

BRICKware for Windows

for
BIANCA/BRICK,
BinGO!, and VICAS

Copyright © 1999 BinTec Communications AG
All rights reserved

NOTE

The information in this manual is subject to change without notice.

This manual provides a description of the BRICKware for Windows utility programs for the BinTec BIANCA/BRICK, BinGO!, and V!CAS routers. The information included in this manual is compatible with software version 4.9.

While every effort has been made to ensure the accuracy of all information in this document, 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 and the BinTec logo are registered trademarks of BinTec Communications AG.

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

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means – graphic, electronic, or mechanical – including photocopying, recording in any medium, taping, or storage in an information retrieval systems, without the prior written permission of the copyright owner.

- kg



BRICKware for Windows

1	Overview	1
1.1	DIME	2
1.2	Remote CAPI Client and Remote TAPI Client	3
1.3	Configuration Wizard	4
1.4	BRICK at COM1 and BRICK at COM2	5
1.5	Token Authentication Firewall (TAF) Login Program	5
1.6	Java Status Monitor	6
2	Installation	7
2.1	Installing BRICKware	7
2.2	Checking and Installing the TCP/IP Protocol	12
2.3	Uninstall BRICKware	13
3	DIME Tools	15
3.1	Starting up the Toolkit	15
3.2	Menu Structure	16
3.3	BootP Server	20
3.4	DIME Tracer	24
	ISDN Trace	25
	CAPI Trace	27
3.5	TFTP Server	28
3.6	Syslog Daemon	30
3.7	Time Server	33

4	DIME Browser	36
4.1	Menu Structure	38
4.2	Using the Keyboard	43
4.3	TRAP Monitor	45
5	Remote CAPI and Remote TAPI	47
5.1	Remote CAPI Client	47
5.2	Remote TAPI Client	48
5.3	Remote CAPI Configuration under Win- dows 3.1	49
5.4	CAPI and/or TAPI Configuration	51
6	Remote Multi CAPI Client	55
6.1	What is it?	55
6.2	Installation	55
6.3	Configuration	55
7	BRICK at COM1/COM2	61
8	TAF Login Program	62
8.1	Requirements for TAF	63
8.2	Installation and Configuration of the TAF Login Program	64
8.3	Using TAF Login	66
9	Java Status Monitor	68
9.1	Structure of the Java Status Monitor	69
	Summary Panel	70
	Interface Panel	71
	PPP Partner Panel	71
	Panels for the Different Slots	73
9.2	Customizing the Java Status Monitor.	75



BRICKWARE FOR WINDOWS

1 Overview

BRICKware for Windows is a software package containing programs to help you install, configure and maintain your BIANCA/BRICK, BinGO!, or V!CAS.

BRICKware for Windows consists of two main parts. Firstly, the *Desktop Internetworking Management Environment*, *DIME* for short, is a suite of utilities for administering and tracing BRICKs 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.

A Configuration Wizard is included with the products BIANCA/BRICK-XS/XS office, BinGO! and BinGO! Plus/Professional and can be used for a basic initial configuration of your router. For a step-by-step description of how to install your router 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.

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.

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 BRICK 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 BRICKs 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 BRICKs. 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 BRICK 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 BRICK and your PC via *TFTP*. You can, for example, use the TFTP Server

to store different versions of your BRICK's configuration, or to update its system software as described in the *User's Guide*.

- ♦ *Syslog Daemon* – actively displays system messages received from the BRICK and stores them in various files for future reference.
- ♦ *Time Server* – enables your PC to supply your BRICK with the current time.
- ***DIME Browser*** – SNMP Manager provides easy access to all the BRICK's SNMP tables and variables via a graphical user interface.

You can use *DIME Browser* for all configuration and administration purposes, provided you know which values need to be changed to achieve your goal. If you are new to BRICK administration, the menu-driven Setup Tool (explained in your *User's Guide*) might be the better choice of tools. For an initial configuration of the BIANCA/BRICK-XS, BinGO! and BinGO! Plus/Professional, 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 BRICK 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 BRICK from your PC, or to display information about the caller from a database to help you decide whether to take the call.

The *Remote TAPI Client* is only available on the BinGO! Plus/Professional and V!CAS.

- *Remote Multi CAPI Client (RMCC)* – provides a CAPI 2.0 interface for multiple BRICKs for Windows NT 4.0 systems. With RMCC installed, you can use the ISDN interfaces of all BRICKs 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

With the *Configuration Wizard* included in the *BRICKware* for Windows, you can start running your BIANCA/BRICK-XS/XS office, BinGO! or BinGO! Plus/Professional 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*.

For a step-by-step description of how to install your BIANCA/BRICK-XS/XS office, BinGO! or BinGO! Plus/Professional 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 BRICK at COM1 and BRICK at COM2

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

1.5 Token Authentication Firewall (TAF) Login Program

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)

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 BRICK. 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 (BRICK-XL2, BRICK-XM with 2 MB flash or BRICK-XMP)
- an ACE Server by Security Dynamics
- a Token Card by Security Dynamics
- a Windows application for the client PC by BinTec

1.6 Java Status Monitor

The included Java Status Monitor allows you to monitor your BRICK dynamically via a Web Browser.

Information monitored covers the current traffic on each interface and connection information. Access to the Status Monitor is secured by passwords and only read access is allowed.

2 Installation

2.1 Installing BRICKware



Note that *BRICKware for Windows* requires the TCP/IP protocol to be installed on your computer. If you are not sure whether the TCP/IP protocol is installed on the PC, see paragraph [2.2 Checking and Installing the TCP/IP Protocol](#) in this chapter.

BRICKware for Windows requires up to 8 MB of space on your hard disk. If you are using *Windows 3.1* and want to use *DIME Browser* and/or the TAF Client, you have to install *Win32s* (it is included on the CD and you are asked for it during installation), which requires an additional 3 MB of hard disk space.



Note that you should install *DIME Browser* and *DIME Tools* on the network 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 BRICK's Remote CAPI or Remote TAPI feature. You can only make use of the TAPI if your BRICK has a POTS module (CM-AB) built in (all BinGO! Plus/Professional and V!CAS routers contain this module as a default).

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.

- 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**.
- Click **BRICKware** to start the setup program.
- Define the directory BRICKware shall be installed to. We recommend accepting the default path settings or using a “short” folder name to stay compatible with 16-bit applications.
- Select one or more types of BinTec routers



Figure 1: Custom Installation - BRICKS

- Select the software components you want to be installed.



Figure 2: Custom Installation - Options

- If you selected to install *DIME Tools*, the setup program suggests to automatically start *DIME Tools* at every start of Windows. This is especially useful when you want to use *BootP Server*, *TFTP Server*, *Syslog Daemon* or *Time Server* (see pp. [20f](#), [28f](#), [30f](#)). 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 the dialog box *Configure your BRICK and this PC* appears. This dialog box, depending on your type of BRICK, contains several options for the configuration of your BRICK (and the local PC):

Initial BRICK configuration with the Wizard

Choose this option to create a new configuration on your BIANCA/BRICK-XS, BinGO! or BinGO! Plus/Professional using the Configuration Wizard (see [Configuration Wizard](#) on page 4). This option is only available for the routers mentioned. It is rec-

ommended to access your router via the serial connection. The Configuration Wizard opens.

Initial basic BRICK configuration using BootP

Choose this option if you want to initially configure your router via BootP to assign an IP address and other basic data. This option only makes sense when your router is absolutely unconfigured and the Configuration Wizard is not available for your type of router (that is for all modular routers). After clicking *Next*, the BootP Server opens.

