable of configuring the BinTec router. To prevent the BinTec router from submitting BootP requests, ensure the router can load its configuration information from its local memory (i.e. store the configuration using **SNMP ➧ Save Configuration** from Configuration Manager or `cmd=save` directly on the router in the SNMP shell or save the configuration using the Setup Tool). Refer to the section on Configuration Files in the **Software Reference**.

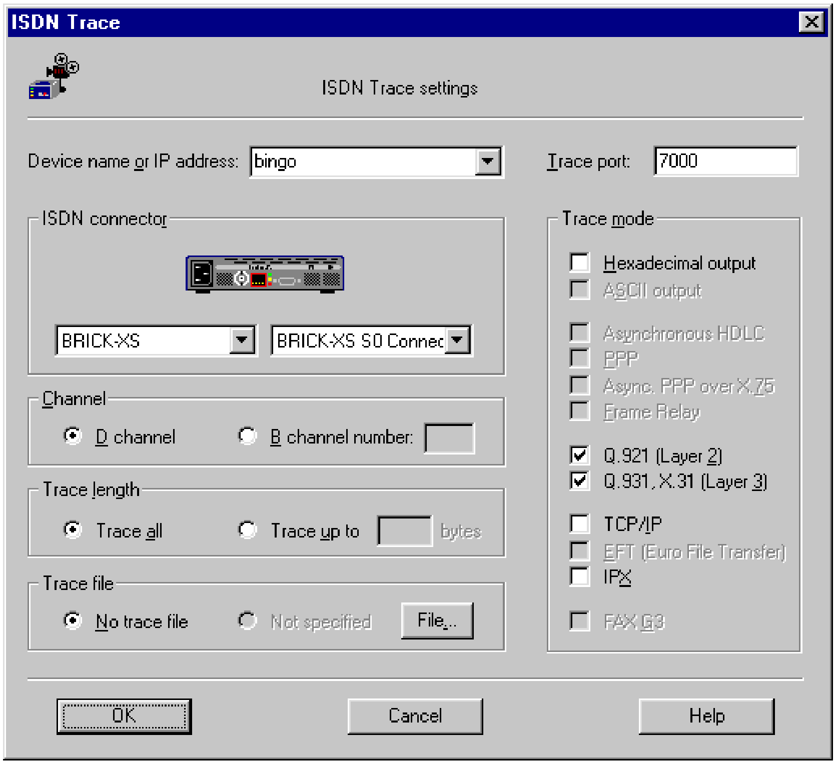
3.4 DIME Tracer

Besides the SNMP and Unix commands, which are available to start traces on the BinTec router (see your product's User's Guide), DIME Tools offer the utilities ISDN Trace and CAPI Trace.

3.4.1 ISDN Trace

You can start an ISDN tracer on a BinTec router to collect and examine the actual contents being sent over an ISDN channel (B or D). This is done by selecting, **File** ➧ **New ISDN Trace** from the main menu bar. You can have multiple trace windows open simultaneously (e. g. one trace window for the D-channel and one for each B-channel). The ISDN tracer runs (and collects trace data) as long as the trace window is open.

Setting the parameters for the trace is done by selecting the options from the ISDN Trace settings window (see figure 3-5, page 37 below):



ISDN Trace

ISDN Trace settings

Device name or IP address: bingo

Trace port: 7000

ISDN connector

BRICK-XS

BRICK-XS S0 Connec

Channel

● D channel ○ B channel number:

Trace length

● Trace all ○ Trace up to bytes

Trace file

● No trace file ○ Not specified

Trace mode

□ Hexadecimal output

□ ASCII output

□ Asynchronous HDLC

□ PPP

□ Async. PPP over X.75

□ Frame Relay

☑ Q.921 (Layer 2)

☑ Q.931, X.31 (Layer 3)

□ TCP/IP

□ EFT (Euro File Transfer)

□ IPX

□ FAX G3

Figure 3-5: DIME ISDN Trace Settings

Parameters for ISDN Trace	Meaning
Device name or IP address	Enter the name (e.g. bingo) or IP address (e.g. 192.168.1.1) of your BinTec router.
Trace port	Specifies the TCP port to use for the trace connection to the device (default value: 7000). Make sure to use the same port as on your router (Setup Tool: ***IP*** ➧ ***STATIC SETTINGS*** menu; SNMP shell: **adminTable**)
ISDN Connector	Choose which ISDN port should be traced. You can select the BinTec router type you are using from the left listbox below the graphic. By selecting **other BinTec device**, the slot and unit numbers can be entered without having to specify the router type. Use the right listbox to select the slot and connector for the ISDN interface you wish to trace.
Channel	Choose which channel should be traced (D or B1 to B31).
Trace length	Restrict trace output to the first n bytes (usually only the first few bytes of each data packet are of interest).
Trace file	Clicking **File** lets you specify a file name to store the trace results in. Such a file can be useful for troubleshooting and for longer traces, since the trace window can only hold a limited amount of data.

Parameters for ISDN Trace	Meaning
Trace mode	The check buttons in this section determine how the trace data is displayed as well as how it is interpreted: ■ **Hexadecimal output** All data is also displayed hexadecimally. ■ **ASCII output** All data is only displayed as ASCII characters. ■ **Layer 2, Layer 3** Layer 2 (Q921) and Layer 3 (Q931) trace data is displayed. The remaining modes are particularly useful if you are using a special protocol (e.g. PPP, Eurofile transfer, Fax, etc.).

Table 3-5: Parameters for ISDN Trace

The remaining modes are particularly useful if you are using a special protocol (e.g. PPP, Eurofile transfer, Fax, etc.).

The options chosen here should be appropriate for the activity you are tracing (e.g. setting PPP mode and tracing an ISDN channel where FAX data is being sent will produce improper results).

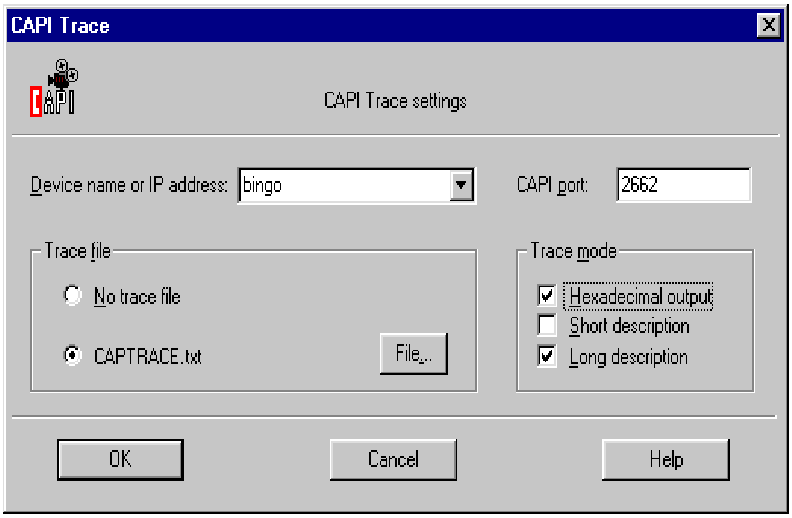
The trace will be started by clicking **OK**.

Note that if a lot of data is traced, older data is scrolled off the screen; however, all data will be saved in the trace file you specified.

3.4.2 CAPI Trace

The CAPI Trace utility allows you to examine the CAPI messages sent to and from your BinTec router. This is done by selecting, **File ➧ New CAPI Trace** from the main menu bar. You can have multiple trace windows open simultaneously (for tracing more than one device at a time). The CAPI tracer runs (and collects trace data) as long as the trace window is open.

Setting the parameters for the trace is done by selecting the options from the CAPI Trace settings window (see figure 3-6, page 40 below):



Device name or IP address: bingo

CAPI port: 2662

Trace file

○ No trace file

● CAPTRACE.txt

Trace mode

☑ Hexadecimal output

□ Short description

☑ Long description

Figure 3-6: CAPI Trace Settings

Parameters for CAPI Trace	Meaning
Device name or IP address	Enter the name (e.g. bingo) or IP address (e.g. 192.168.1.1) of your BinTec router.
CAPI port	Specifies the TCP port to use for the CAPI trace connection (default value: 2662). Make sure to use the same port as on your BinTec router (Setup Tool: ***IP*** ➧ ***STATIC SETTINGS***; SNMP shell: **adminTable**).
Trace file	Clicking **File** lets you specify the name of a file to store the trace results in. This can be useful for longer traces - the trace window can only hold a limited amount of data - and for troubleshooting.
Trace mode	The check buttons in this section determine how the trace data is displayed as well as how it is interpreted. ■ **Hexadecimal output** All data is also displayed hexadecimally. ■ **Short description** Gives just the names and the most essential data for each CAPI message. ■ **Long description** Gives a detailed listing and explanation of all the information in each CAPI message.

