

LAN-Admin

Configuration Software for
Network DAQ System LAN-AD16fx

User Manual

Version 4.6

▶ www.bmcm.de

bavarian measurement company munich



CONTENTS

1 OVERVIEW	5
1.1 INTRODUCTION	5
1.2 BMC MESSSYSTEME GMBH	6
1.3 COPYRIGHTS	7
1.4 QUICKSTART	8
2 INSTALLATION AND START	10
2.1 SYSTEM REQUIREMENTS	10
2.2 INSTALLATION OF LAN-ADMIN	10
2.3 CONNECTING THE DEVICE	13
2.4 STARTING THE PROGRAM	14
3 DEVICE CONFIGURATION	15
3.1 OPERATING THE SOFTWARE	15
3.1.1 SELECT DEVICE	16
3.1.2 CHANGE SETTINGS	17
3.2 TCP/IP	18
3.2.1 EXCURSUS: BASICS OF TCP/IP	18
3.2.1.1 4-LAYER SYSTEM	19
3.2.1.1.1 NETWORK LAYER	19
3.2.1.1.2 INTERNET LAYER	20
3.2.1.1.3 TRANSPORT LAYER	20
3.2.1.1.4 APPLICATION LAYER	20
3.2.1.2 SENDING DATA VIA NETWORK	21
3.2.1.3 IP ADDRESS	22
3.2.1.3.1 NOTATION	22
3.2.1.3.2 NETWORK ID AND HOST ID	22
3.2.1.3.3 SPECIAL CASES	23
3.2.1.4 NETWORK CLASSES	23
3.2.1.4.1 CLASS A	23
3.2.1.4.2 CLASS B	24
3.2.1.4.3 CLASS C	24

CONTENTS

3.2.1.4.4	OTHER CLASSES	25
3.2.1.4.5	SUMMARY	25
3.2.1.5	SUBNETTING, SUPERNETTING	26
3.2.1.5.1	SUBNET MASK	26
3.2.1.5.2	SUBNETTING	26
3.2.1.5.3	SUPERNETTING	27
3.2.1.5.4	IDENTIFICATION OF NETWORK ID AND HOST ID	28
3.2.1.6	PRIVATE IP ADDRESSES	28
3.2.1.7	USEFUL COMMANDS	29
3.3	DEVICE SETTINGS	30
3.3.1	TAB "TCP/IP"	30
3.3.2	TAB "NTP"	32
3.3.3	TAB "ETHERNET"	33
3.4	DEVICE TESTS	34
3.4.1	CONNECTION TEST	34
3.4.2	DEVICE STATISTICS	36
3.5	TIME-SYNCHRONOUS SAMPLING	37
3.5.1	CHECK TIME-SYNCHRONOUS SAMPLING	39
3.6	UPDATE FIRMWARE	40
4	GLOSSARY	42
5	INDEX	46

1 OVERVIEW

1.1 INTRODUCTION



Fig. 1

The software **LAN-AD16f Administration Utility** is a program for the installation, configuration, and examination of the LAN data acquisition systems LAN-AD16fx(x) and AMS42/84-LAN16fx(x) of BMC Messsysteme GmbH. The devices of the LAN series are network data acquisition systems connected via Ethernet basing on the TCP/IP protocol.

To clearly identify the DAQ systems as hosts of a certain network, it is necessary to assign a unique IP address to each device according to the rules of the TCP/IP standard. All connected LAN devices are listed with their currently set IP address and serial number in the **LAN-AD16f Administration Utility**. Here the IP address can also be configured manually.

As intelligent DAQ systems, the LAN devices use their own operating system. New versions of the internal software (firmware) in the hardware can easily be updated with the **LAN-AD16f Administration Utility**.

In addition, several **device tests** allow examining the functional efficiency.



A firewall software installed on the PC might interfere with the operation of the LAN device. In this case, please contact your network administrator.

1.2 BMC MESSSYSTEME GMBH



BMC Messsysteme GmbH stands for innovative measuring technology made in Germany. We provide all components required for the measuring chain, from sensor to software.

Our hardware and software components are perfectly tuned with each other to produce an extremely user-friendly integrated system. We put great emphasis on observing current industrial standards, which facilitate the interaction of many components.

Products by BMC Messsysteme are applied in industrial large-scale enterprises, in research and development, and in private applications. We produce in compliance with ISO-9000-standards because standards and reliability are of paramount importance to us - for your profit and success.

Please visit us on the web (<http://www.bmcm.de>) for detailed information and latest news.

► ***www.bmcm.de***
bavarian measurement company munich

1.3 COPYRIGHTS

The software **LAN-AD16f Administration Utility** has been developed and tested with utmost care. BMC Messsysteme GmbH does not provide any guarantee in respect of this manual, the hardware and software described in it, its quality, its performance or fitness for a particular purpose. BMC Messsysteme GmbH is not liable in any case for direct or indirect damages or consequential damages, which may arise from improper operation or any faults whatsoever of the system. The system is subject to changes and alterations which serve the purpose of technical improvement.

The software **LAN-AD16f Administration Utility**, the manual provided with it, and all names, brands, pictures, other expressions, and symbols are protected by law as well as by national and international contracts. The rights established therefrom, in particular those for translation, reprint, extraction of depictions, broadcasting, photomechanical or similar way of reproduction - no matter if used in part or in whole - are reserved. Reproduction of the programs and the manual as well as passing them on to others is not permitted. Illegal use or other legal impairment will be prosecuted by criminal and civil law and may lead to severe sanctions.

Copyright © 2014

Updated: 09/20/2014

BMC Messsysteme GmbH

Hauptstrasse 21
82216 Maisach
GERMANY

Phone: +49 8141/404180-1

Fax: +49 8141/404180-9

E-mail: info@bmcm.de

1.4 QUICKSTART

➤ **Installation:**

- Insert the "Software Collection" CD into your CD-ROM drive and open the file **openhtml.exe** if the AutoPlay function is not active.
- First click the category "Products" and then your DAQ system (LAN-AD16fx, AMS42-LAN16fx, or AMS84-LAN16fx)" listed beneath the "LAN" interface.
- To start the installation, choose the entry "LAN-Admin" in the section "LAN-AD16f Administration Utility" on the product page of the LAN devices.
- The installation can be opened directly. If your browser does not allow this, please first save the file **install-lanadmin.exe** to hard disk and then start the installation by clicking on it.
- Follow the instructions of the installation wizard and enter the program group and directory where the **LAN-AD16f Administration Utility** is to be stored.

➤ **Operation:**

- Connect the LAN device to power (add. switch on AMS device!), and provide a **TCP/IP** connection between the PC and the LAN data acquisition system.
- Start the LAN configuration software via the program group or the directory defined during installation.
- All properly connected LAN data acquisition systems are listed with their serial number in the window on the left.
- Click a LAN device to view its specific configuration on the right. To modify **Device settings**, press the "Options" button.
- The program is closed by choosing the command "Exit" of the "File" menu.

➤ **Manual network settings:**

- When connecting to a network, a Link-local IP address will be assigned to the device. However, the IP address can also be configured manually in the "Device settings" dialog (button "Options / tab "TCP/IP"). Only assign an IP address that is still available, free, and unique in the network.
- Example: Use the following configuration if there is only the PC and one DAQ system in your network (network number 192.168.32.0):

```
IP address of the PC:           192.168.32.1
IP address of the LAN device:  192.168.32.2
Netmask:                       255.255.255.0
```

The IP address of the PC is shown in the title bar of the LAN configuration software and can be changed in the dialog "Local Area Connection" under "Properties" ("Control panel / Network and Dial-up Connections").