Keep old BRICK configuration

Choose this option to keep the current configuration of your router or if you just want to modify the configuration later, for example, using the Setup Tool. After you clicked *Next*, the CAPI(/TAPI) configuration of your PC is started.

Keep old BRICK and PC configuration (exit setup)

Choose this option to keep the current configuration of your router and also to keep the CAPI/TAPI configuration of the local PC. When you choose this option, setup is finished and no additional configuration is requested.

**DIME Browser &
Windows 3.1**

If you are installing *DIME Browser* under Windows 3.1, the setup program will check to see if version 1.3 of Win32s is installed on your system (*DIME Browser* is a Win32-based application that needs the operating system extension Win32s to run under Windows 3.1). If version 1.3 of Win32s is not found, the setup program asks if you want to install it first. If you answer *yes*, the program will automatically start Win32s' own installation program (located on the CD in the `\addons\win32s` directory), which then takes over.



After the Win32s installation is complete and you have rebooted the system, you have to start *setup* again, as described above.

**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 the products BIANCA/BRICK-XS, BinGO! and BinGO! Plus/Professional, we recommend using the BinTec Configuration Wizard for an initial configuration.

Other BRICKs can be configured via the serial interface of your PC using the Setup Tool (see [7 BRICK at COM1/COM2](#)).

To use Setup Tool via telnet (see *User's Guide*) or the DIME Browser (see p. [36](#)) for a configuration of your BRICK, first a name, IP address and netmask must be assigned to the BRICK with the help of the BootP Server.

As soon as the *BootP Server* receives a BootP request from your new BRICK, it opens the *BootP Server Configuration* window (see p. [21](#)). Here you can enter the name, IP address and netmask for your BRICK.

Another way to carry out remote configuration is to use the *isdnlogin* command from a remote BRICK on the BRICK 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 3: BRICKware Start Menu Group

2.2 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. 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 [2.1 Installing BRICKware](#).

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.

2.3 Uninstall BRICKware

You can use the Uninstall from the BRICKware submenu to uninstall BRICKware.

In addition to removing all the files copied to your hard disk during the installation process, Uninstall also removes all entries made to the Windows system files—except for configuration entries. All BRICKware applications which are running when you start Uninstall are stopped.

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

Another way to uninstall BRICKware is to choose **Software** from Windows **Control Panel** and there select **BRICKware** and uninstall it.



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

3 DIME Tools

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 re-opened 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.

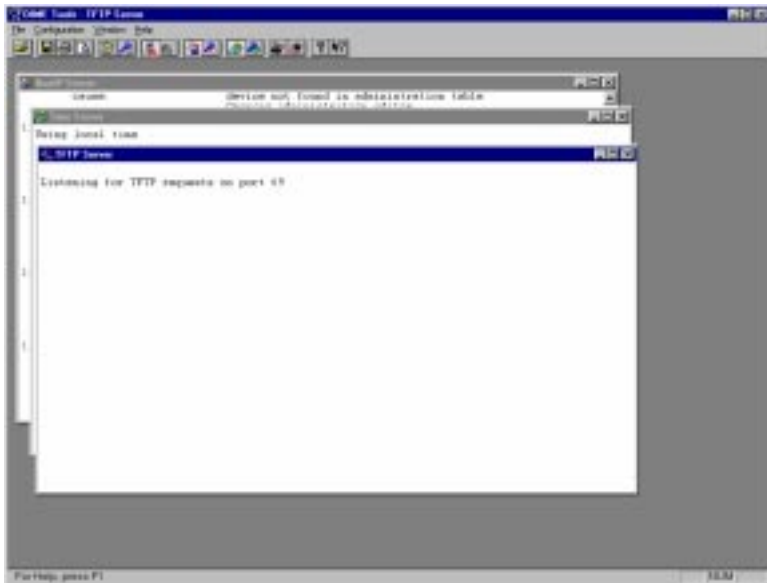


Figure 4: DIME Tools – Main window

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

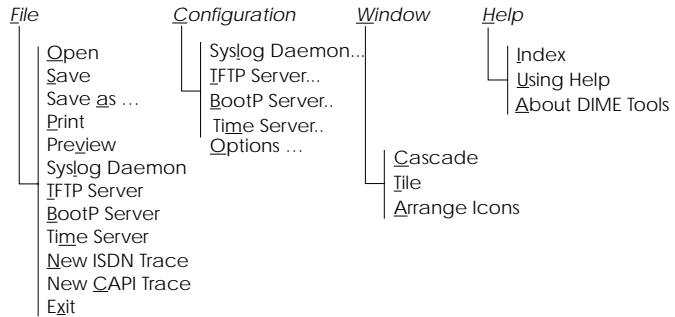
The different parts of DIME Tools are then described in detail separately.



Notice that DIME Tools is a 16-bit application and therefore you must use the MS-DOS 8.3 notation for file names and directories, for example.












3.2 Menu Structure

DIME Tools has the following 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 BRICK 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
	File	New CAPI Trace - Open a new DIME Tracer window
	Help	About DIME Tools - Display a short copyright message
		Activate context-sensitive help

The following is a short run through all menu items:


File


- Open** Opens a configuration, syslog or trace file of a BRICK for viewing or editing. This function can also be activated by clicking the  icon.
- 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.


Save as Save text contents of current window in the specified file.

Print Prints the text contents of the active window. This function can also be activated by clicking the  icon.

Preview Displays a print-preview of the text contents of the active window. This function can also be activated by clicking the  icon.


Syslog Daemon

Opens the Syslog Daemon window (if not already open).

This function can also be activated by clicking the  icon.


TFTP Server

Opens the TFTP Server window (if not already open).

This function can also be activated by clicking the  icon.


BootP Server

Opens the BootP Server window (if not already open).

This function can also be activated by clicking the  icon.


Time Server

Opens the Time Server window (if not already open).

This function can also be activated by clicking the  icon.


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 page [25](#)).

This function can also be activated by clicking the  icon.

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 page [25](#)).

This function can also be activated by clicking the  icon.

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.


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.


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.

Time Server

Opens a dialog box where you can select whether the PC's local time or GMT shall be sent to the BRICK.

This function can also be activated by clicking the  icon.

Options Opens a dialog box from which you can change the IP broadcast behaviour of the BRICK and the colours used for the output in all DIME Tools windows. You can also restore the default colour settings.

Window

Cascade Cascade all open DIME Tools windows.

Tile Tile all open DIME Tools windows horizontally.

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.

Using Help


Provides help on how to use the help function.

About DIME Tools

Displays an information box and copyright notice for DIME Tools.

This function can also be activated by clicking the  icon.



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 mouseclick.

3.3 BootP Server

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



Figure 5: BootP Server – Initial BRICK Configuration

If you power up your BRICK 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 BRICK is received by a PC running DIME Tools, the BootP Server Window opens a dialog box as shown in [Figure 5](#) above.

Here you can enter the most important network parameters.

BootP Configuration

BRICK Parameters: The following parameters – which will be sent to the requesting BRICK – are mandatory.

- **Name**
The host name for the BRICK, as it should be used by a DNS server, for example.
- **IP Address**
The IP address of the ethernet interface on the BRICK.

- **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 BRICK's ethernet interface (the hardware address is located on either the ethernet module or the underside of your BRICK). This address is included in the BootP requests from a BRICK. The field is automatically set to the address received.

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.

- **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 BRICK. 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 BRICK's flash.

- **Ignore boot request of this BRICK**

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.

Administry
Editor

With the Administry Editor (available from **Configuration - BootP Server**), you can specify any number of BRICKs (devices) to manage BootP. The **New**, **Edit**, and **Delete** buttons, shown in [Figure 6](#) below, allow you to define which BRICKs to manage from this PC.