Table 3-6: Parameters for CAPI Trace

3.5 TFTP Server

TFTP Server manages the transfer of configuration files between the BinTec router and your PC via TFTP. It can be used to update your BinTec router's system software via the LAN.

Once TFTP Server is configured, the device can send and receive TFTP files to/from the PC. TFTP requests initiated on the device can then be serviced by TFTP Server.

Configuration files

There are several different ways to generate TFTP requests for the transfer of configuration files between your BinTec router and your PC.

The easiest way is to use the ***CONFIGURATION MANAGEMENT*** menu of the Setup Tool on your device. (You can access the BinTec router via Telnet over the LAN or via a Hyperterminal, when the device is attached to the serial interface of your PC.) There you have all the options available for transferring configuration files between your BinTec router's Flash ROM and memory and a TFTP server. Other ways include issuing the appropriate command by hand from the BinTec router's SNMP command shell, e.g.

```
cmd=put host=192.168.1.2 path=”file.cf”
```

For further information, please refer to the **User's Guide**.

System Software Updates

There are different ways to update your BinTec router's system software. The easiest way is to issue the update command from the SNMP command shell:

```
update <TFTP server> <image file name>
```

Once the image has been successfully transferred to the BinTec router, you will be asked whether you want to perform the update (i.e. actually write the image to Flash ROM) and then whether you want to reboot the BinTec router to use the new system software.

You can also update the system software from the BOOTmonitor, as described in your **User's Guide**.

Note that all of the above will only work if the TFTP Server is running on your PC and the TFTP Path is set (see following sections).

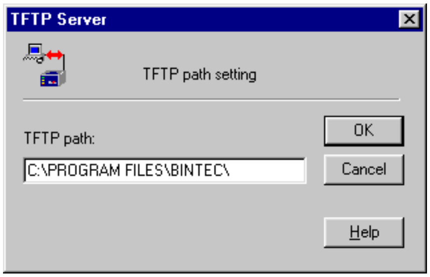
File names have to correspond to the MS DOS 8.3 file name notation.

For firmware logic or BOOTmonitor updates, please refer to the Release Note Logic, which is available via BinTec's FTP Server at http://www.bintec.de.

As long as the TFTP Server window is open, all transfer requests received from the BinTec router are serviced by the TFTP daemon. The TFTP Server window shows each request it receives, along with its appropriate result status (success or error).

Setting the TFTP Path

Choosing **Configuration** ➧ **TFTP Server** allows you to specify/change the TFTP path where all incoming/outgoing files are retrieved/stored (see figure 3-7, page 43 below):



TFTP Server

TFTP path setting

TFTP path: C:\PROGRAM FILES\BINTEC\

Figure 3-7: TFTP Server - TFTP Path Setting

The TFTP path is set to **C:\Program Files\BinTec** by default. References to subdirectories while transferring files are not possible.

3.6 Syslog Daemon

Syslog Daemon allows the reception of system messages (see section Syslog Messages in Appendix E of the **Software Reference**) sent from the BinTec router. The only requirement is that the PC is configured to be the BinTec router's syslog host (either by entering the PC's IP address in the Syslog Host field in the BootP Server dialog – see figure 3-3, page 31 – for this device, or using Configuration Manager to enter it in the **addr** field of the **biboAdmLogHostTable** in the administration group, or by using the menu ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING*** of Setup Tool (see **User's Guide**).

As long as the Syslog Daemon window is open, all messages are displayed on the screen and written to their respective log files. Each syslog message on the BinTec router has a priority level (**biboAdmSyslogTable** – **Level**) and a subject (**biboAdmSyslogTable** – **Subject**) associated with it. By default, all syslog messages (all subjects and all levels) are saved in the brick.log file.

Configuring Syslog Daemon

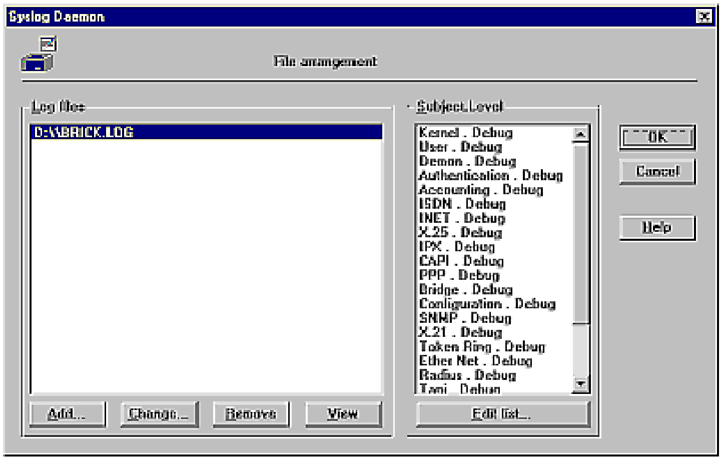
The configuration for Syslog Daemon is found under **Configuration** ➧ **Syslog Daemon** from the main menu bar. Here, you can change the default settings or add files where syslog messages are saved and set the types of messages to save in them.

Note that these settings only affect the way syslog messages are saved in files. Regardless of these settings, all syslog messages are displayed in the open Syslog Daemon window.

Information saved into log files can be sorted by subject and level, but it is not possible to sort by different BinTec routers, when you are receiving syslog messages from more than one BinTec router.

Note that activated DNS Name Resolution for Syslog Daemon can lead to unwanted ISDN connections if WAN connections have to be established for DNS requests. So check the entry in **Configuration** ➧ **Options...**.

The window opens with a list of current log files and their respectively assigned subject level combinations on the right:



D:\\BRICK.LOG

Kernel . Debug
User . Debug
Demon . Debug
Authentication . Debug
Accounting . Debug
ISDN . Debug
INET . Debug
X.25 . Debug
IPX . Debug
CAPI . Debug
PPP . Debug
Bridge . Debug
Configuration . Debug
SNMP . Debug
X.21 . Debug
Token Ring . Debug
Ether Net . Debug
Radius . Debug
Tapi . Debug

Figure 3-8: Syslog Daemon Configuration Dialog Box

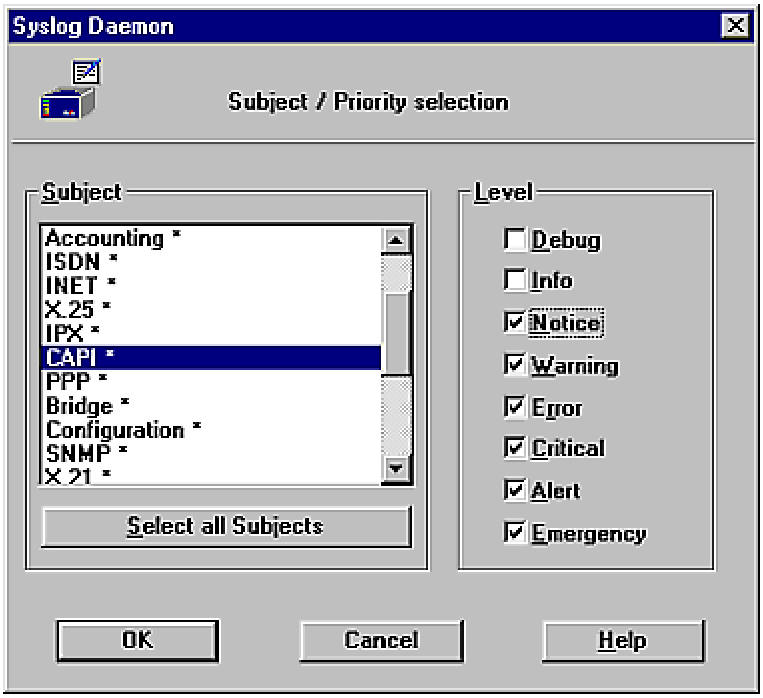
There are five buttons at the bottom of this window:

Button	Meaning
Add	Lets you add a new log file to the list. If this file already exists, it will be overwritten.
Change	Allows you to change the name of the file where these message combinations are stored. If the new filename already exists, then message data will be appended to it.
Remove	Removes a file from the list, but not from the physical disk.
View	Lets you view the contents of a log file on screen.
Edit list	Once a log file is highlighted, you can select this button to change the file's Subject/Level combinations. A new window will be opened as shown in figure 3-9, page 47.

Table 3-7: Buttons in the Syslog Daemon Configuration Dialog Box

Subject/Priority combinations

Here, you can define the Subject/Priority Level combinations for messages to be saved in the log file.



Subject

- Accounting *
- ISDN *
- INET *
- X.25 *
- IPX *
- CAPI *
- PPP *
- Bridge *
- Configuration *
- SNMP *
- X.21 *

Level

- ☐ Debug
- ☐ Info
- ☑ Notice
- ☑ Warning
- ☑ Error
- ☑ Critical
- ☑ Alert
- ☑ Emergency

Figure 3-9: Syslog Daemon – Subject / Priority Selection

Each Subject can have a different range of Priority Levels associated with it. After highlighting a Subject, its levels are displayed to the right. Subjects which have been selected (are to be used for the saving of messages) are displayed with an (*) after its name.