➤ **Miscellaneous:**

- Other parameters (e.g. NTP server connection, transmission settings) can also be configured in the "Device settings" dialog.
- The menu item "Device" includes items for a connection test and to scan device data ("device statistics") as well as the command to update the internal device software (firmware).



- **A firewall software installed on the PC might interfere with the operation of the LAN device. In this case, please contact your network administrator.**
 - **Any changes concerning the automatic network settings should only be done by a network administrator.**
-

2 INSTALLATION AND START

2.1 SYSTEM REQUIREMENTS

- PC with Windows® XP/7/8
- Network card (Ethernet) with TCP/IPv4

2.2 INSTALLATION OF LAN-ADMIN

The software **LAN-AD16f Administration Utility** to configure the LAN-AD16fx or AMS42/84-LAN16fx is located on the "Software Collection" CD from **BMC Messsysteme GmbH** included with delivery.

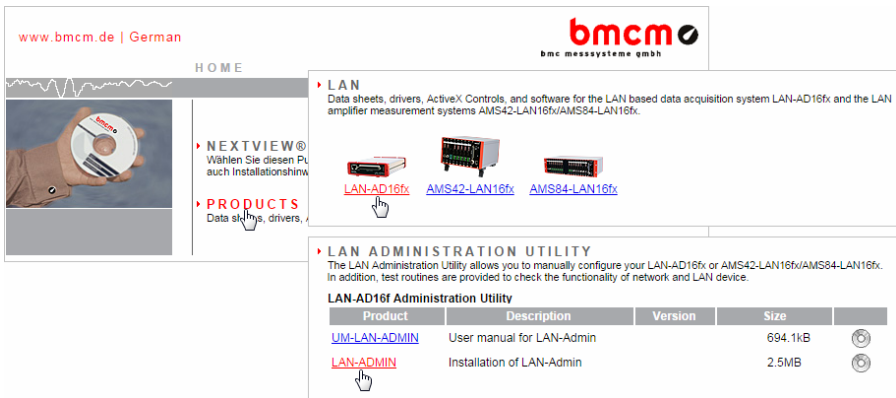


Fig. 2

When inserting the CD, a CD starter automatically opens (manually: **openhTML.exe**). Click the "Products" item and select your DAQ system LAN-AD16fx or AMS42/84-LAN16fx beneath the "LAN" product group. Start the installation by opening the entry "LAN Admin" in the section "LAN Administration Utility".

If using the CD starter in HTML format, you can decide to directly open the installation program or to save it to disk. Both options are possible.

Some browsers require saving the installation program to hard disk before. In this case, you must explicitly start the installation program **install-lanadmin.exe** after copying.

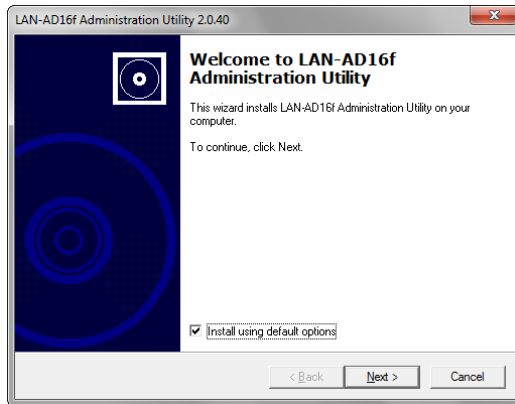


Fig. 3

An installation wizard will guide you through the installation step by step. The button "Next" will lead you to the next dialog box, with "Back" you go one step backwards. The installation can always be stopped early without saving anything by pressing "Cancel".

If you do not want to use default settings, you can uncheck this option in the first window of the installation program and decide where to install the **LAN-AD16f Administration Utility**.

Of course, the suggested program group "LAN-AD16f Administration Utility", from where you can reach the software in the Windows[®] start menu, as well as the default directory path can be modified as desired.

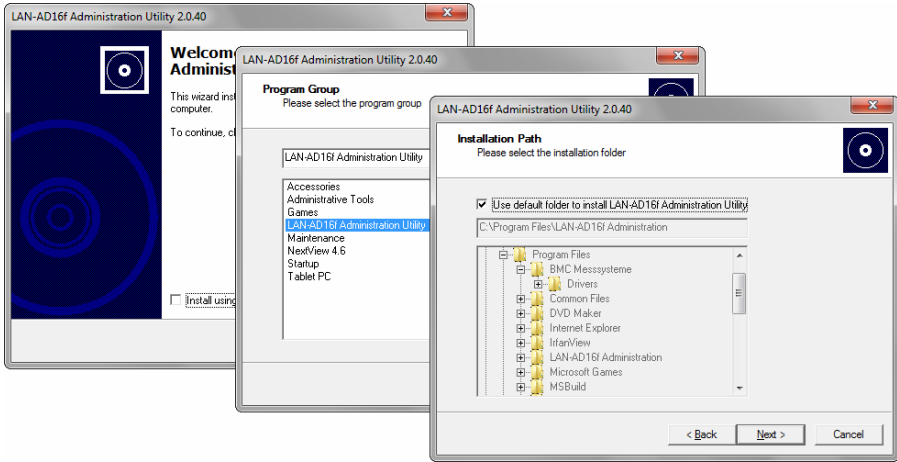


Fig. 4

To switch to another installation directory, uncheck the checkbox for to activate the boxes below.

After verifying if enough disk space is available, the installation process is started and the required files are copied into the selected folder.

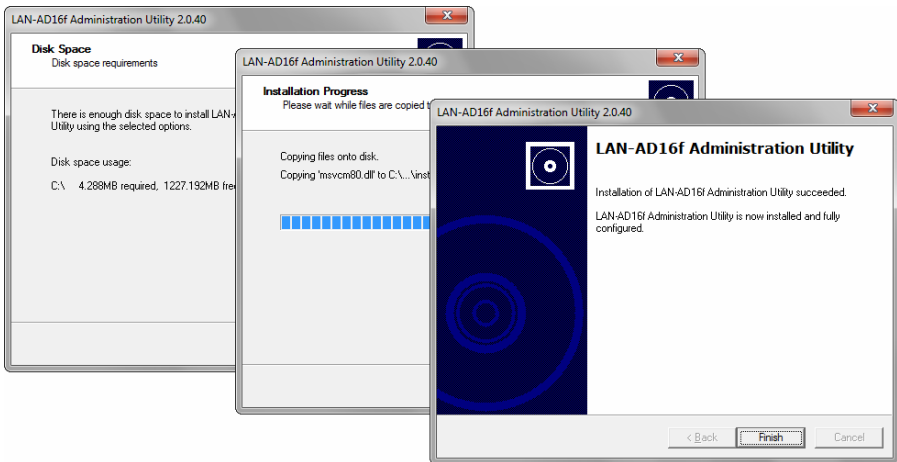


Fig. 5

2.3 CONNECTING THE DEVICE

Connect your LAN device to power supply (3-pole DIN connector) and network (Twisted Pair connector). The connectors are located on the front and back side of the LAN-AD16fx and on the front panel of the AMS42/84-LAN16fx. See the data sheet of the LAN-AD16fx or AMS42/84-LAN16fx for further details.



Power supply and network connection are essential to show the LAN device in LAN Admin!