Here you can also enter BRICKs 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.



Figure 6: BootP Server – Administration Editor

Security Considerations

Since the BRICK 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 BRICK. To prevent the BRICK from submitting BootP requests, ensure the BRICK can load its configuration information from its local memory (i.e. store the configuration using **SNMP – Save Configuration** from DIME Browser or `cmd=save` directly on the BRICK in the SNMP shell or save the configuration using the Setup Tool). Refer to the section on *BRICK Configuration Files* in the *Software Reference*.

3.4 DIME Tracer

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

ISDN Trace

You can start an ISDN tracer on a BRICK 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 7](#) below).

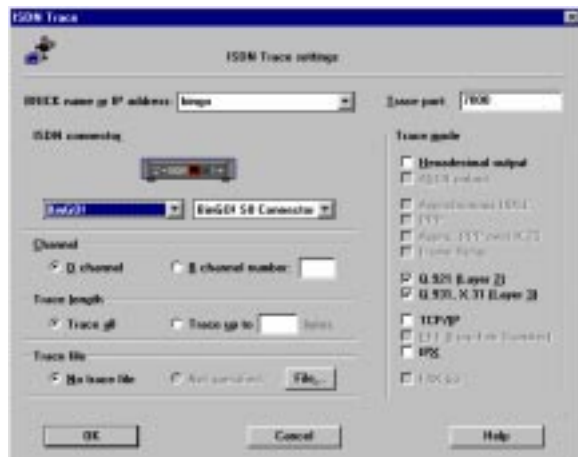


Figure 7: DIME ISDN Trace Settings

- **BRICK name or IP address**
Enter the name (e.g. bingo) or IP address (e.g. 192.168.1.1) of your BRICK.
- **Trace port**
Specifies the TCP port to use for the trace connection to the BRICK (default value: 7000). Make sure to use the same port as on your BRICK (Setup Tool: IP/Static Settings menu; SNMP shell: *adminTable*).

- **ISDN Connector**

Choose which ISDN port should be traced.



You can select the BRICK type you are using from the left listbox below the BRICK graphic. 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.

- **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.).

The options chosen here should be appropriate for the activity you are tracing (e.g. setting PPP mode and trac-

ing 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.

CAPI Trace

The CAPI Trace utility allows you to examine the CAPI messages sent to and from your BRICK. 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 BRICK 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 8](#) below).



Figure 8: CAPI Trace Settings

- **BRICK name or IP address**
Enter the name (e.g. bingo) or IP address (e.g. 192.168.1.1) of your BRICK.
- **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 BRICK (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.

3.5 TFTP Server

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

Once *TFTP Server* is configured, the BRICK can send and receive TFTP files to/from the PC. TFTP requests initiated on the BRICK 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 BRICK and your PC.

The easiest way is to use the *Configuration Management* menu of the Setup Tool on your BRICK. (You can access the BRICK via Telnet over the LAN or via a Hyperterminal, when the BRICK is attached to the serial interface of your PC.) There you have all the options available for transferring configuration files between your BRICK’s

Flash ROM and memory and a TFTP server. Other ways include issuing the appropriate command by hand from the BRICK'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 BRICK's system software. The easiest way is to issue the **update** command from the BRICK's SNMP command shell:

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

Once the image has been successfully transferred to the BRICK, 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 BRICK 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 BRICK 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 9](#) below).

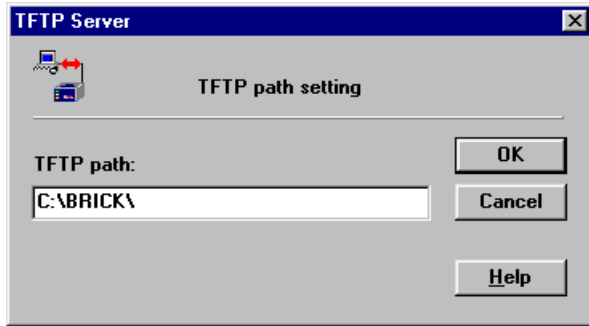


Figure 9: TFTP Server – TFTP Path Setting

The TFTP path is set to **C:\BRICK** 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 BRICK. The only requirement is that the PC is configured to be the BRICK's syslog host (either by entering the PC's IP address in the *Syslog Host* field in the BootP Server dialog – see page 21 – for this BRICK, or using DIME Browser to enter it in the *addr* field of the *biboAdmLogHostTable* in the *administration* group, or by using the **SYSTEM** → **EXTERNAL SYSTEM LOGGING** menu of Setup Tool (please refer to the section *Basic System Configuration* in your *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 BRICK has a priority level (*administration* – *biboAdmSyslogTable* – *Level*) and a subject (*administration* – *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 BRICKs, when you are receiving syslog messages from more than one BRICK.

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

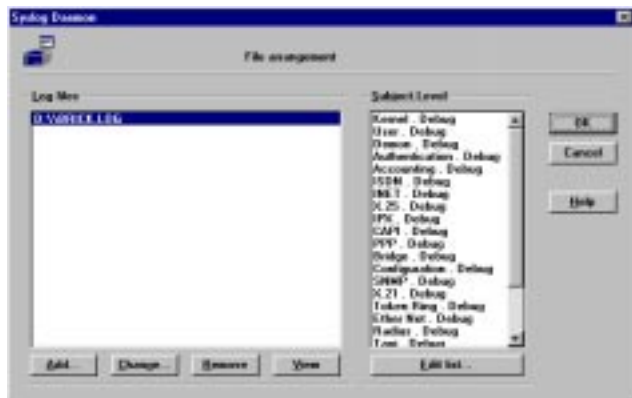


Figure 10: Syslog Daemon Configuration Dialog Box

There are five buttons at the bottom of this window:

- **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 11](#).

Subject/Priority
Combinations

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

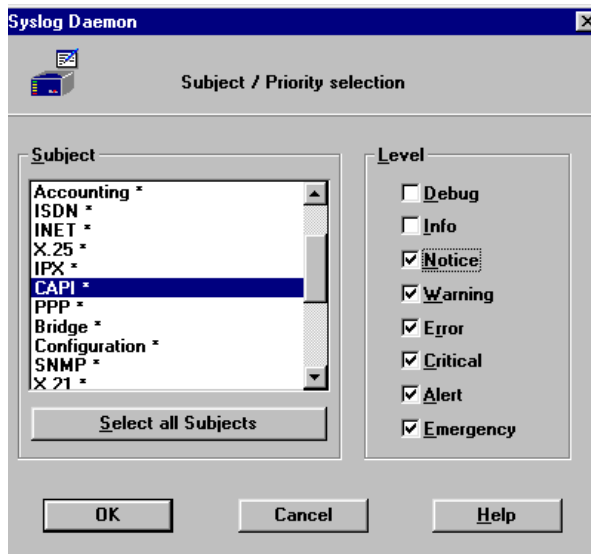


Figure 11: Syslog Daemon – Subject / Priority Selection

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 BRICK 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.

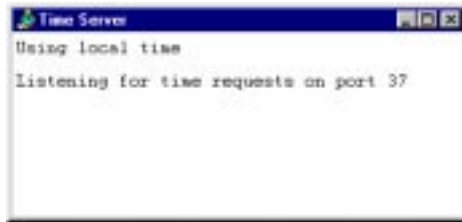


Figure 12: Time Server Window

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**.



Figure 13: 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 BRICK 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 BRICK should be set to 0.