As soon as one or more Subjects are highlighted, you can make Level selections from the check buttons on the right. Selecting a message Level includes all messages on Levels below it, i.e. setting the Critical level would select Critical, Alert, and Emergency levels. To deselect the highlighted Levels, you have to click the **Emergency** button twice. Selecting the **OK** button accepts the list and the logging of messages can begin.

3.7 Time Server

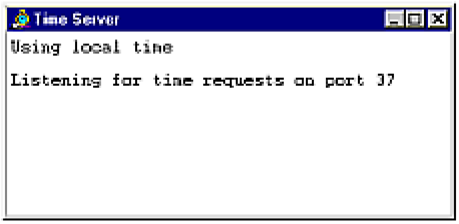
A host can act as time server by answering to clients, which are sending time requests with correct time information.

DIME Tools include a UDP Time Server according to RFC 738. This server can initially set the clock of your BinTec router and synchronize it at regular intervals.

The Time Server replies to all time requests (UDP packets) received on port 37 by sending a UDP packet containing the current time. These time packets contain a 32 bit value representing the number of seconds that have passed since January 1, 1900, 0000 hours.

The **Time Server** command in the **File** menu starts the Time Server and the Time Server is active until you close the Time Server window.

When you are using the Time Server, it is advisable to put the DIME Tools to the Autostart folder so that the Time Server is always available.

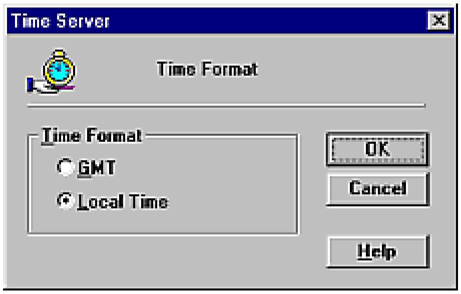


```
Using local time
Listening for time requests on port 37
```

Figure 3-10: Time Server Window

In the Time Server window all received time requests and the replies to them are displayed.

The Time Server supports the formats Local Time and GMT according to RFC 738. You can configure the Time Server with the command **Configuration ➧ Time Server**:



Time Server

Time Format

Time Format
○ GMT
● Local Time

Figure 3-11: Time Server Configuration

- **GMT**
  Greenwich Mean Time (GMT/UTC) according to RFC 738 (no daylight savings time).
  When you choose GMT, the time offset on the BinTec router should be set to the correct value. In summer, you may have to add 1 hour to this value. Notice that the recalculation of GMT depends on the environment variable TZ set in the autoexec.bat of your PC. The value and the interpretation of this variable is displayed in the Time Server window when you select the option GMT.
  Example for settings of TZ in the autoexec.bat:
  - `set TZ=GST1GDT` or
  - `set TZ=GST+1GDT`

  These strings use GST to indicate German standard time. Where it is assumed that Germany is one hour ahead and that daylight savings time is on (GDT= daylight savings time). If the variable TZ is empty, the default value taken is PST8PDT, which signifies the Pacific time zone.

- **Local Time**
  Local Time is the default value in this dialog box. Here the current value of the PC’s system clock is used. This may include daylight saving time. When

selecting this option, the Time Offset on the BinTec router should be set to 0.

The advantage of selecting Local Time is that the correct local time will be set, although the BinTec router does not support daylight saving time. But you must notice that this setting does not correspond to RFC 738, which may lead to the consequence that other devices using this Time Server may be set to an incorrect current time. The variable TZ is not taken into account with this option.

4 Configuration Manager

The Configuration Manager is an SNMP manager which allows you to access all SNMP tables and variables on your BinTec router from a graphical user interface, thus facilitating the configuration of the device.

By default, Configuration Manager first scans the local network for any connected BinTec routers by sending SNMP broadcasts and lists the devices in a tree diagram. You can also add BinTec routers manually, which can be saved in a permanent list. Devices saved in the permanent list are displayed with every start of the Configuration Manager.

Using Configuration Manager’s network options, you can select different adjustments for listing the devices in the network. Changes made to SNMP variables using the Configuration Manager take effect immediately in the RAM of the BinTec router. To save changes to the flash ROM, you must explicitly save the changes by using the **Save Configuration** command from the **SNMP** menu.

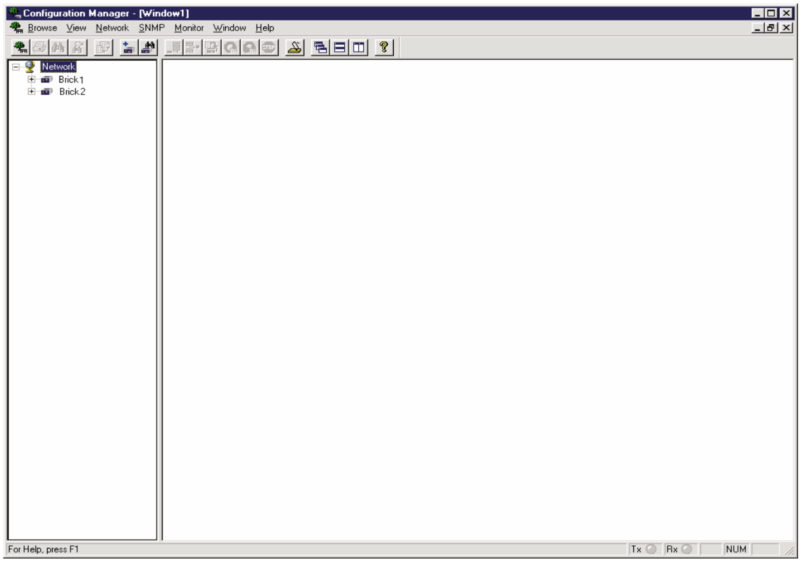


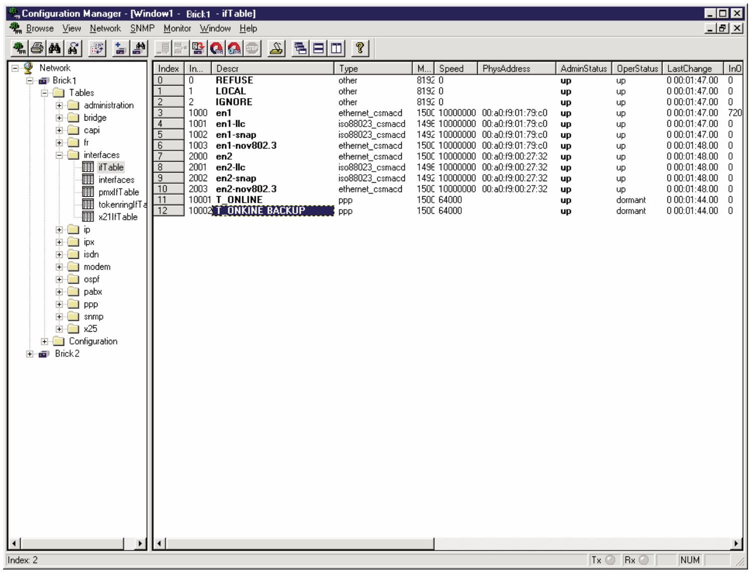
Figure 4-1: Configuration Manager

Beneath the device names (click on the "+" sign), you will find the MIB tables and variables (see figure 4-2, page 54 below).

The PABX folder that lies beneath the Configuration folder is a special extension intended for the configuration of the PABX part of XCENTRIC only.

When you first access a table to be modified, you are prompted for a community password of the BinTec router (default passwords are `bintec` for the admin community and `public` for the write and read communities; for further information on communities, please refer to your **User's Guide**).