2.4 STARTING THE PROGRAM

After installation of the software, the new entry "LAN-AD16f Administration Utility" has been added to the Windows® Start menu (see "Installation of LAN-Admin", p. 10) or to the Windows® 8 start screen, and to the respective directory.

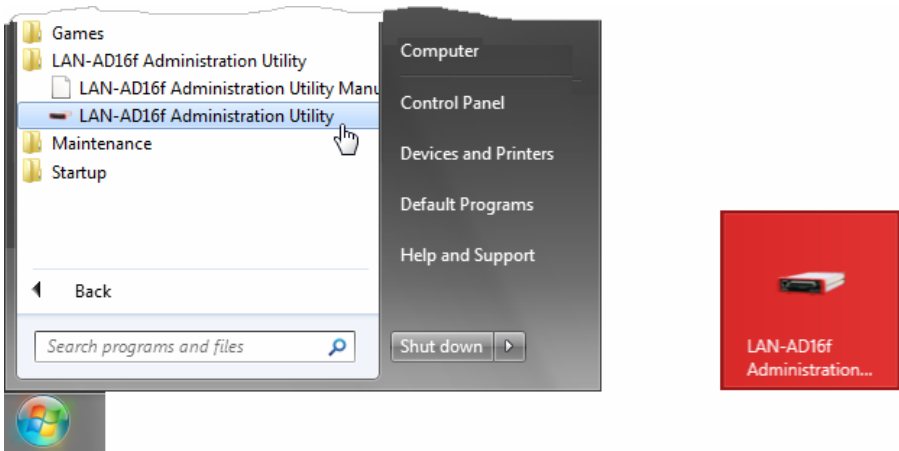


Fig. 6

Select this item to open the configuration software **LAN-AD16f Administration Utility**. All connected LAN data acquisition systems are listed with their serial number in the window on the left.

3 DEVICE CONFIGURATION

3.1 OPERATING THE SOFTWARE

In terms of operation, **LAN-AD16f Administration Utility** follows the commonly used Windows® standard.

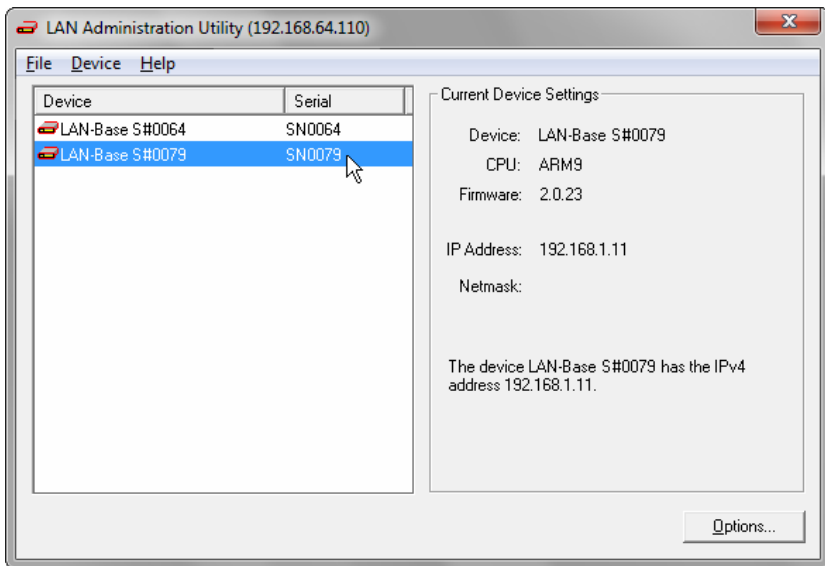


Fig. 7

The menu bar displays the entries "File" and "Device" containing the commands to update the internal software (see "Update", p. 40), start device tests, and to exit the program.

The current settings of the LAN data acquisition system selected on the left are shown on the right side. Press the "Options" button to make configuration changes.

3.1.1 SELECT DEVICE

When starting the program, all connected and operable LAN data acquisition systems are listed (see "Connecting the device", p. 13). The devices differ from each other by the device address located at the device housing.

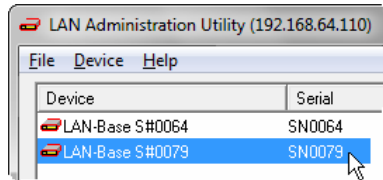


Fig. 8

A device can be identified by the serial number on the outside of the device. The IP address is automatically assigned by the DHCP (*Dynamic Host Configuration Protocol*) server (Link-Local) when connecting to the network. It serves for the unique identification of a device in the network.

When connecting other LAN data acquisition systems, they will be added to the list whereas unplugged devices will be grayed out (alternatively: command "Device / Refresh Device List" or press function key F5).

To select a device, click it with the mouse. The selection of several devices is done either by drawing a frame with the mouse over them or by clicking the individual DAQ systems while pressing the <CTRL> key. If you hold the <SHIFT> key while selecting two devices, all entries in between will be marked, too.

The current settings of the selected DAQ hardware are displayed on the right.

Entry	Function
<i>Device:</i>	shows name (LAN-Base) and serial number of the selected device
<i>CPU:</i>	name of the integrated processor unit
<i>Firmware:</i>	version of the internal software of the device
<i>IP address:</i>	current address used to identify the device in the network (only displayed with manual settings)
<i>Netmask:</i>	indicates the size of the network and how many bits of the IP address belong to the network number (see "Subnet mask", p. 26, only displayed with manual settings)

3.1.2 CHANGE SETTINGS



- To change device settings, the respective LAN data acquisition system must be connected, operable, and selected in the list!
- When being connected, the LAN devices automatically (DHCP) self-assign correct settings. Changing the configuration may have severe consequences. Therefore they should only be done by a network administrator.

Changes only influence the selected device and are done in the "Device settings" dialog, which opens when pressing the "Options" button. The command to install or change internal device software (firmware) is located in the menu item "Device".

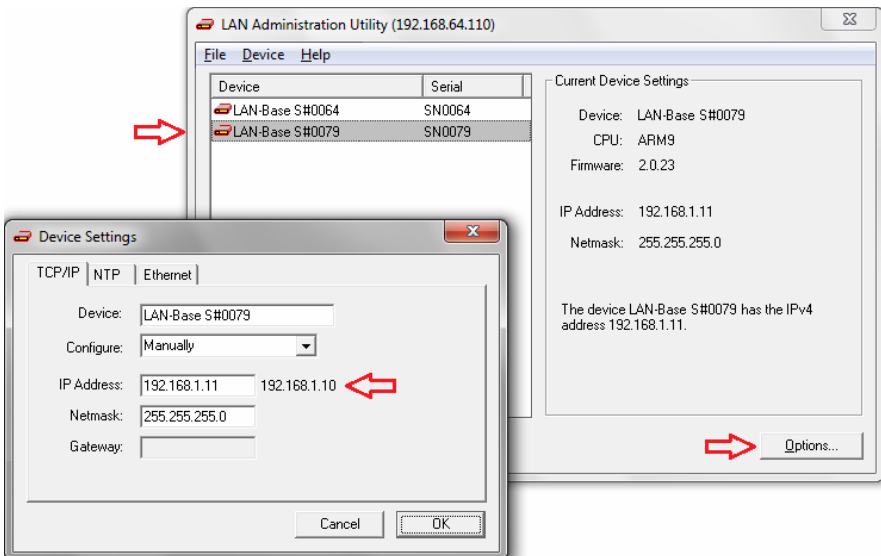


Fig. 9

To be able to undo changes, always the last setting stored in the device is displayed right next to the relating input field.