The advantage of selecting Local Time is that the correct local time will be set, although the BRICK 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 DIME Browser

The DIME Browser is an SNMP manager, which allows you to access all SNMP tables and variables on your BRICK from a graphical user interface, thus facilitating the configuration of the BRICK.

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

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

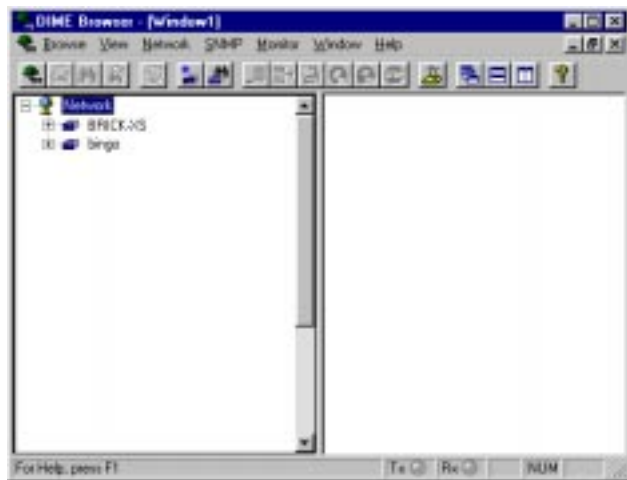


Figure 14: DIME Browser

Beneath the BRICK names (click on the “+” sign), you will find the MIB tables and variables (see [Figure 15](#) below).

When you first access a table to be modified, you are prompted for a community password of the BRICK (default passwords are *bintec* for the admin community and *public* for the write and read communities; for further information on communities, please refer to the section *Basic System Configuration* in your BRICK’s *User’s Guide*).

All editable indices of a table are displayed in **bold** print, read-only values are displayed in normal print (see [Figure 15](#) below).

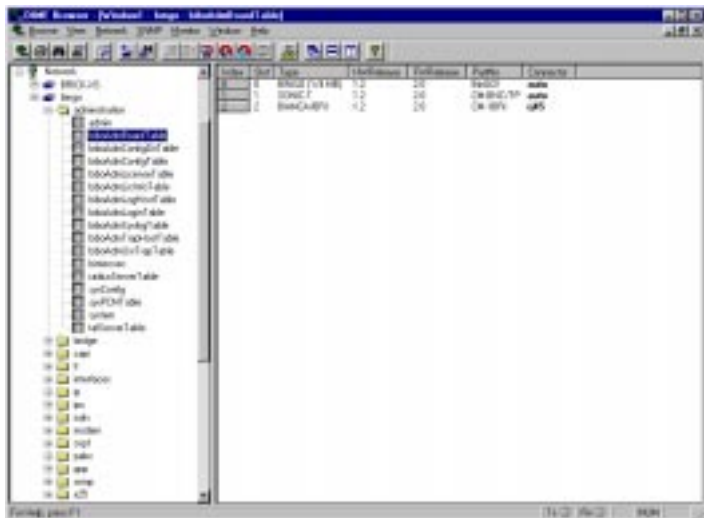


Figure 15: DIME Browser – Tables

When double-clicking an editable index, you get a dialog box in which you can enter a new value for this in-

dex. Note that most numerical values can be entered in either decimal, hexadecimal, or octal format.

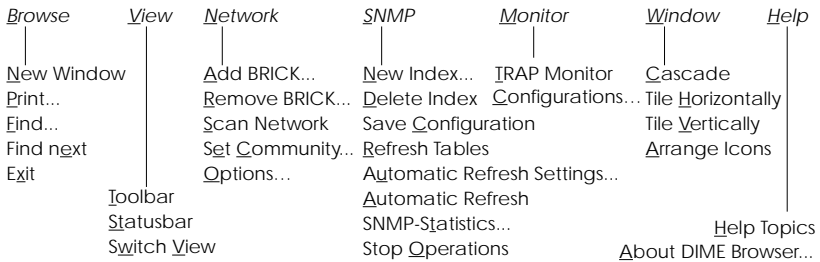
Format	Prefix	Example
Decimal	none	12
Hexadecimal	0x	0xc
Octal	0	014





For an explanation of all SNMP tables and variables please refer to your BRICK's *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 DIME Browser's context-sensitive online-help by highlighting a table name or variable name and pressing **F1**.
















4.1 Menu Structure


DIME Browser has the following 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 BRICK
	Network	Scan Network - Search for connected BRICKs
	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 BRICK
	SNMP	Refresh Tables - Update all tables
	SNMP	Automatic Refresh - Toggle automatic refresh on/off
	SNMP	Stop Operations - Cancel all current SNMP operations
	Monitor	TRAP Monitor - Enables the TRAP Monitor
	Window	Cascade - Cascades all open windows
	Window	Tile Horizontally
	Window	Tile Vertically


	Help	About DIME Browser - Displays a short copyright notice
---	------	--


The following is a short run through of all menu items:

Browse

New Opens a new Browser window.
This command can also be activated by clicking the  icon.

Print Prints the current table.
This command can also be activated by clicking the  icon.

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.


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.

Exit Leaves DIME Browser.

View

Toolbar Toggles toolbar on/off.


Statusbar
Toggles statusbar on/off.

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 BRICK; e.g. to maintain a BRICK from a remote network.


This command can also be activated by clicking the  icon.

Remove BRICK

Removes the selected BRICK from the tree.

Scan Network

Scans the local network for connected BRICKS. This function can be used to update the list of BRICKS currently online.

This command can also be activated by clicking the  icon.

Set Community


Prompts you to enter a community password to gain access to the SNMP tables of a BRICK.

Options Opens a dialog box from which you can change the IP broadcast behaviour of the BRICK 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.



Note that you can also access the commands from the SNMP menu by clicking the right mouse button inside the table part of a Browser window.


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.


Save Configuration

Stores the current contents of all tables to the BRICK 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.

Refresh Tables

Updates the contents of all tables.


This command can also be activated by clicking the  icon.

Automatic Refresh Settings

Lets you enter the settings for the automatic refresh of all tables.

Automatic Refresh

Toggles automatic refresh of all tables on/off.


This command can also be activated by clicking the  icon.

SNMP Statistics

Displays statistical data on SNMP packets received or sent by the current BRICK.

Stop Operations


Cancels all current SNMP operations. This can be useful to terminate operations for a BRICK no longer online.

This command can also be activated by clicking the  icon.

Monitor

TRAP Monitor


Enables the TRAP Monitor.

This command can also be activated by clicking the  icon.


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.

Tile Horizontally

Tiles all open Browser windows horizontally. This command can also be activated by clicking the  icon.

Tile Vertically

Tiles all open Browser windows vertically. This command can also be activated by clicking the  icon.

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

About DIME Browser

Displays a copyright notice and version information for the DIME Browser.

This command can also be activated by clicking the  icon.

4.2 Using the Keyboard

You can operate DIME Browser 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 under-

lined 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	
Ctrl-P	Print current table	
Ctrl-F3	Find ...	Browse
F3	Find next	
Alt-F4	Exit	
Ctrl-W	Switch View	View
Ctrl-A	Add BRICK	
Ctrl-Del	Remove BRICK	Network
Ctrl-Alt-S	Scan Network	
Ctrl-E	Set Community	
Ctrl-I	New Index	
Ctrl-Alt-I	Delete Index	
Ctrl-S	Save Configuration	SNMP
Ctrl-R	Refresh Tables	

Shortcut	Function	Menu
Ctrl-O	Stop Operations	

The shortcuts are also displayed next to the appropriate menu item.

4.3 TRAP Monitor

SNMP traps are sent by the BRICK 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 authenticationFailure”. Enterprise specific traps can be defined in the *biboAdmUsrTrapTable* on the BRICK 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 BRICK’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 DIME Browser 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 BRICK. The TRAP Monitor must be enabled.