All editable indices of a table are displayed in bold print, read-only values are displayed in normal print (see figure 4-2, page 54 below),



Index	In...	Descr	Type	M...	Speed	PhysAddress	AdminStatus	OperStatus	LastChange	InO
0	0	**REFUSE**	other	8192	0		**up**	up	0 00:01:47.00	0
1	1	**LOCAL**	other	8192	0		**up**	up	0 00:01:47.00	0
2	2	**IGNORE**	other	8192	0		**up**	up	0 00:01:47.00	0
3	1000	**en1**	ethernet_csmacd	1500	10000000	00:a0:f9:01:79:c0	**up**	up	0 00:01:47.00	720
4	1001	**en1-llc**	iso88023_csmacd	1496	10000000	00:a0:f9:01:79:c0	**up**	up	0 00:01:47.00	0
5	1002	**en1-snap**	iso88023_csmacd	1492	10000000	00:a0:f9:01:79:c0	**up**	up	0 00:01:47.00	0
6	1003	**en1-nov802.3**	ethernet_csmacd	1500	10000000	00:a0:f9:01:79:c0	**up**	up	0 00:01:48.00	0
7	2000	**en2**	ethernet_csmacd	1500	10000000	00:a0:f9:00:27:32	**up**	up	0 00:01:48.00	0
8	2001	**en2-llc**	iso88023_csmacd	1496	10000000	00:a0:f9:00:27:32	**up**	up	0 00:01:48.00	0
9	2002	**en2-snap**	iso88023_csmacd	1492	10000000	00:a0:f9:00:27:32	**up**	up	0 00:01:48.00	0
10	2003	**en2-nov802.3**	ethernet_csmacd	1500	10000000	00:a0:f9:00:27:32	**up**	up	0 00:01:48.00	0
11	10001	**T_ONLINE**	ppp	1500	64000		**up**	dormant	0 00:01:44.00	0
12	10002	**T_ONKINE BACKUP**	ppp	1500	64000		**up**	dormant	0 00:01:44.00	0

Figure 4-2: Configuration Manager – Tables

When double-clicking an editable index, you get a dialog box in which you can enter a new value for this index. Note that most numerical values can be entered in either decimal, hexadecimal, or octal format:

Format	Prefix	Example
Decimal	none	12
Hexadecimal	0x	0xc
Octal	0	014

Table 4-1: Formats of numerical values

For an explanation of all SNMP tables and variables please refer to the MIB Reference, which can be found on BinTec's Companion CD or on BinTec's FTP Server at http://www.bintec.de.

You can also consult the Configuration Manager's context-sensitive online-help by highlighting a table name or variable name and pressing F1.

The PABX folder that lies beneath the Configuration folder is a special extension intended for the configuration of the PABX part of XCENTRIC only.

4.1 Menu Structure

Configuration Manager has the following menu structure:

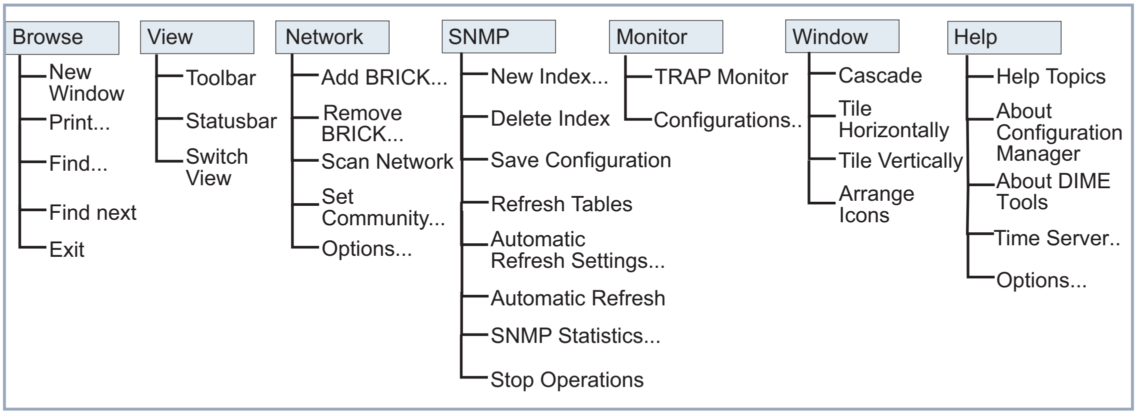


Figure 4-3: Configuration Manager – menu structure

The more important menu items can also be accessed by clicking the appropriate icon in the toolbar:

Icon	Menu	Command
	Browse	New - Open new Browser window
	Browse	Print - Print current table
	Browse	Find - Search for first match of given string in a table name
	Browse	Find next - Search for the next occurrence of the string
	View	Switch View - Swap rows and columns in the current table
	Network	Add BRICK - Add new BinTec router
	Network	Scan Network - Search for connected BinTec routers
	SNMP	New Index - Create new index in current table
	SNMP	Delete Index - Delete selected index from current table
	SNMP	Save Configuration - Store current configuration in the flash ROM of the BinTec router
	SNMP	Refresh Tables - Update all tables
	SNMP	Automatic Refresh - Toggle automatic refresh on/off
STOP	SNMP	Stop Operations - Cancel all current SNMP operations

Icon	Menu	Command
	Monitor	TRAP Monitor - Enables the TRAP Monitor
❐	Window	Cascade - Cascades all open windows
☰	Window	Tile Horizontally
◫	Window	Tile Vertically
?	Help	About Configuration Manager - Displays a short copyright notice

Table 4-2: Icons

The following is a short run through all menu items:

Menu	Command	Meaning
Browse	**New**	Opens a new Browser window. This command can also be activated by clicking the icon.
Browse	**Print**	Prints the current table. This command can also be activated by clicking the 🖨 icon.
Browse	**Find**	Finds the first occurrence of the given string in an SNMP table name and selects that table for viewing. This command can also be activated by clicking the icon.
Browse	**Find Next**	Finds the next occurrence of the string supplied in the Find dialog box. This command can also be activated by clicking the icon.
Browse	**Exit**	Leave Configuration Manager.

Menu	Command	Meaning
View	**Toolbar**	Toggles toolbar on/off.
View	**Statusbar**	Toggles statusbar on/off.
View	**Switch View**	Swaps table view from rows to columns and vice versa. This command can also be activated by clicking the icon or on the top left field of a table (Index or Description).
Network	**Add BRICK**	Add a new BinTec router; e.g. to administrate a BinTec router from a remote network. This command can also be activated by clicking the icon.
Network	**Remove BRICK**	Removes the selected BinTec router from the tree.
Network	**Scan Network**	Scans the local network for connected BinTec routers. This function can be used to update the list of devices currently online. This command can also be activated by clicking the icon.
Network	**Set Community**	Prompts you to enter a community password to gain access to the SNMP tables of a BinTec router.
Network	**Options**	Opens a dialog box from which you can change the IP broadcast behaviour of the BinTec router and the scanning sequence at program start.
SNMP	**New Index**	Creates a new index in the current table. Note that this command and its icon are disabled if no new indices are permitted in this table. This command can also be activated by clicking the icon.
SNMP	**Delete Index**	Deletes the selected index from a table. Note that this command and its icon are enabled only if the current table contains removable indices. This command can also be activated by clicking the icon.

Menu	Command	Meaning
SNMP	**Save Configuration**	Stores the current contents of all tables to the BinTec router as the default boot file boot (same as `cmd=save` issued from the SNMP shell). This command can also be activated by clicking the icon.
SNMP	**Refresh Tables**	Updates the contents of all tables. This command can also be activated by clicking the icon.
SNMP	**Automatic Refresh Settings**	Lets you enter the settings for the automatic refresh of all tables.
SNMP	**Automatic Refresh**	Toggles automatic refresh of all tables on/off. This command can also be activated by clicking the icon.
SNMP	**SNMP Statistics**	Displays statistical data on SNMP packets received or sent by the current BinTec router.
SNMP	**Stop Operations**	Cancels all current SNMP operations. This can be useful to terminate operations for a BinTec router no longer online. This command can also be activated by clicking the STOP icon.
Monitor	**TRAP Monitor**	Enables the TRAP Monitor. This command can also be activated by clicking the icon.
Monitor	**Configurations**	Let’s you define a history file for the output of the TRAP Monitor.
Windows	**Cascade**	Cascades all open Browser windows. This command can also be activated by clicking the icon.
Windows	**Tile Horizontally**	Tiles all open Browser windows horizontally. This command can also be activated by clicking the icon.

Menu	Command	Meaning
Windows	**Tile Vertically**	Tiles all open Browser windows vertically. This command can also be activated by clicking the ◫ icon.
Windows	**Arrange Icons**	Arranges all iconified Browser windows in an orderly fashion.
Help	**Help Topics**	Opens the help window. This function can also be activated by pressing the **F1** key.
Help	**About Configuration Manager**	Displays a copyright notice and version information for the Configuration Manager. This command can also be activated by clicking the ? icon.

Table 4-3: Menu items

4.2 Using the Keyboard

You can operate Configuration Manager from your keyboard without using the mouse.

Select a menu by pressing the **Alt** key together with the underlined letter in the desired menu (e.g. **Alt**-**V** for the **View** menu). You can then select the menu items by either pressing the **Alt** key together with the underlined letter in the item or you can use the cursor **up** and **down** keys to highlight an item and the cursor **left** and **right** keys to change menus – **Return** selects the highlighted item.

When not in the menu, you can switch between the tree display and the table display using the **Tab** key, and move around in the tree or table using the cursor keys. Again, to select the highlighted table or Variable press the **Return** key.

Shortcuts There are a few keyboard shortcuts for frequently used commands. These are mostly activated by simultaneously pressing the **Ctrl** key and the appropriate letter.