3.2 TCP/IP

The network DAQ systems LAN-AD16fx and AMS42/84-LAN16fx use the protocol suite TCP/IP (version 4) following the official standardized rules for data transfer via network. The internet e.g. is also based on these principles.



We strongly recommend using the automatically assigned configuration. Manual changes should only be done by a network administrator.

The settings in tab "TCP/IP" of the "Device settings" dialog ("Option" button) in the **LAN-AD16f Administration Utility** are decisive for the successful communication between DAQ system and PC. They have to be entered according to the rules of TCP/IP. For a better understanding, the following chapters give a brief summary about basics and main ideas of TCP/IP.

If your network contains only the PC and one DAQ system, you can use the settings as suggested in the "QuickStart" (see p. 8).

3.2.1 EXCURSUS: BASICS OF TCP/IP

TCP/IP (*Transmission Control Protocol / Internet Protocol*) actually is a collection of various protocols - universally valid rules laying down data transmission via network. The web in particular is a collection of networks using the same protocol series (TCP/IP).

Initially developed on behalf of the American ministry of defense, TCP/IP allows for the communication between computers of the most different size, manufacturer, and operating system.

3.2.1.1 4-LAYER SYSTEM

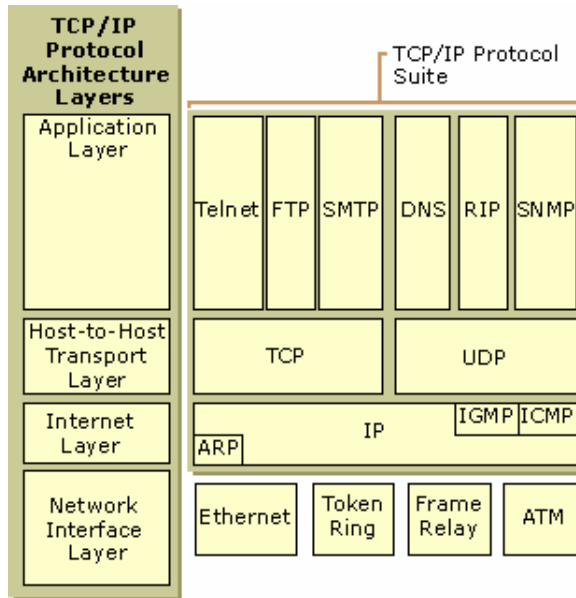


Fig. 10

The TCP/IP structure corresponds to a 4-layer system. Every layer comprises a number of protocols each being responsible for one aspect of communication. Together they form the TCP/IP protocol family. The layers are independent from each other, but build on each other. The advantage of this system is its flexibility, as each layer only communicates with the next upper or lower layer.

3.2.1.1.1 NETWORK LAYER

The lowest level is responsible for all the hardware details regarding the physical network connection and describes the electrical signals and the way of passing it forward. The protocols apply to different network types (e.g. Ethernet, token ring, ATM), which TCP/IP can be based on.

3.2.1.1.2 INTERNET LAYER

The protocols comprised in this layer settle the data transport in the network or between different networks and take care that the packages get to the correct address (*routing*).

In this context to mention is mainly IP (*Internet Protocol*) finding out and realizing the optimum route between transmitter and receiver. In case of an oversize data package IP separates it into several small packages (*fragmentation*). However, it does not check any data loss en route or if packages arrive in the correct order being not considered as safe.

3.2.1.1.3 TRANSPORT LAYER

This layer comprises the two connection-orientated protocols TCP (*Transmission Control Protocol*) and UDP (*User Datagram Protocol*) making data flow between two network hosts possible.

Here TCP guarantees safe data transmission, because it takes care that received packages are put into the correct order and missing packages are resent if an acknowledgement of receipt is not returned to the transmitter in time.

Although the simpler constructed UDP does not provide for this controlling mechanism, it is still recommended for the transmission of small amounts of data, as in this case using TCP sometimes sends more protocol information than useful data.

3.2.1.1.4 APPLICATION LAYER

The highest layer provides protocols handling the details for the respective application. Well-known protocols e.g. are the following:

- DHCP (*Dynamic Host Configuration Protocol*): automatic configuration of a LAN device in the network
- DNS (*Domain Name System*): Assignment of domain names (e.g. www.bmcm.de) and IP address
- FTP (*File Transfer Protocol*): Data transfer
- HTTP (*Hypertext Transfer Protocol*): Transfer of web pages
- NTP (*Network Time Protocol*): same time reference for LAN devices

- SMTP (*Simple Mail Transfer Protocol*): Transfer of e-mail
- SNMP (*Simple Network Management Protocol*): Network management
- Telnet (*Network Terminal*): Remote login

3.2.1.2 SENDING DATA VIA NETWORK

If an application dispatches data, the command is processed layer by layer from top to bottom in the TCP/IP protocol suite. Each layer adds its control information to the data package (*header*) until the command is sent as a bit stream (*encapsulation*) through the net.

When receiving data on the other side, each layer removes its header and gives the rest of the package to the next upper layer (*demultiplexing*).

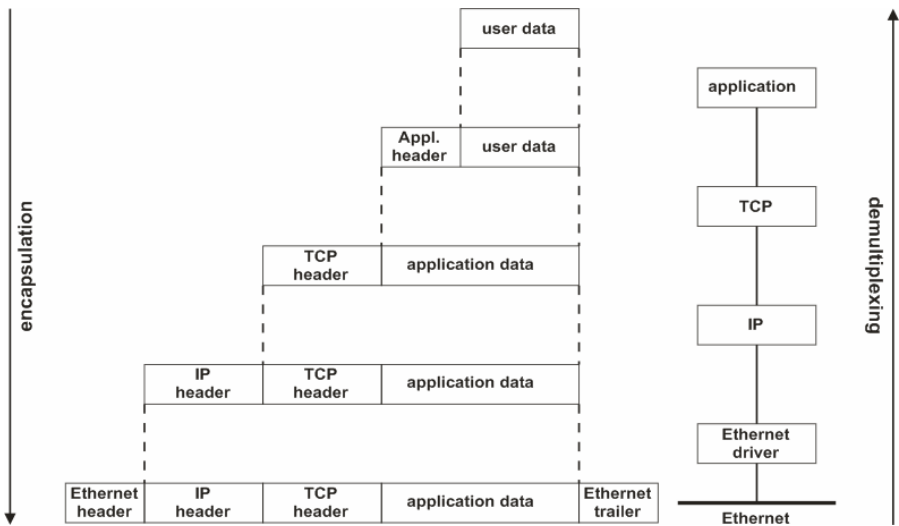


Fig. 11

3.2.1.3 IP ADDRESS

IP addresses serve for the clear identification and addressing of a network host. There are *static* IP addresses, permanently set on the network card of the PC, or *dynamic* IP addresses, which are assigned only for a certain period of time, e.g. when accessing the internet. In this case, the provider assigns an IP address to the user for the time of connection.

As IP addresses must be unique to guarantee correct data transmission, there is an institution, the *Internet Network Information Center* (InterNIC) for the worldwide assignment and administration of IP addresses. Of course, a local network without connection to the outside can use any IP addresses different from each other. In this case, however, it is also strongly recommended to follow certain rules and conventions (see "Private IP addresses", p. 28).