Figure 16: 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

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 BRICK). The CAPI Server allows CAPI applications running on different hosts (on the local network) to simultaneously access the ISDN interfaces of the BRICK.

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*), and the “hidden application” *CAPI2WSA*. For Windows NT 4.0 and higher, a special CAPI 2.0 library (*CAPI2032.DLL*) is provided, which supports the Remote Multi CAPI (see [Remote Multi CAPI Client](#) on page 55).

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 Windows 3.1, Windows 95/98 and Windows NT 3.51 and higher providing an interface for 16-bit CAPI 1.1 and CAPI 2.0 applications respectively.

CAPI2032.DLL

Dynamic link library for Windows 95/98 and Windows NT 3.51 and higher, providing an interface for 32-bit CAPI 2.0 applications.

For Windows NT 4.0 and higher, this dynamic link library supports the Remote Multi CAPI (see [Remote Multi CAPI Client](#) on page 55).

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 BRICK.

CAPIVIEW.EXE

Remote CAPI Configuration program for 16-bit CAPI 1.1 and 2.0 under Windows 3.1. For a description of this application, please refer to page [49](#).

Remote Clients Configuration program

Windows 95/98 and NT 3.51 and higher, a configuration tool for CAPI and TAPI. For a description of this application (Rxc_cfg.exe), please refer to page [51](#).

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 BRICK. The TAPI Server allows TAPI applications running on your PC access to the POTS interfaces¹ of your BRICK. TAPI is available on the products BinGO! Plus/Professional and V!CAS.

1. Please note that POTS interfaces are only available with the BinGO! Plus / BinGO! Professional and V!CAS teleworking routers.

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

Each PC that you intend to run TAPI telephony applications from should have the following files present:

RTC_SPI.TSP

Telephony Service Provider for Windows 95/98, providing an interface for TAPI 1.4 applications.

RTC32.TSP

Telephony Service Provider for Windows NT 4.0, providing an interface for TAPI 2.0 applications.

Remote Clients Configuration program

For a description of this application, please refer to page [51](#).

5.3 Remote CAPI Configuration under Windows 3.1

On Windows 3.1 systems the **Remote CAPI Configuration / 16-bit** program can be used to set up a BRICK as a CAPI Server for running remote 16-bit CAPI applications or to view the activity of CAPI applications. After starting the program, the Remote CAPI Configuration dialog box is displayed, as shown in [Figure 17](#) below.



Figure 17: Remote CAPI Configuration / 16 bit – Main Window



Please note that Windows 3.1 systems are not capable of storing CAPI user and password data. The 16-bit CAPI for Windows 3.1 will always try to use the **default** user with no password. Make sure that the **default** user is configured on your BRICK (in the [PABX][User] menu of Set-up Tool) if you want to use its CAPI features from your Windows 3.1 system.

- **BRICK settings**

Enter the BRICK's IP address (or host name) here. The CAPI port to which remote CAPI applications should be connected can remain at its default value (2662), unless you changed this parameter in the **admin** table of the BRICK (*biboAdmCapiTcpPort*).

The status line in this section shows the CAPI status based on its current settings. Note that the status may change to “CAPI is NOT ready” if the remote CAPI server is detected as not active.

- **Registered CAPI application IDs**
This section shows a list of all registered CAPI application IDs.
- **CAPI viewer**
When the viewer is turned on, CAPI messages are displayed. Normally, the CAPI viewer is turned off. Since turning on the viewer may slow down data throughput of the CAPI client on slower systems, it is recommended that the viewer only be turned on when you need to verify messages for specific CAPI IDs.

5.4 CAPI and/or TAPI Configuration

On Windows 95/98 and NT 3.51 and later systems, the **Remote Clients Configuration** program can be used to enter a BRICK 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 18](#) 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 BinGO! Plus/Professional and VICAS. All other BRICKs only run a CAPI Server

- **BRICK IP address or host name**
Enter the BRICK's IP address or host name here. You can use the listbox to choose from the BRICKs 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. Make sure to use the same ports as on your BRICK



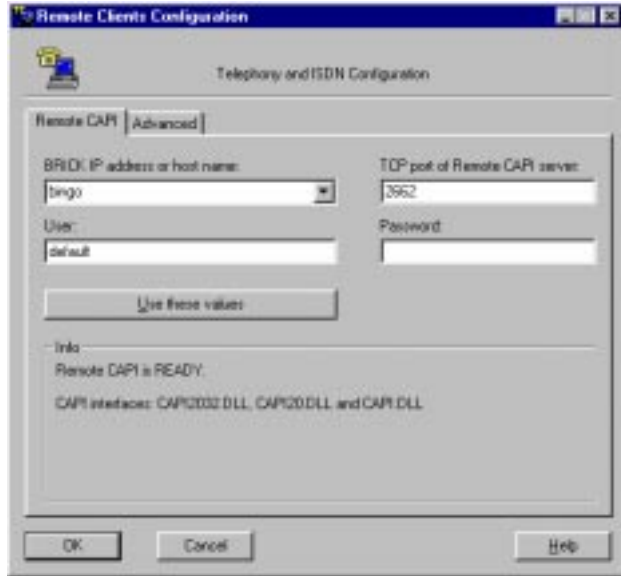


Figure 18: Remote Clients Configuration

(Setup Tool: `[IP][Static Settings]` for the CAPI port, `[PABX][Static Settings]` for the TAPI port; SNMP shell: **admin** table for both ports).

You should only change these values if—for some reason—these TCP ports are already being used for other purposes on your PC.

- **User**

In this field you can enter the user who is authorized to use the CAPI (or TAPI) features of this BRICK. 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 BRICK in the `[CAPI][User]` menu (or `[PABX][User]` menu) of Setup Tool.

On the BRICK 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 BRICK (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 BRICK 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 ‘mybrick’, port 2662”.

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

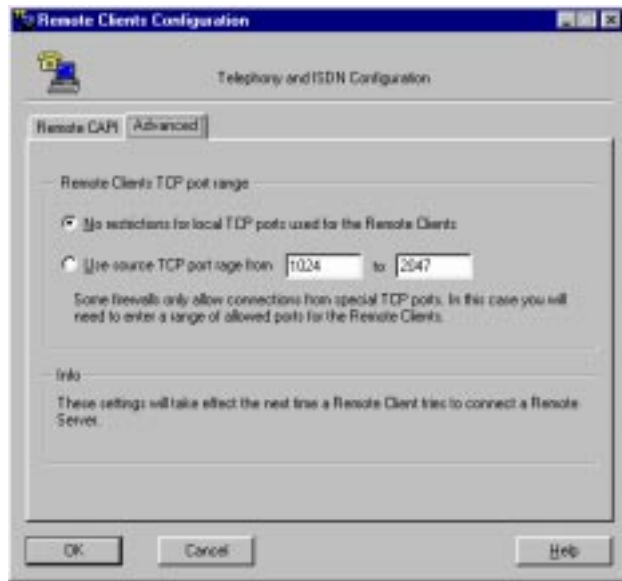


Figure 19: Source TCP port range settings

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.

6 Remote Multi CAPI Client

6.1 What is it?

The Remote Multi CAPI Client (RMCC), an enhanced 32-bit CAPI (capi2032.dll), enables you to use multiple BRICKs for CAPI 2.0 connections from one PC running Windows NT 4.0. The RMCC allows your CAPI 2.0 applications to take advantage of all ISDN controllers available through one or more BRICKs 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.

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

6.2 Installation

If you have Windows NT 4.0 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 BRICK at a time.