Shortcut	Function	Menu
Ctrl-**N**	Open new Browser window	**Browse**
Ctrl-**P**	Print current table	**Browse**
Ctrl-**F3**	Find ...	**Browse**
F3	Find next	**Browse**
Alt-**F4**	Exit	**Browse**
Ctrl-**W**	Switch View	**View**
Ctrl-**A**	Add BRICK	**Network**
Ctrl-**Del**	Remove BRICK	**Network**
Ctrl-**Alt**-**S**	Scan Network	**Network**
Ctrl-**E**	Set Community	**Network**
Ctrl-**I**	New Index	**SNMP**
Ctrl-**Alt**-**I**	Delete Index	**SNMP**
Ctrl-**S**	Save Configuration	**SNMP**
Ctrl-**R**	Refresh Tables	**SNMP**
Ctrl-**O**	Stop Operation	**SNMP**

Table 4-4: Shortcuts

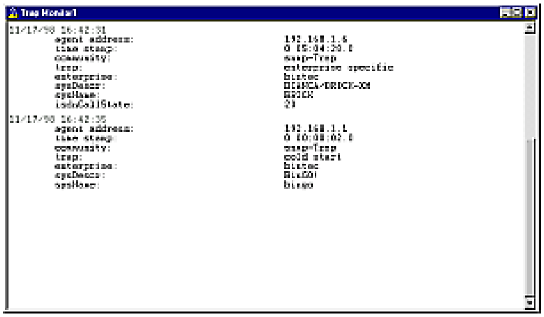
4.3 TRAP Monitor

SNMP traps are sent by the BinTec router to report events. Traps are sent in the form of SNMP PDUs (Protocol Data Units) and can be broadcasted or addressed to defined trap hosts.

Standard traps include information about “coldStart, warmStart, linkDown, linkUp and authentificationFailure”. Enterprise specific traps can be defined in the **biboAdmUsrTrapTable** on the BinTec router by assigning a MIB variable to the variable **biboATrpObj**. Changes in this object are then reported by sending a trap. Only certain objects (columns or tables) are suitable to initialize a trap PDU.

You can enable network-wide broadcasting of traps with the variable **biboAdmTrapBrdCast** in the **biboAdminTable** in the device’s MIB. Another possibility is to define one or more trap hosts traps shall be sent to in the **biboAdmTrapHostTable**. The default SNMP trap port is port 162.

The Configuration Manager includes a TRAP Monitor, which listens for traps on port 162. Traps are received when broadcasted or when your PC is configured as trap host on the BinTec router. The TRAP Monitor must be enabled.



```
11/17/98 16:42:31
         agent address:                        192.168.1.6
         time stamp:                           0 05:04:20.0
         community:                            snmp-Trap
         trap:                                 enterprise specific
         enterprise:                           bintec
         sysDescr:                             BIANCA/BRICK-XM
         sysName:                              BRICK
         isdnCallState:                        28
11/17/98 16:42:35
         agent address:                        192.168.1.1
         time stamp:                           0 00:00:02.0
         community:                            snmp-Trap
         trap:                                 cold start
         enterprise:                           bintec
         sysDescr:                             BinGO!
         sysName:                              bingo
```

Figure 4-4: TRAP Monitor

With the command **Monitor** ➧ **TRAP Monitor**, the TRAP Monitor is started and with **Monitor** ➧ **Configurations**, you can define a history file for the TRAP Monitor.

5 Remote CAPI and Remote TAPI

This chapter contains information about the following items:

- Remote CAPI Client
- Remote TAPI Client
- CAPI and/or TAPI Configuration

5.1 Remote CAPI Client

The CAPI (Common ISDN Application Programming Interface) provides an interface for communication applications (CAPI applications) that are used for file transfer, fax or application-sharing like RVS-COM Lite, for example.

The Remote CAPI Client acts as a mediator between local CAPI applications (running on the PC) and the CAPI Server (running on the BinTec router). The CAPI Server allows CAPI applications running on different hosts (on the local network) to simultaneously access the ISDN interfaces of the BinTec router.

The Remote CAPI Client comprises the 16-bit CAPI 1.1 and CAPI 2.0 dynamic link libraries (CAPI.DLL and CAPI20.DLL) and a 32-bit CAPI 2.0 library (CAPI2032.DLL). For Windows NT 4.0, 98, ME, 2000 and higher, a special CAPI 2.0 library (CAPI2032.DLL) is provided, which supports the Remote Multi CAPI (see chapter 6, page 73).

For CAPI applications to be able to access the server the CAPI.DLL or CAPI20.DLL must be available locally. Each PC that you intend to run CAPI applications from should have the following files present:

- **CAPI.DLL** and **CAPI20.DLL**
  Dynamic link libraries for all operating systems supported, providing an interface for 16-bit CAPI 1.1 and CAPI 2.0 applications.
- **CAPI2032.DLL**
  Dynamic link library for Windows 95/98 and Windows NT 4 and higher, providing an interface for 32-bit CAPI 2.0 applications.
  For Windows NT 4.0, 98, ME, 2000 and higher, this dynamic link library supports the Remote Multi CAPI (see chapter 5, page 63).
- **CAPI2WSA.EXE**
  Required by CAPI.DLL and CAPI20.DLL, CAPI messages are sent to this “hidden application” by the DLLs. Here, the messages are placed in TCP/IP packets and subsequently sent to the CAPI server on your BinTec router.

- **Remote Clients Configuration program**
  For all operating systems supported, a configuration tool for CAPI and TAPI. For a description of this application (Rxc_cfg.exe), please refer to chapter 5.3, page 67.

5.2 Remote TAPI Client

The TAPI (Telephony Application Programming Interface) is an interface that is accessed by telephony applications (CTI) to use telephone equipment attached to the router to place, accept and monitor calls.

The Remote TAPI Client acts as a mediator between local telephony applications running on the PC and the TAPI Server running on the BinTec router. The TAPI Server allows TAPI applications running on your PC access to the POTS interfaces of your BinTec router. TAPI is available, for example, on the products BinGO! Plus/Professional and XCentric.

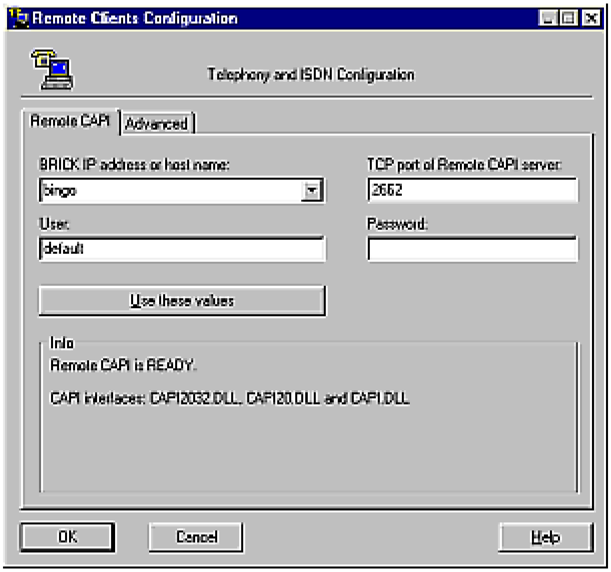
The Remote TAPI Client comprises the 16-bit TAPI 1.4 Telephony Service Provider (RTC_SPI.TSP for Windows 95) and the 32-bit TAPI 2.0 Telephony Service Provider (RTC32.TSP for Windows NT 4.0, 98, ME, 2000).

5.3 CAPI and/or TAPI Configuration

On all operating systems supported, the Remote Clients Configuration program can be used to enter a BinTec router as a CAPI or TAPI Server for running remote CAPI or TAPI applications on your PC. After starting the program, a configuration page is displayed, as shown in figure 5-1, page 67 below. Depending on whether you installed TAPI, either the TAPI and/or the CAPI page is displayed.

If you want to configure CAPI instead of TAPI, simply select the **Remote CAPI** tab. The CAPI page contains the same fields as the TAPI page, so we'll only explain these fields once.

TAPI is only available on products with analog POTS ports and PABX functionalities. All other BinTec routers only run a CAPI Server.


Remote Clients Configuration
Telephony and ISDN Configuration
Remote CAPI
Advanced
Use these values
OK
Cancel
Help

BRICK IP address or host name: bingo

TCP port of Remote CAPI server: 2662

User: default

Password:

Info

Remote CAPI is READY.

CAPI interfaces: CAPI2032.DLL, CAPI20.DLL and CAPI.DLL

Figure 5-1: Remote Clients Configuration

- **Device IP address or host name**
  Enter the BinTec router's IP address or host name here. You can use the listbox to choose from the BinTec routers already known to your PC, or enter a name or IP address manually.

- **TCP Port of remote CAPI/TAPI server**
  This field contains the default TCP port for CAPI or TAPI connections, 2662 for CAPI, 2663 for TAPI. You should only change these values if – for some reason – these TCP ports are already being used for other purposes on your PC.

Make sure to use the same ports as on your BinTec router (Setup Tool: ***IP*** ➧ ***STATIC SETTINGS*** for the CAPI port, ***PABX*** ➧ ***STATIC SETTINGS*** for the TAPI port; SNMP shell: **admin** table for both ports).