3.2.1.3.1 NOTATION

The IP address is a 32-bit number divided in 4 octets (8-bit numbers), which are written in decimal notation (values between 0 and 255) separated from each other by a point (preceding zeroes may left out). Example: 192.168.64.2

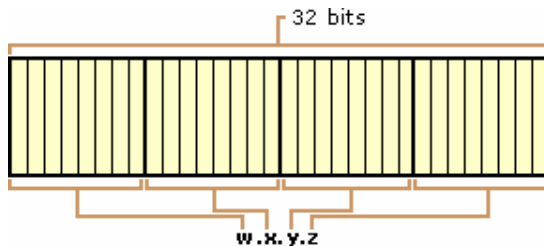


Fig. 12

3.2.1.3.2 NETWORK ID AND HOST ID

The IP address is divided into the network ID to identify the network and the host ID to identify a computer within the network. All users (*hosts*) of a network must have the same network ID. The number of bits reserved by the network ID and the number left for the host ID depends on the class and the size of the network you use (see "Network classes", p. 23) and cannot be determined exactly just by the IP address (see "Subnetting, Supernetting", p. 26).

3.2.1.3.3 SPECIAL CASES

➤ **Network address:**

all bits of the host ID are 0, identifies the network itself; example: 192.168.64.0 (network ID: 192.168.64)

➤ **Broadcast address:**

all bits of the host ID are 1, data package is sent to all network users; example: 192.168.64.255 (network ID: 192.168.64)

3.2.1.4 NETWORK CLASSES

The network class determines how many bits of the IP address are used for the network ID and how many for the host ID, and hence the maximum number of users that can be connected to a network. Basically, the following applies: the more network IDs are available in a class, the less users are possible in one of these networks.

TCP/IP provides for 5 standard classes (class A-E) but only three of those (class A-C) are supported by Windows®. A network class can be identified by the first 8 bits of the IP address.

3.2.1.4.1 CLASS A

The first bit of the IP address of a class A network is always 0. The first 8 bits are reserved for the network ID. That means that all IP addresses with the first decimal between 0 and 127 belong to a class A network.

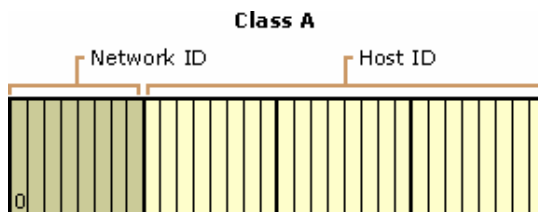


Fig. 13

Reserved network IDs are 0 (default route to simplify routing) and 127 (*loopback*)

address). So $2^7-2 = 126$ network IDs with $2^{24}-2 = 16777214$ host IDs each (without network and broadcast address) are available, which are only assigned to conglomerates on account of their size.

3.2.1.4.2 CLASS B

The first two bits of a class B network are always 10. The first 16 bits are reserved for the network ID. That means that all IP addresses with the first decimal between 128 and 191 belong to a class B network.

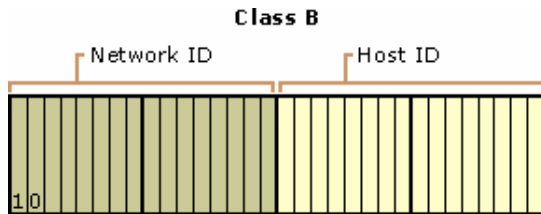


Fig. 14

Therefore, class B contains $2^{14} = 16384$ different network IDs and per network maximum $2^{16}-2 = 65534$ connectable hosts (without network and broadcast address).

3.2.1.4.3 CLASS C

According to the same pattern, the first 24 bits are used for the network ID of a class C network. The first three bits are always 110. So if an IP address starts with 192..223, it belongs to a class C network.

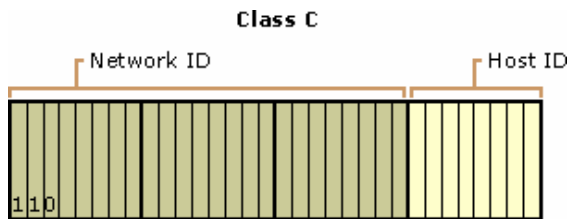


Fig. 15

In this case, $2^{21} = 2097152$ network IDs with maximum $2^8 - 2 = 254$ hosts each (without network and broadcast address) are available.

Because of the fast growth of the Internet, IP addresses are soon running short. Therefore, networks of the different classes itself were divided (see "Subnetting, Supernetting", p. 26) so that the original standard classes only exist in theory today.

3.2.1.4.4 OTHER CLASSES

➤ **Class D:**

If the first 4 bits of an IP address start with 1110, it is a multicast group. In this case, not only one user is addressed, but always the whole group. There is no division into network ID and host ID, but only a 28 bit multicast ID.

➤ **Class E:**

Networks of this class only exist on paper so far and are reserved for future use. In this case, the first 5 bits of the IP address start with 11110.

3.2.1.4.5 SUMMARY

Class	IP address	Network ID		Host ID	
		Length (bits)	Max. number	Length (bits)	Max. number
A	0.0.0.0 - 127.255.255.255	8	126	24	16777214
B	128.0.0.0 - 191.255.255.255	16	16384	16	65534
C	192.0.0.0 - 223.255.255.255	24	2097152	8	254
D	224.0.0.0 - 239.255.255.255	28 bits, 268435456 multicast IDs			
E	240.0.0.0 - 247.255.255.255	27 bits, 134217728 IDs			

3.2.1.5 SUBNETTING, SUPERNETTING

As mentioned before, the IP addresses registered worldwide are running short on account of the fast internet growth so that networks of the standard classes (see "Network classes", p. 23) were divided into several small networks (*subnets*). That means that a subnet of a network class provides less host addresses than the standard network would.

This makes sense for a small company, for example, using a class C network and not needing 254 IP addresses which can be reached from the outside. Many of those addresses would not be used, but on the other side were not available to anyone else. With subnetting, a more efficient utilization of the network is achieved.

3.2.1.5.1 SUBNET MASK

The subnet mask is a 32-bit number written like IP addresses, indicating which part of the IP address belongs to the network ID and which to the host ID. All bits of the network ID are 1 and all bits of the host ID are 0.

As this part is known for networks of standard classes (see "Network classes", p. 23), the standard subnet masks of these classes are always:

Class	Length Net ID	Subnet mask	
		binary	decimal
A	8	11111111.00000000.00000000.00000000	255.0.0.0
B	16	11111111.11111111.00000000.00000000	255.255.0.0
C	24	11111111.11111111.11111111.00000000	255.255.255.0

3.2.1.5.2 SUBNETTING

To divide a standard network, use leading bits of the host ID of the standard subnet mask for the network ID, i.e. set it to 1.

➤ **Example:**

A standard network (class C) with the network number 192.168.64.0 provides 254 available IP addresses and the subnet mask 255.255.255.0. If changing the leading bit of the host ID to 1 also, you receive the binary subnet mask

11111111.11111111.11111111.10000000 (dec: 255.255.255.128). Now the network is divided in two. The network IDs of both subnets are 25 bits long and only 126 (without network and broadcast address) host IDs are available.

	Subnet 1	Subnet 2
Host IDs	192.168.64.1 - 192.168.64.126	192.168.64.129 - 192.168.64.254
Net ID	192.168.64.0	192.168.64.128
Broadcast ID	192.168.64.127	192.168.64.255
Subnet mask	255.255.255.128	255.255.255.128

3.2.1.5.3 SUPERNETTING

If the number of available network users is too small, the standard subnet mask is slightly changed by reducing the length of the network ID, i.e. setting the last bits of the network ID of the subnet mask to 0.