6.3 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 above in section [CAPI and/or TAPI Configuration](#). The BRICK 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.

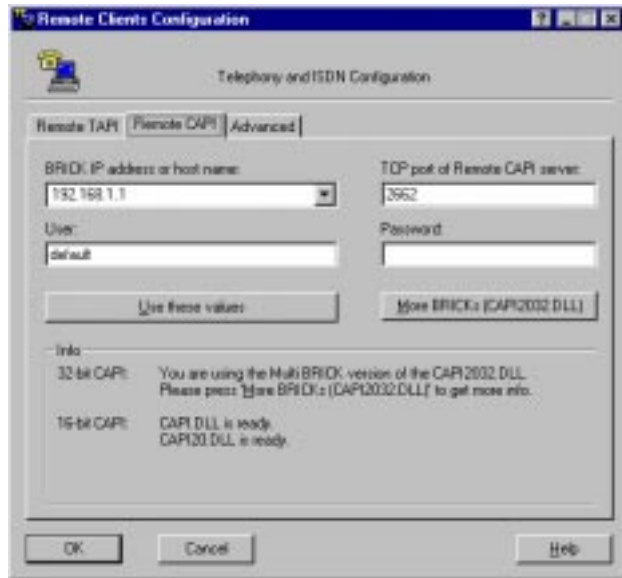


Figure 20: Remote Clients Configuration—CAPI page

More BRICKs

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

You will then get a list of all BRICKs currently configured and their controllers which will be available for 32-bit CAPI 2.0 applications (see [Figure 21](#)).

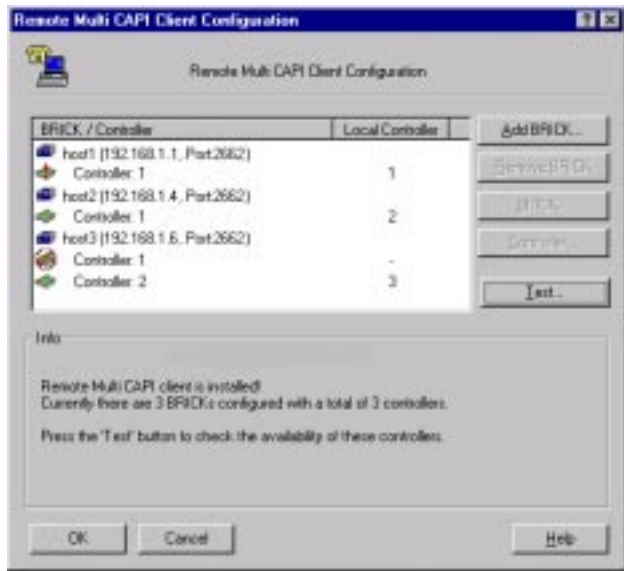


Figure 21: Remote Multi CAPI Configuration—More BRICKs

The list will initially be empty (unless you have already configured a BRICK on the main CAPI page, see [Figure 20](#) above).

If you select a BRICK from this list, the Info field in the lower half of the dialog box will display the number of controllers available on this BRICK, 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 BRICKs* dialog have the following meanings.

Add BRICK

To add a BRICK click the *Add BRICK* button. Enter its host name or IP address, its CAPI TCP port, the User name and Password (see explanation of User and Password on page [52](#) above) in the appropriate fields. When you click the *OK* button to confirm your entries, the application will try to establish a connection to the BRICK, verify the given User and Password entries, and retrieve information on the number of controllers available on this BRICK and on its system software release and serial number.

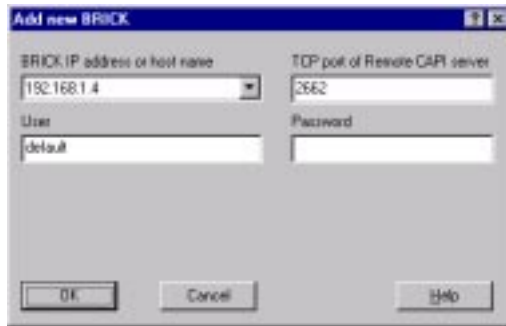


Figure 22: Add BRICK

This may take a couple of seconds. If the connection fails, make sure the BRICK 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 BRICK 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 BRICK or disable a controller, the remaining controllers are automatically renumbered.

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

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

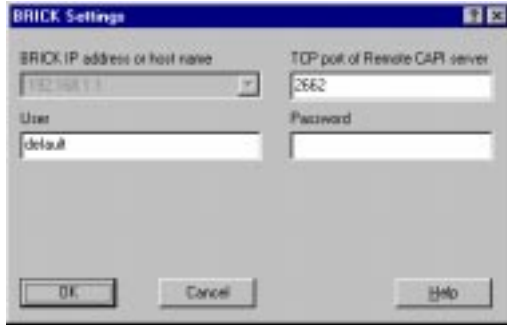


Figure 23: BRICK Settings

Here you can change the CAPI TCP port, User and Password settings for this BRICK. When you click the OK button the application will try to establish a connection to the BRICK. See section [Add BRICK](#) 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.

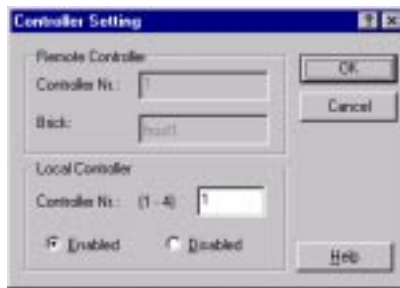


Figure 24: Configure Controller

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 BRICKs 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.



Figure 25: 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 BRICKs and controllers (see [Figure 21](#)).

7 BRICK at COM1/COM2

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

You can use these programs to configure and administer your BRICK 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 BRICK. Along with this license you will get 10 *TAF Login* licenses for PCs you wish to use as TAF clients.

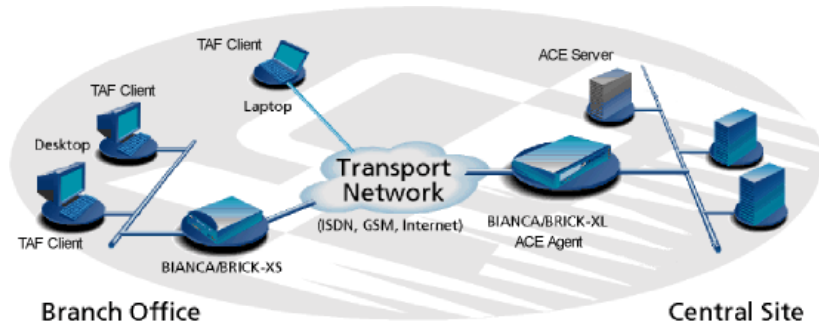


Figure 26: TAF Clients, ACE Agent and ACE Server

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

- an ACE/Agent by BinTec (BRICK-XL2, BRICK-XM with 2 MB flash or BRICK-XMP) 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 (Windows 3.1, Windows 95/98 and Windows NT)

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 BRICK 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 27: Token Card

TAF, on the whole, and all its configuration steps are described in detail in BinTec's Extended Feature Reference Guide, which can be retrieved from BinTec's file server (Section: FTP Server) 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 BRICK's (ACE/Agent of the central site LAN) **IP address** in this dialog box and can modify the **Listen Port**, if necessary (the listen port setting on the PC must be identical to the setting on the BRICK). Above that you must enter

the program's license key for the TAF client, which is provided together with your BRICK's TAF license.