- **User**
  In this field you can enter the user who is authorized to use the CAPI (or TAPI) features of this BinTec router. You can configure a user for the CAPI features and, if available, for the TAPI features.
  Note that these users must also be configured on the device in the ***CAPI*** ➧ ***USER*** menu (or ***PABX*** ➧ ***USER*** menu) of Setup Tool.
  On the BinTec router there is a factory-configured user default, which does not have a password, and has all rights for CAPI and TAPI usage.
  This user is also the default setting used in the Remote Clients Configuration program.

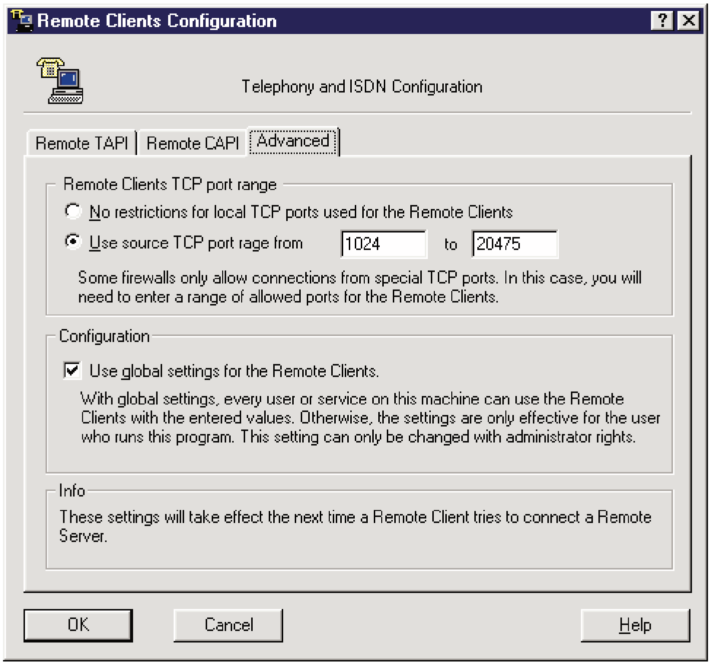
- **Password**
  The password for this user. If you leave this field empty, no password is used. On the BinTec router (in the ***CAPI*** ➧ ***USER*** menu / ***PABX*** ➧ ***USER*** menu of Setup Tool), the corresponding **Password** field must then also be empty.
  CAPI and TAPI user and password settings are stored in the Registry of Windows 95/98 or NT separately for each Windows user. This way you can configure different CAPI/TAPI user settings for each Windows user at the same PC.
  If a new Windows user logs in to your system, he will get the router configuration of the previous user, but all CAPI and TAPI users will be set to user default.

Under Windows NT, system services, which are started automatically, normally login using the NT system account. Since you cannot login to the system account yourself – and therefore cannot configure CAPI or TAPI users and passwords for the system account – you will have to configure the services which use CAPI or TAPI in order to login to a Windows NT user account, but not to the system account. (e.g. your own Windows account). This can be achieved from the **Control Panel** ➧ **Services dialog**. Some service like RAS, for example, however, will not work with this configuration, because they need to run in the system context.

- **Use these values**
  Once you have entered the correct host and TCP port click the **Use these values** button to activate your settings.

- **Info**
  The info area in the lower half of the page shows the CAPI or TAPI status based on its current settings. Note that the status may change, depending on the current operating status, e.g. “Trying to connect to host ‘mybintec’, port 2662”.

On the **Advanced** page you can specify a source TCP port range to be used for CAPI and TAPI connections.



Remote Clients Configuration

Telephony and ISDN Configuration

Remote TAPI | Remote CAPI | Advanced

Remote Clients TCP port range

○ No restrictions for local TCP ports used for the Remote Clients

● Use source TCP port rage from 1024 to 20475

Some firewalls only allow connections from special TCP ports. In this case, you will need to enter a range of allowed ports for the Remote Clients.

Configuration

☑ Use global settings for the Remote Clients.

With global settings, every user or service on this machine can use the Remote Clients with the entered values. Otherwise, the settings are only effective for the user who runs this program. This setting can only be changed with administrator rights.

Info

These settings will take effect the next time a Remote Client tries to connect a Remote Server.

Figure 5-2: Source TCP port range settings

As a default there are no restrictions for the TCP ports, which should be fine for most environments.

However, in conjunction with certain firewalls, which – for security reasons – only allow TCP traffic over a limited range of TCP ports, these settings are necessary.

User-Specific or Global CAPI/TAPI Settings

Users can store their CAPI/TAPI configurations in one of two different ways. Either the settings apply to all users on that machine or to just the current user.

You can either select the **Use global settings for the Remote Clients** check box to make settings available to all users of that machine, or you can clear the box and the CAPI/TAPI settings are user-specific.

The **Use global settings for the Remote Clients** check box is selected by default.

For most fax server applications the default setting for the **Use global settings for the Remote Clients** check box is required.

Windows NT/2000

The **Use global settings for the Remote Clients** check box is disabled if the user does not have the necessary administration rights. This measure is designed to prevent unauthorised users from switching the CAPI/TAPI settings from the global to the user-specific settings.

Windows 95/98

The **Use global settings for the Remote Clients** check box is permanently enabled.

6 Remote Multi CAPI Client

The Remote Multi CAPI Client (RMCC), an enhanced 32-bit CAPI (capi2032.dll), enables you to use multiple BinTec routers for CAPI 2.0 connections from one PC running Windows NT 4.0, 98, ME, 2000. The RMCC allows your CAPI 2.0 applications to take advantage of all ISDN controllers available through one or more BinTec routers on the LAN. By providing a pool of available ISDN controllers, access to the ISDN remains transparent to the application.

This can, for example, be useful for fax server applications which can then send and receive several faxes at the same time.

To make use of the RMCC feature, your 32-bit CAPI 2.0 applications must be able to address several different CAPI controllers at the same time.

To make use of the RMCC feature, your 32-bit CAPI 2.0 applications must be able to address several different CAPI controllers at the same time.

RMCC is also able to automatically reconnect to a BinTec router after it has rebooted, i.e. you do not manually have to stop and restart all CAPI 2.0 applications if the device reboots.

6.1 Installation

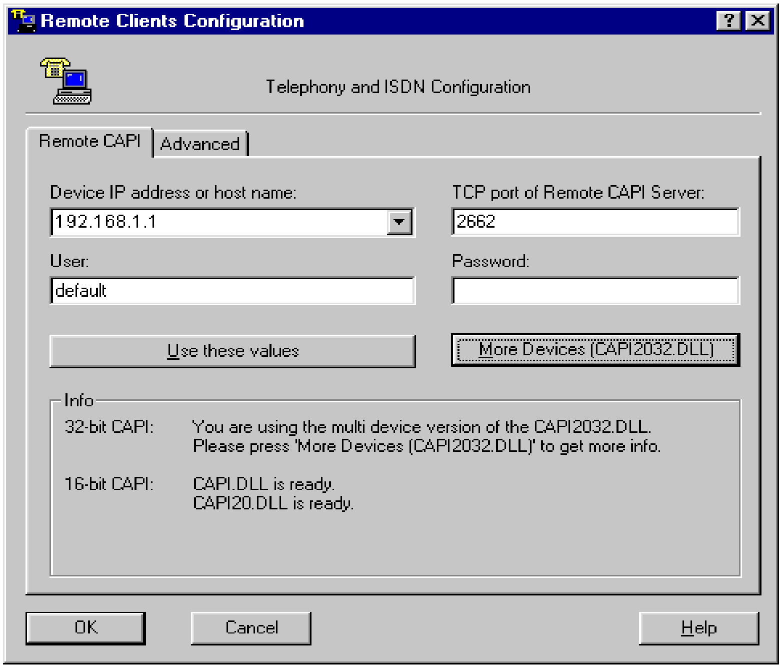
If you have Windows NT 4.0, 98, ME, 2000 running on your PC, the Remote Multi CAPI Client (an enhanced version of the CAPI2032.DLL) will be installed automatically during the BRICKware for Windows installation.

The 16-bit versions of CAPI 1.1 (CAPI.DLL) and of CAPI 2.0 (CAPI20.DLL) are, of course, still available for use with one BinTec router at a time.

6.2 Configuration

Make sure to close all CAPI applications before changing your CAPI configuration.

You can configure the 16-bit CAPI versions and TAPI as described in chapter 5.3, page 67. The BinTec router configured in this dialog will be used for 16-bit CAPI applications and is also used initially for 32-bit CAPI applications, i.e. for the Remote Multi CAPI.