➤ **Example:**

To enlarge the standard network with the network address 192.168.64.0, change its subnet address from 255.255.255.0 to 255.255.254.0 (binary: 11111111.11111111.11111110.00000000). In this case, there are not only $2^8 - 2 = 254$ hosts (without network and broadcast address) available, but $2^9 - 2 = 510$ now.

	Class C net	Class C net after supernetting
Host IDs	192.168.64.1 - 192.168.64.254	192.168.64.1 - 192.168.65.255
Net ID	192.168.64.0	192.168.64.128
Broadcast ID	192.168.64.255	192.168.65.255
Subnet mask	255.255.255.0	255.255.254.0

3.2.1.5.4 IDENTIFICATION OF NETWORK ID AND HOST ID

The difficulty resulting from subnetting or supernetting is the fact that the line between network and host ID, i.e. their maximum available number, cannot be identified clearly by the IP address anymore. You need the subnet mask to tell which IP addresses are available in your network.

➤ **Example:**

A computer has the IP address 192.168.64.54 and the subnet mask 255.255.255.192 (binary: 11111111.11111111.11111111.11000000).

Altogether, there are $2^6 = 64$ IP addresses available in this network. That means the user with the IP address 192.168.64.54 is a host of a class C subnet with the network address 192.168.64.0 and the broadcast address 192.168.64.63. The IP addresses that can be assigned in this network are within the range of 192.168.64.1 - 192.168.64.62.

3.2.1.6 PRIVATE IP ADDRESSES

Local area networks (*LANs*) that are not connected to the internet or that cannot be reached from the outside may use any IP addresses, of course, without having to care if they are already used by other networks. The only condition is to keep the rules for the assignment of IP addresses, as described before (e.g. uniqueness, same network ID, etc.).

The best and safest way, however, is to use private IP addresses for local networks. Those are not given out by the InterNIC, because they are reserved for private use only. There are reserved numbers in all network classes (see "Network classes", p. 23) for private IP addresses, which cannot be addressed via Internet.

Class	Private IP addresses
A	10.0.0.1 - 10.255.25.254
B	172.16.0.1 - 172.31.255.254
C	192.168.0.1 - 192.168.255.254

3.2.1.7 USEFUL COMMANDS

Use the commands "ipconfig" and "ping" in the MS-DOS command prompt (Windows® Start menu: *Programs / Accessories / Command Prompt*) as a simple test of a working TCP/IP installation on a PC.

After opening the command prompt, enter the command "ipconfig". Something like the following printout should be displayed:

```
C:\>ipconfig
Windows NT IP Configuration
Ethernet adapter E190x1:

    IP Address. . . . . : 192.168.65.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

C:\>
```

Here you will find the IP address of the PC, in the example above "192.168.65.1". This address can be used together with "ping" to build up and test a local IP connection. Enter "ping 192.168.65.1" and replace the address of this example by the address edited by "ipconfig".

```
C:\>ping 192.168.65.1
Pinging 192.168.65.1 with 32 bytes of data:

Reply from 192.168.65.1: bytes=32 time<10ms TTL=128
Reply from 192.168.65.1: bytes=32 time<10ms TTL=128
Reply from 192.168.65.1: bytes=32 time<10ms TTL=128
Reply from 192.168.65.1: bytes=32 time<10ms TTL=128

C:\>
```



This simple test just makes sure that TCP/IP is installed. It is not tested if the physical network connection is working. To verify this, use the command "ping" with the IP address of another PC in the network.

3.3 DEVICE SETTINGS

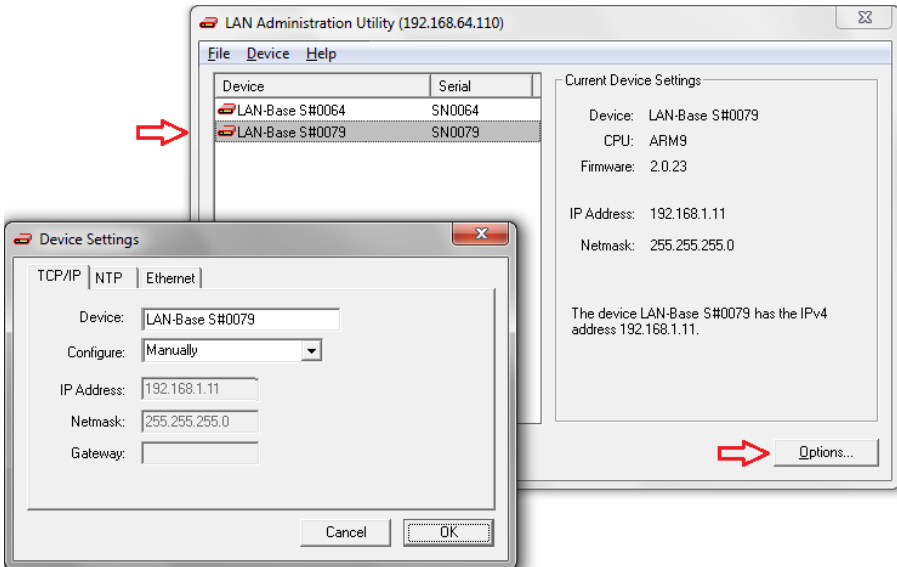


Fig. 16

The "Device settings" dialog is opened via the "Options" button. Changes always relate to the selected LAN devices.

3.3.1 TAB "TCP/IP"

The parameters that can be set in the "Device settings" dialog are very important network settings. They are the condition for a correct connection of the LAN devices in the network and have to be done according to the guidelines of TCP/IP (see "Excursus: Basics of TCP/IP", p. 18).



We strongly recommend using the automatically assigned configuration. Manual changes should only be done by a network administrator.

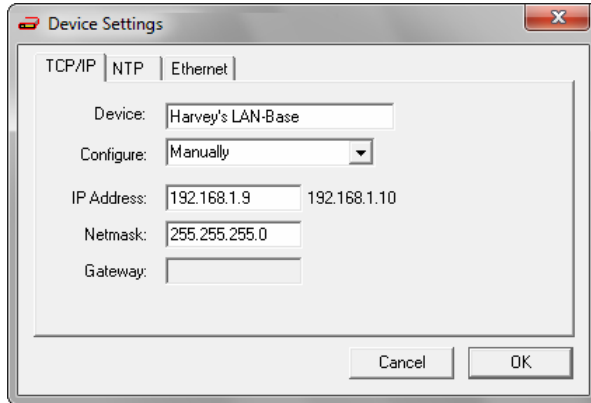


Fig. 17

If switching from automatic configuration to "Manually", settings can individually be modified. When changing the contents of the input fields, the last saved configuration is displayed on the right.

Entry	Description
<i>Device:</i>	assign a name for the selected device; default setting: LAN-Base(SN<serial number>)
<i>Configure:</i>	change between automatic (<i>DHCP</i>) or manual settings
IP address:	assign an IP address available in the connected network for the clear identification of the device
<i>Netmask:</i>	subnet mask of the (sub-)net you are using to ascertain the network size and the number of maximum connectable hosts (see "Subnet mask", p. 26)

The example above (see Fig. 17) uses a local network (see "Private IP addresses", p. 28) of the standard class C (netmask: 255.255.255.0 → network ID: 192.168.1.9). It provides for 254 possible IP addresses within the range of 192.168.1.1 - 192.168.1.254 (without network and broadcast address).