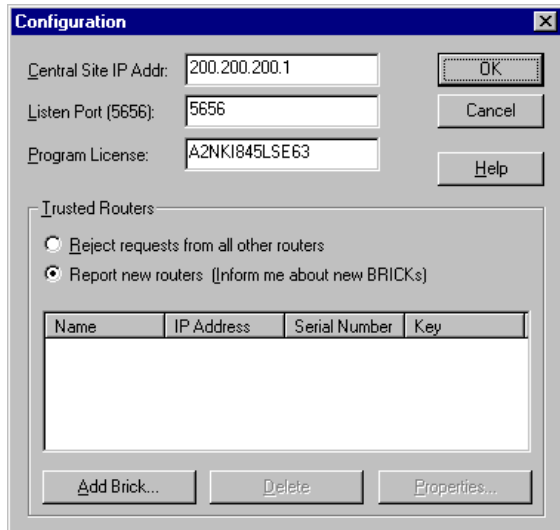


Figure 28: TAF Configuration

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.

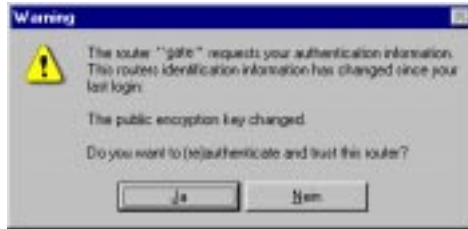


Figure 29: Notification about the login request of a router not contained in the trusted routers list

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.

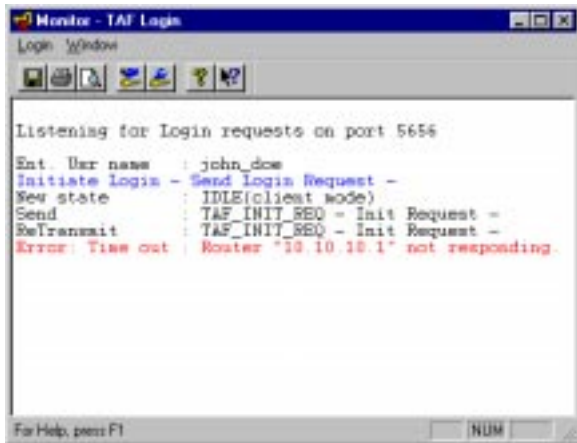


Figure 30: TAF Login

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**.

The image shows a Windows-style window titled "Monitor - TAF Login". The window has a standard title bar with minimize, maximize, and close buttons. Below the title bar is a menu bar with "Login Window" and a toolbar with several icons. The main area of the window contains a text-based log of network activity. The log starts with "Listening for Login requests on port 5656". It then shows a sequence of events: "Ent. User name : john_doe", "Initiate Login - Send Login Request -", "New state : IDLE(client mode)", "Send : TAF_INIT_SEQ - Init Request -", and "ReTransmit : TAF_INIT_SEQ - Init Request -". The final line of the log is "Error: Time out Router '10.10.10.1' not responding.", where "Error:" and "not responding." are highlighted in red. At the bottom of the window, there is a status bar with "For Help, press F1" on the left and a "NUM" button on the right.

```
Monitor - TAF Login
Login Window
Listening for Login requests on port 5656
Ent. User name : john_doe
Initiate Login - Send Login Request -
New state : IDLE(client mode)
Send : TAF_INIT_SEQ - Init Request -
ReTransmit : TAF_INIT_SEQ - Init Request -
Error: Time out Router '10.10.10.1' not responding.
For Help, press F1 NUM
```

Figure 31: 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 Java Status Monitor

The Java Status Monitor has been developed by BinTec to let you monitor your BRICK dynamically via a Web Browser.

Access to a BRICK's Status Monitor is secured by a password and the information displayed is read-only.

Information available using the Java Status Monitor covers the following items, which are described in detail later on:

- static information like BRICK name, software version, location.
- traffic information for all interfaces
- information about connections to the respective WAN partners
- information on communication and feature modules installed on your BRICK

The Java Status Monitor needs a Java-enabled Web Browser, i.e. Netscape Modzilla or Microsoft Internet Explorer. It requires Modzilla (Netscape) version 2.0, 3.0 or 4.0 (tested under Windows 95/98, Windows NT 4.0 and Solaris 2.5/2.6) or Microsoft Internet Explorer version 3.0 or 4.0 (tested under Windows 95/98 and Windows NT 4.0). When you start the Java Status Monitor from the Start/Programs folder it will be opened with your default Web Browser.

The 4.0 versions of both Browsers comprise security restrictions to ensure that Java applets have not been manipulated. In compliance with these requirements, BinTec's Java applets are signed using a certificate ("digital ID") issued by the company VeriSign Inc., which verifies the integrity of the application by means of checksum and encryption. The security restrictions mentioned pro-

duce an alert message when starting the Java Status Monitor for the first time, to notify you that the application is accessing your BRICK over the LAN/IP. The Java applet establishes a connection to your BRICK, where it is only allowed to read out values. It does not contact or influence your local system or any other system.

9.1 Structure of the Java Status Monitor

The Java Status Monitor is divided up into different panels, which can be accessed via tabs.

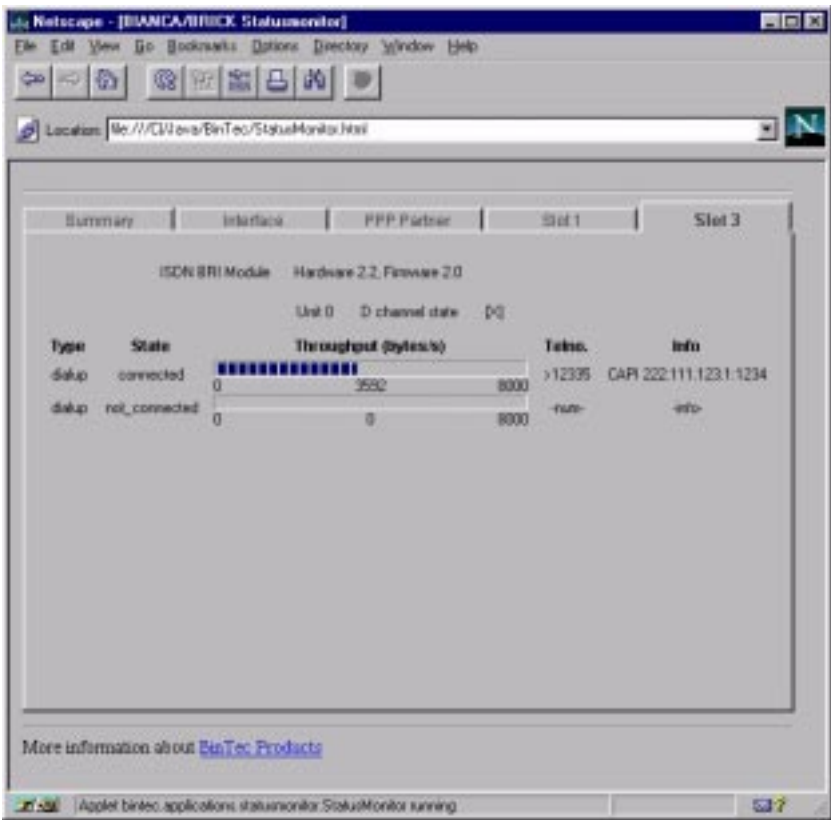


Figure 32: Java Status Monitor

Three tabs/panels are always available: **Summary**, **Interface** and **PPP Partner**. Additionally, there are panels for each slot of your BRICK where a communication or feature module is installed. (In the following description of the panels, variable names in parenthesis denote the corresponding SNMP variables).

Summary Panel

The summary panel contains mainly static information about the BRICK, which is presented under the following items.