Remote Clients Configuration

Telephony and ISDN Configuration

Device IP address or host name: 192.168.1.1

TCP port of Remote CAPI Server: 2662

User: default

Password:

Info

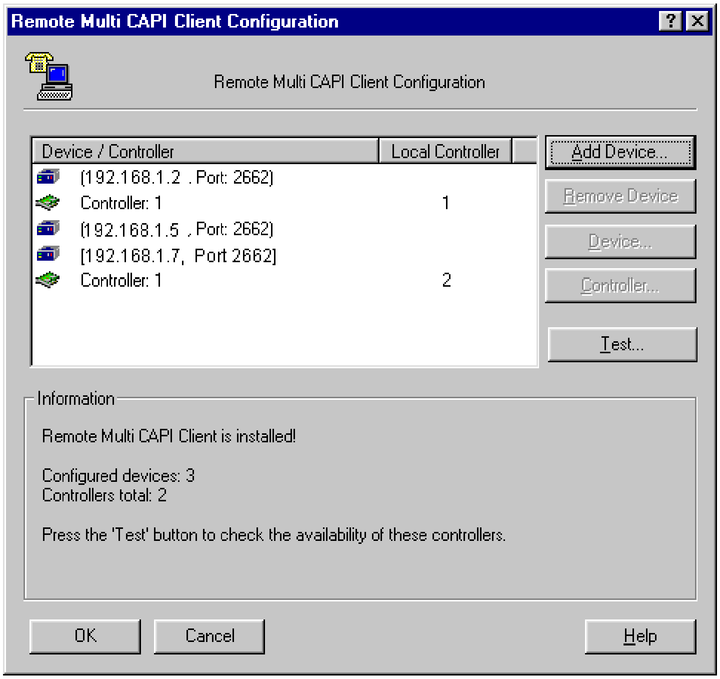
32-bit CAPI: You are using the multi device version of the CAPI2032.DLL. Please press 'More Devices (CAPI2032.DLL)' to get more info.

16-bit CAPI: CAPI.DLL is ready. CAPI20.DLL is ready.

Figure 6-1: Remote Clients Configuration – CAPI page

More devices To configure the Remote Multi CAPI Client – i.e. if you want to use two or more devices simultaneously – press the **More Devices** button.

You will then get a list of all devices currently configured and their controllers which will be available for 32-bit CAPI 2.0 applications (see figure 6-2, page 76).


Remote Multi CAPI Client Configuration

Remote Multi CAPI Client Configuration

Device / Controller	Local Controller
[192.168.1.2 . Port: 2662]	
Controller: 1	1
[192.168.1.5 , Port: 2662]	
[192.168.1.7, Port 2662]	
Controller: 1	2

Information

Remote Multi CAPI Client is installed!

Configured devices: 3
Controllers total: 2

Press the 'Test' button to check the availability of these controllers.

Figure 6-2: Remote Multi CAPI Configuration – More devices

The list will initially be empty (unless you have already configured a BinTec router on the main CAPI page, see figure 6-1, page 75 above).

If you select a BinTec router from this list, the **Info** field in the lower half of the dialog box will display the number of controllers available on this BinTec router, the system software revision, the serial number, and the CAPI version.

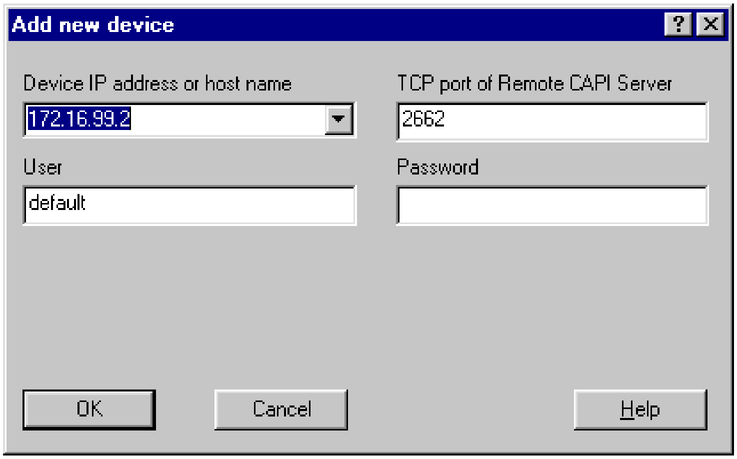
If you select a controller from this list, the **Info** field will display the number of B-channels available from this controller, whether DTMF tones are supported, and the supported B1, B2, and B3 layer protocols.

Changes made to this list (for 32-bit CAPI applications) will not affect the settings made for 16-bit CAPI applications in the main CAPI dialog.

The buttons on the right hand side of the **More devices** dialog have the following meanings.

Add device

To add a device click the **Add Device** button. Enter its host name or IP address, its CAPI TCP port, the User name and Password (see explanation of User and Password in chapter 5.3, page 67) in the appropriate fields. When you click the **OK** button to confirm your entries, the application will try to establish a connection to the device, verify the given User and Password entries, and retrieve information on the number of controllers available on this device and on its system software release and serial number.



Device IP address or host name: 172.16.99.2

TCP port of Remote CAPI Server: 2662

User: default

Password:

Figure 6-3: Add device

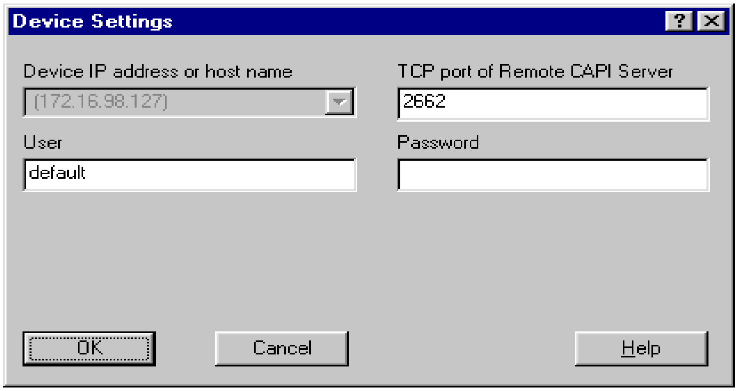
This may take a couple of seconds. If the connection fails, make sure the device is switched on, connected to the network, the IP address, CAPI TCP port, and user and password data are correct, and try again.

All controllers of the device will be added to the list of available controllers and will automatically be assigned a new local controller number.

The list of local controller numbers always starts with controller #1 and does not contain any gaps, e.g. if you remove a device or disable a controller, the remaining controllers are automatically renumbered.

Remove device Removes the selected device and its controllers from the list of available controllers.

Device... By double-clicking a device (or first selecting the device and then clicking the **Device** button) you get the following dialog box:



Device Settings

Device IP address or host name: (172.16.98.127)

TCP port of Remote CAPI Server: 2662

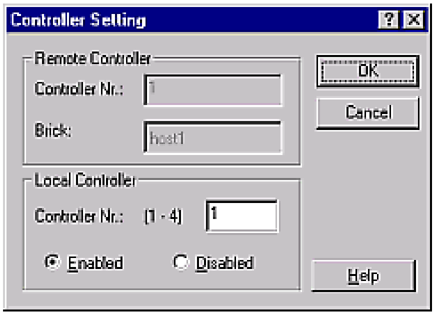
User
default

Password:

Figure 6-4: Device Settings

Here you can change the CAPI TCP port, User and Password settings for this device. When you click the OK button the application will try to establish a connection to the device. See section Add device above for details.

Controller... By double-clicking a controller (or first selecting the controller and then clicking the **Controller..** button) you get the following dialog:


Controller Setting

Remote Controller

Controller Nr.: 1

Brick: host1

Local Controller

Controller Nr.: (1 - 4) 1

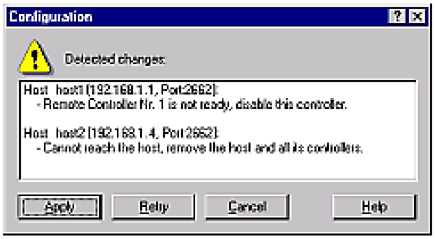
● Enabled ○ Disabled

Figure 6-5: Configure Controller

Here you can assign a different local controller number to the controller, or enable or disable it for CAPI connections.

Test After changing your configuration you should click the **Test** button. The program will try to verify the data of all devices and controllers currently configured. You can interrupt the test with the **Stop Test** button. If the test reports no errors, you can save your configuration with the **OK** button.

If any errors are detected, the program will display a dialog box similar to the following, suggesting what to do in the case of the detected discrepancies.


Configuration

Detected changes:

Host host1 [192.168.1.1, Port:2662]:
- Remote Controller Nr. 1 is not ready, disable this controller.

Host host2 [192.168.1.4, Port 2662]:
- Cannot reach the host, remove the host and all its controllers.

Figure 6-6: Error message

Click the **Apply** button to make the suggested changes. Clicking **Cancel** leaves your configuration unchanged, but the discrepancies found will be marked with an exclamation mark(❗ or ❗) in the list of devices and controllers (see figure 6-2, page 76).