3.3.2 TAB "NTP"

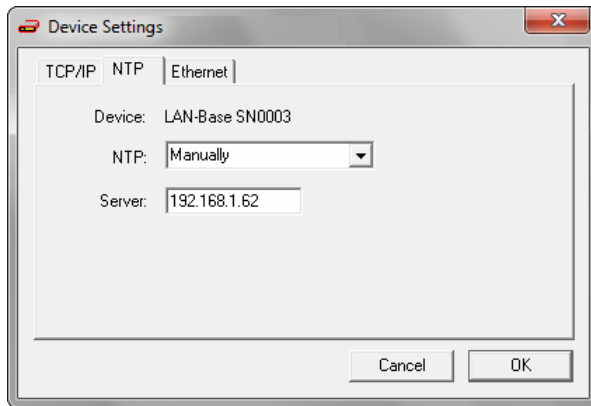


Fig. 18

NTP (*Network Time Protocol*) is a standard to synchronize clocks via network in computer systems. By default, LAN devices get a common time relation via DHCP.

If an NTP server installed in the network is to be used instead, it has to be enabled in TAB "NTP" of the "Device settings" dialog and specified by the IP address.

Entry	Description
<i>Device:</i>	shows name (LAN-Base) and serial number of the selected device
<i>NTP:</i>	<ul style="list-style-type: none"> • Automatically (DHCP): applies the NTP server address provided by DHCP (only works if the TCP/IP configuration in tab "TCP/IP" is also set to "Automatically"!) • Manual: uses the manually configured address of the NTP server • Off: NTP is turned off
<i>Server:</i>	IP address of the server providing the <i>NTP</i> protocol

3.3.3 TAB "ETHERNET"

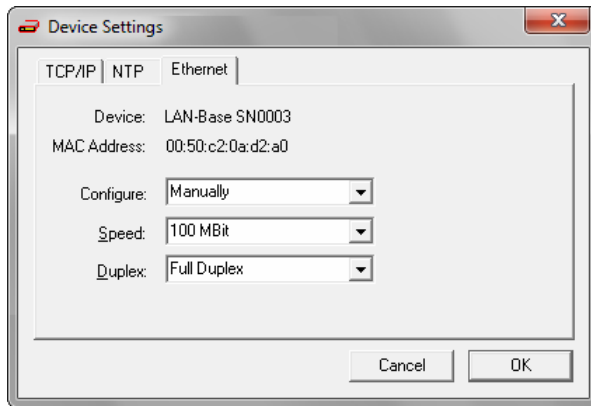


Fig. 19

The settings on tab "Ethernet" of the "Device settings" dialog relate to network transmission.

It is recommended to use the automatic configuration. Manual changes are only required in case of great transmission problems (e.g. Link LED at the LAN device does not turn on).

Entry	Description
<i>Device:</i>	shows name (LAN-Base) and serial number of the selected device
<i>MAC Address:</i>	Hardware address (Media-Access-Control address) of the LAN device
<i>Configure:</i>	change between automatic (recommended) or manual settings
<i>Speed:</i>	transmission rate for the data packages
<i>Duplex:</i>	choose if sending and receiving of data packages is to be at the same time (<i>Full Duplex</i>) or in series (<i>Half Duplex</i>)

3.4 DEVICE TESTS

Besides the configuration of the LAN devices, the software **LAN-AD16f Administration Utility** also serves for operation tests of the DAQ system. Tests are always done for the selected device(s).

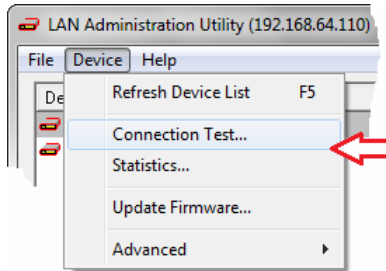


Fig. 20

The commands to start a **connection test** and record a **device statistics** are included in the "Device" menu.

3.4.1 CONNECTION TEST

The connection test (menu "Device") verifies the correct transmission of data packages via Ethernet.

The relevant parameters are continuously displayed for the respective selected LAN device. Press the button "End" to stop the connection test.

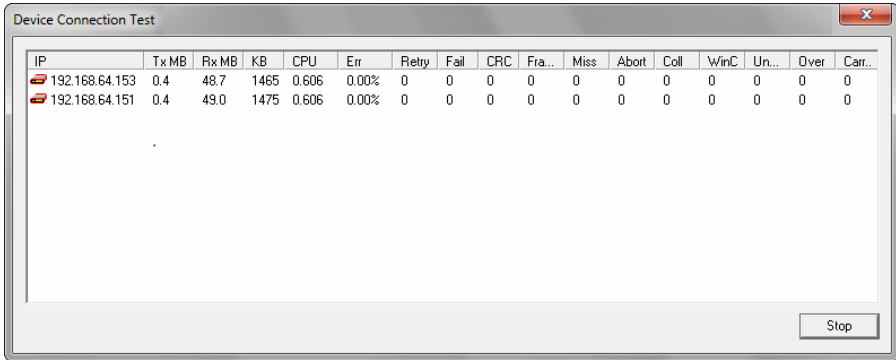


Fig. 21

Entry	Description
<i>IP</i>	IP address of the tested LAN data acquisition system
<i>Tx MB</i>	number of transmitted MB
<i>Rx MB</i>	number of received MB
<i>KB</i>	transmission rate (in kB/sec) of the data packages (app. 100kB/sec)
<i>CPU</i>	processor load in percent (0..1)
<i>Err</i>	error rate in percent (= (Tx MB – Rx MB) : Tx MB)
<i>Retry</i>	number of retries (max. 10) to send a data package (should be 0)
<i>Fail</i>	number of data packages that have not been sent (should be 0)
<i>CRC</i>	checksum error
<i>Frame</i>	framing error of the TCP/IP data package
<i>Miss</i>	number of lost data packages
<i>Abort</i>	number of transmission errors
<i>Coll</i>	number of "collisions" when sending data packages (→ transmission is repeated)
<i>WinC</i>	number of window collisions
<i>Under</i>	internal error of the Ethernet controller of the LAN device (<i>underrun</i>)
<i>Over</i>	internal error of the Ethernet controller of the LAN device (<i>overrun</i>)
<i>Carrier</i>	the transmission pulse saved in the data package is not recognized → data package cannot be sent (<i>carrier lost</i>)

The "KB" value is the one-way transmission rate. As the LAN device both sends and receives data packages, the transmission rate is effectively twice as much.

If the transmission of a data package is not successful, it will be repeated up to 10 times ("Retry") and then cancelled ("Fail" counts up 1, "Retry" is reset).

Errors of the category "Miss" and "Aborted" are typical errors occurring at high network load. In case of an *underrun* or *overrun*, we recommend contacting us, as this must not happen in a working measurement setup. *Carrier lost* is an indication for a short-time interruption of a cable (e.g. loose contact).

3.4.2 DEVICE STATISTICS

Choose the command "statistics" in the "Device" menu to record various hardware data.

If you click the button "Record", these key values will be stored in a signal file. It can be mailed to bmc for remote diagnostics of problems concerning installation and during operation.

The relevant parameters are continuously displayed for the respective selected LAN device. Press the button "Stop" to finish the scan.