- **Address**
The host name or IP address of the BRICK.
- **Type**
Describes the product type of the BRICK, e.g. BI-ANCA/BRICK-XM or BinGO!. (*sysDescr*)
- **Name**
The name assigned to the BRICK. (*sysName*)
- **Version**
The system software version/release. (*sysAdmSWVersion*)
- **Contact**
Information about the contact person, responsible for managing this BRICK, e.g. e-mail address. (*sysContact*)
- **Location**
Location of the BRICK. (*sysLocation*)
- **Uptime**
The time elapsed since the last reboot of the BRICK in the following format: days HH:MM:SS.hh (HH=hours; MM=minutes; SS=seconds; hh=hundredth of a second). This value is updated every two seconds. (*sysUpTime*)

Interface Panel

Interfaces from the BRICK's *ifTable* are displayed on the interface panel. You are informed about all interfaces which are not local (like *LOCAL*, *REFUSE*) and which are up (the variable *ifAdminStatus* in the *ifTable* has the value *up*).

On the left, you can see the interface's name and next to it a throughput display with the minimum display noted on the left edge (in bytes/s). The maximum throughput possible is on the right edge of the display. In the middle of the throughput display the current throughput (in bytes/s) is stated. This value is given as an average. The calculation of the current throughput is updated every two seconds.

From the throughput display, you can see the average current throughput, in relation to the maximum value, represented by a blue bar.

The values given in this panel are updated every two seconds.

PPP Partner Panel

In the PPP partner panel all interfaces for WAN partner connections are listed. This list comprises all WAN partner interfaces from the BRICK's *ifTable* with the interface type being *PPP*.

The respective information is updated every two seconds and contains the following items:

- **Interface**
Interface number from the *ifTable*. (*ifIndex*)
- **State**
The current state of the PPP partner connection can be, for example, *idle*, *incoming*, or *outgoing*. (*bi-boPPPConnState*)

- **Partner**
The partner name, as entered in the Setup Tool's WAN Partner menu. (*ifDescr*).
- **Speed**
The maximum speed that can be reached on this connection. The unit used for the maximum speed is kbit/s.
This value considers multiple B-channels, when channel bundling is enabled. (*ifSpeed*)
- **Throughput**
Here you find a throughput display that shows the current throughput for the partner connection, which is taken from the variable *biboPPPTthroughput* in the *biboPPPStatTable*.
Note that the throughput is given in units of bytes/s. A maximum speed of 64000 kbits/s results in a maximum throughput of 8000 bytes/s. (*biboPPPTthroughput*)
Note that due to data compression and rounding errors, the current throughput may exceed the physical line throughput. In these cases, the throughput display scales to the new maximum value automatically.
- **Duration**
The duration of the current connection on this interface in seconds. The value corresponds to the variable *biboPPPConnDuration*.
- **Charging**
Here the charging units for all B-channels used for the current connection are counted. (*biboPPPConnUnits*)

Panels for the Different Slots

The numbered slots contain information about the respective modules installed in these slots.

The information provided differs depending on the module installed. The modules are divided up into ISDN/BRI modules, ISDN/PRI modules, LAN/WAN modules and Function Modules for more detailed description.

Here also, information is updated every two seconds.

- **ISDN/BRI Modules**

On top of the panel, you find the hardware and firmware version of the BRI module followed by the **Unit** number and **D-channel state**. The units are numbered starting with “0”. Each unit represents an S_0 interface with two B-channels. When the D-channel is active it is marked “[X]”, when it’s not active it is marked “[_]”. (*isdnIfLayer1State*)

Below that there is a line of information for each B-channel:

Type can be “dialup” for an ISDN dialup line or “leased” line, if the channel is configured as a leased line. **State** is taken from the *isdnChState* variable and can be “connected” if the channel is currently in use or otherwise “not_connected”. If the B-channel is part of a bundle, the bundle number is appended to the channel type, e.g. “dialup B1” if the channel belongs to bundle 1.

The throughput display shows the minimum throughput, the average current throughput and the maximum possible throughput (values from left to right) for the respective B-channel, where the current throughput is also represented by the blue bar. The current throughput value corresponds either to the value of the variable *isdnChReceivedOctets* or *isdnChTransmitOctets*, in each case depending on which variable contains the highest value.

On the right side of the display, the item **Telno.** shows the caller's telephone number for an incoming call (e.g. <1234) or the called number for an outgoing call (e.g. >1234). The number corresponds respectively to *isdnCallRemoteNumber* and the type of call to *isdnCallType*. Finally, under **Info** you find information about the kind of call. You are informed whether the call is e.g. a CAPI call or an isdnlogin. (*isdnCallInfo*)

- **ISDN/PRI Modules**

Slots that contain PRI modules bear information about all 30 B-channels and the D-channel of the S_{2M} connection.

At the top of the panel, the **State** of the D-channel, which is taken from the variable *pmxIfLayer1State*, is shown. Typical values are *active* or *no_signal*.

At the bottom and numbered from 0 to 32, the B-channels are listed in two columns. (In this display the channel numbers 0 and 16 are reserved.) Each channel is described with 5 items, which are:

- **Active**
“_” is not active and “X” is active/connected. (*isdnCHState*)
- **#**
The channel number. (*isdnChNumber*)
- **Type**
Type can be “dialup”, “leased_dte” or “leased_dce”. (*isdnChType*)
- **Rem. No.**
The remote telephone number, preceded by “<” for incoming calls and “>” for outgoing calls. (*isdnCallType*, *isdnCallRemoteNumber*)
- **Info**
Information about the kind of call. (*isdnCallInfo*)
- **LAN/WAN Modules**

On panels for slots containing LAN or WAN modules, only the interfaces using the respective module are listed. The interfaces in turn can be looked up on the **Interface** panel.

- **Feature Modules**

The panels for feature modules (FM-STAC and FM-8MOD) only contain information about hardware, logic and firmware version of the module.

9.2 Customizing the Java Status Monitor

The startup of the Java Status Monitor can be customized by editing the file “statmon.htm”, which you can find in the BRICK folder (the Java Status monitor was installed together with the BRICKware). This makes sense, when you are always watching the same BRICK via the Status Monitor.

This file contains three entries for parameters, which are read out at the start of the Status Monitor:

```
<PARAM NAME="*brickaddress"   VALUE=" ">
<PARAM NAME="user"           VALUE="http">
<PARAM NAME="password"       VALUE="bintec">
```

The parameter “*brick address” can be adjusted to the BRICK’s IP address or its assigned name in the quotation marks of the VALUE variable. Additionally, you must delete the asterisks in front of “brickaddress”, so that the Java applet can recognize this parameter.

The parameter “user” must keep the value “http”, because that’s the name of the user who has access to HTTP information, it cannot be changed.



The parameter “password” contains the default password for the user “http” as it is predefined on the BRICK. For security reasons, this password must be changed from its default on the BRICK (via the Configuration Wizard, Setup Tool or the *bintecsectable:biboAdmHttpPassword*) and similarly, we do not recommend entering your password in this HTML file.

When you have customized the file “statusmon.htm” by specifying your BRICK’s IP address, the Status Monitor automatically connects to your BRICK at every start-up and you can access it by manually entering your secret password.

Tip for Netscape Users

Finally a hint for users who open the Java Status Monitor using Netscape:

You can restart the Java Status Monitor (e.g. to enter a new BRICK name or IP address) by pressing SHIFT and at the same time clicking the **Reload** button.

For more detailed information on the Java Status Monitor and, free of charge, the Java source code, have a look at BinTec’s Website at <http://www.bintec.de/ftp/status-mon/>.