7 Device at COM1/COM2

Device at COM1 and Device at COM2 are links to the Windows Hyperterminal, configured to allow you to communicate directly with a BinTec router that is connected to serial port COM1 or COM2 of your PC respectively.

You can use these programs to configure and administer your BinTec router manually using either the Setup Tool described in the **User's Guide**, or the SNMP shell commands described in the **Software Reference**.

8 TAF Login Program

Token Authentication Firewall (TAF) is an advanced feature for controlling access to central site computing resources that goes beyond the theoretical limitations of existing security mechanisms. TAF is a user-oriented security system, which affords human interaction and thus ensures that an authorized user is sitting in front of the remote host, which is connected to the central site.

TAF login user verification is based on the tried and trusted Token-Card-ACE/Server solution provided by Security Dynamics.

You will need a special TAF license to use TAF on your BinTec router. Along with this license you will get 10 TAF Login licenses for PCs you wish to use as TAF clients.

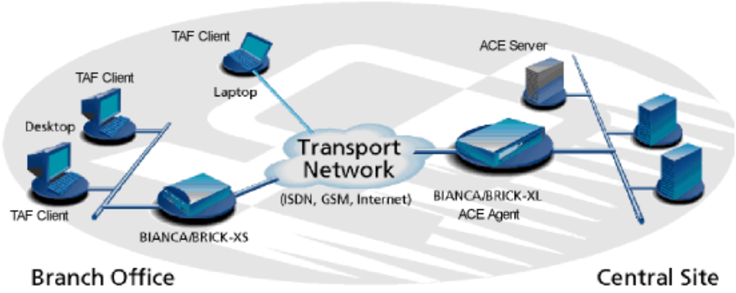


Figure 8-1: TAF Clients, ACE Agent and ACE Server

A security solution using TAF is made up of four components:

- an ACE/Agent by BinTec in the central site
- an ACE/Server by Security Dynamics in the central site
- a Token Card by Security Dynamics for the user of the TAF client PC
- an application for the TAF client PC by BinTec

8.1 Requirements for TAF

As a requirement for the TAF authentication procedure the four components (as mentioned above) must be established. Based on an existing WAN partner connection (Remote Client - LAN, LAN - LAN) the following conditions must be provided.

In the central site LAN, an ACE/Server must be set up and the central site's BinTec router must be configured as an ACE agent to serve as remote access server to the central site's LAN.

The client side PC must have the TAF login program installed and configured, and its user must be in possession of the Token Card, which generates the passwords for the TAF login.

Figure 8-2: Token Card

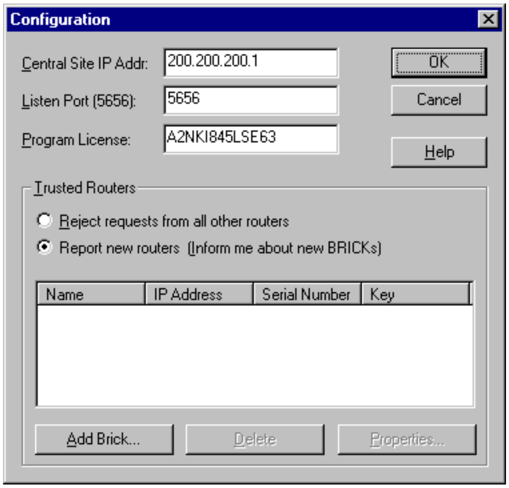
TAF, on the whole, and all its configuration steps are described in detail in BinTec's **Extended Feature Reference**, which can be retrieved from BinTec's file server (Section: Download) at http://www.bintec.de.

In this part of the **BRICKware for Windows** documentation, we will only describe the configuration of the client PC using the TAF login program contained in BRICKware for Windows.

8.2 Installation and Configuration of the TAF Login Program

When you want to use TAF Login from a PC, you must select TAF Login in the Components list during the installation of BRICKware for Windows. In case you already have installed other components of BRICKware and want to add TAF Login, we recommend reinstalling all components of BRICKware (including TAF).

The TAF Login program will automatically be installed in your Autostart menu (you may have to select this during installation). If the TAF Login is not automatically started after the installation is complete, you must select TAF Login from the BRICKware group in the Start menu. In the Login dialog box, you must select Configuration to configure the Login program. You enter the BinTec router's (ACE/Agent of the central site LAN) IP address in this dailog box and can modify the Listen Port, if necessary (the listen port setting on the PC must be identical to the setting on the BinTec router). Above that you must enter the program's license key for the TAF client, which is provided together with your BinTec router's TAF license.



Configuration

Central Site IP Addr: 200.200.200.1

Listen Port (5656): 5656

Program License: A2NKI845LSE63

Trusted Routers

○ Reject requests from all other routers

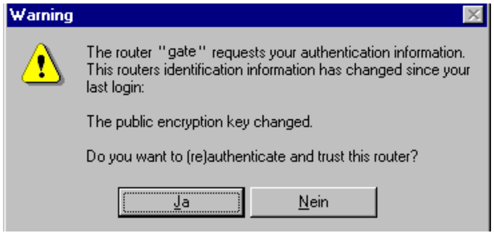
● Report new routers (Inform me about new BRICKs)

Name	IP Address	Serial Number	Key

Figure 8-3: TAF Configuration

Repeat this procedure on each PC you want to use for TAF authentication. Each PC needs its own TAF client license.

In the **Trusted Routers** group you can select whether only to accept logins from trusted routers or also be notified when a router not contained in the trusted routers list below sends a login request. In the notification (shown below), you can then decide whether to trust the new router. Trusted routers are displayed in the list at the bottom of the Trusted Routers group.



The router "gate" requests your authentication information.
This routers identification information has changed since your last login:

The public encryption key changed.

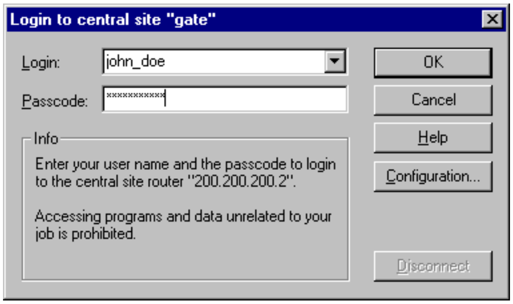
Do you want to (re)authenticate and trust this router?

Figure 8-4: Notification about the login request of a router not contained in the **trusted routers** list

8.3 Using TAF Login

The TAF Login program is added to the Autostart menu and remains in the background until it receives an authentication request from the remote LAN.

You can also activate the program by double-clicking the TAF icon in the task bar or by starting it from the BRICKware program group to start the authentication procedure from your TAF client PC.



Login to central site "gate"

Login: john_doe

Passcode: ************

Info

Enter your user name and the passcode to login to the central site router "200.200.200.2".

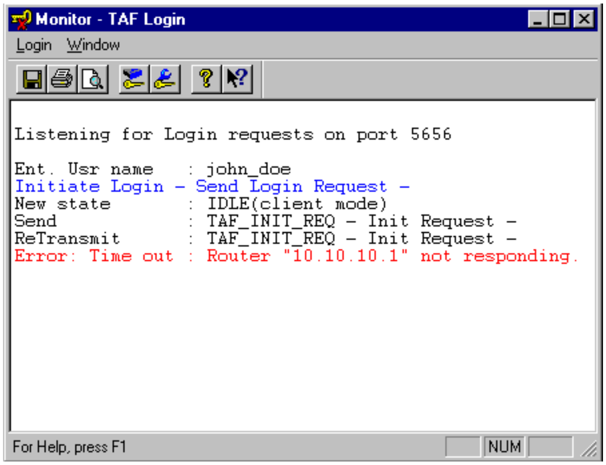
Accessing programs and data unrelated to your job is prohibited.

Figure 8-5: TAF Login

Enter your login name for the ACE/Server and the passcode displayed on your Token Card. Click the **OK** button.

If the authentication is successful, the TAF Login dialog is closed and the TAF icon in the task bar changes to ✓ , if the authentication fails, an error message is displayed and the icon remains ✗ .

TAF Login also includes a monitoring function. If you right-click the TAF icon you will get a menu from which you can select **Show Monitor Window**.



```
Listening for Login requests on port 5656

Ent. Usr name    : john_doe
Initiate Login - Send Login Request -
New state        : IDLE(client mode)
Send             : TAF_INIT_REQ - Init Request -
ReTransmit       : TAF_INIT_REQ - Init Request -
Error: Time out  : Router "10.10.10.1" not responding.
```

Figure 8-6: TAF Monitor

All important activities concerning TAF are logged in this window. You can also initiate a login or configure the program from this window.

9 Windows Activity Monitor

From BRICKware version 5.2.1, an online Help is available with the Activity Monitor program. There you will find the complete documentation for this application.

10 Configuration Wizard

A context-sensitive online Help is available with the Configuration Wizard program. There you will find the complete documentation for this application.