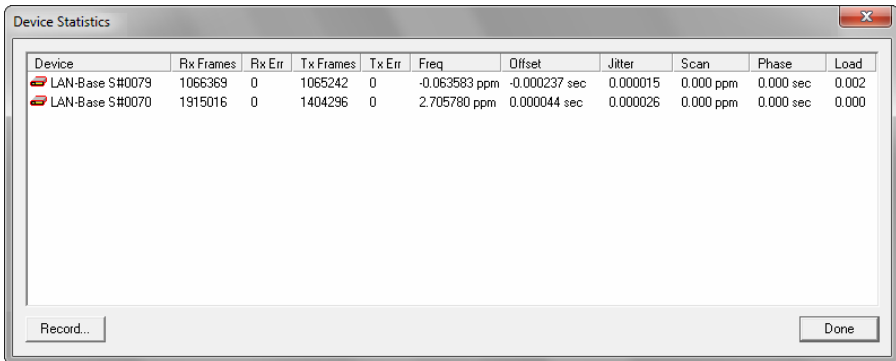


Fig. 22

3.5 TIME-SYNCHRONOUS SAMPLING

The LAN-AD16fx generates the sample period by means of an internal quartz. In addition to a specific basic accuracy of the frequency produced, all quartzes depend on temperature. Even with precise quartzes, this frequency error can be up to 40msec per hour. During long measurements, this error adds up causing a time offset between a LAN-AD16fx and the measuring PC or between several LAN-AD16fx devices.

In combination with NextView®4, the LAN-AD16fx can do measurement time-synchronously in relation to real-time to minimize the time offset. For time-synchronous measurements the device uses the selected NTP server to regulate the frequency of the sample clock. This adjustment compensates all frequency errors of the sample clock reducing the time offset between sampling time and real time to a minimum.

To do time-synchronous measurement, a DHCP and an NTP server is required in the local network of the LAN-AD16fx. The DHCP server must have been set by the system administrator to automatically assign the IP addresses to the LAN-AD16fx. Besides that, the NTP option (42) must be configured in the respective entry of the DHCP server (the LAN-AD16fx uses the first NTP server from the list). The LAN-AD16fx should automatically get TCP/IP settings (see tab "TCP/IP", p. 30) as well as NTP settings (see tab "NTP", p. 32) from the DHCP.

A time-synchronous measurement must also be configured in NextView®4 by activating the option "synchronized" on tab "Clock" of the "Device Configuration" dialog.

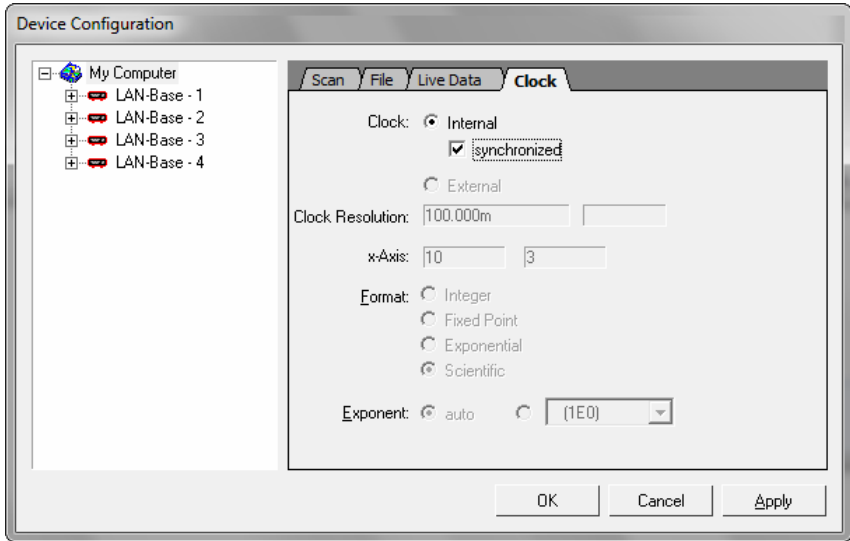


Fig. 23

Of course, the accuracy to be achieved depends on the accuracy of the NTP server used. A "normal" NTP server synchronizing the time via internet (DSL) should reach app. $\pm 10\text{msec}$. The same accuracy can be expected from the LAN-AD16fx devices then, too.

The best results are received by an NTP server with GPS synchronization realizing phase errors of clearly less than $\pm 0.1\text{ms}$ from device to device under optimum conditions.

3.5.1 CHECK TIME-SYNCHRONOUS SAMPLING

To test the settings concerning NTP server and time-synchronous measurement, open the device statistics.

The columns "Freq" and "Offset" return the current values of the NTP client in the LAN-AD16fx. If they are 0.0, an NTP server has not been configured for the LAN-AD16fx (or the NTP server is not available).

The columns "Scan" and "Phase" show the current values of the sampling clock adjustment. If both are 0.0, the option "synchronized" has not been checked in NextView®4 (see "Time-synchronous sampling", p. 37).

Device	Rx Frames	Rx Err	Tx Frames	Tx Err	Freq	Offset	Jitter	Scan	Phase	Load
LAN-Base S#0079	1066369	0	1065242	0	-0.063583 ppm	-0.000237 sec	0.000015	0.578 ppm	0.002 sec	0.002
LAN-Base S#0070	1915016	0	1404296	0	2.705780 ppm	0.000044 sec	0.000026	0.063 ppm	0.001 sec	0.000

Fig. 24

3.6 UPDATE FIRMWARE

You can continuously keep your DAQ system up to date, as in case of extended functionality or possible bug-fixing the latest software versions can be transmitted to the device. These are available in the **LAN-AD16f Administration Utility**.

The latest version of the **LAN-AD16f Administration Utility** can be downloaded for free from our website at <http://www.bmcm.de> .

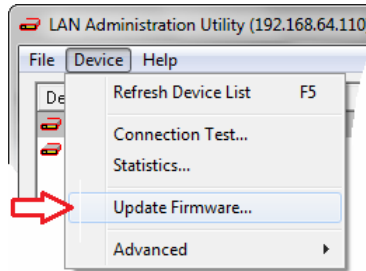


Fig. 25

The command to update the internal device software (firmware) is included in the "Device" menu.

The currently used firmware version of the LAN device is displayed in the "Current Device Settings" on the right side of the user-interface.

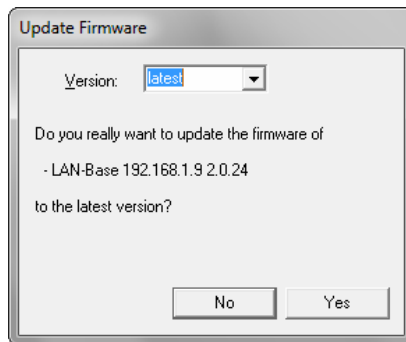


Fig. 26

In **LAN-AD16f Administration Utility**, select the device that needs a firmware update and open the command "Update firmware..." (menu "Device").

Before the copying process is started, you can choose the version. You are prompted to confirm the updating before the process of copying starts.

4 GLOSSARY

BOOTLOADER

Internal device software in the Read Only Memory (ROM) to automatically upload the operating system when turning on or restarting the device.

BROADCAST ADDRESS

Reserved IP address for sending data packages to all network hosts; in this case all bits of the host ID are set to 1.

DEVICE ADDRESS

Each LAN device is supplied with a chip assigning a worldwide unique 6x2 byte digit number to the device. It is located on the device label on the outside of the housing.

DHCP

Protocol to automatically integrate a LAN device into an existing network without manual configuration settings being necessary.

ETHERNET

Network standard for modern networks based on IP technology; connection via coaxial-, fiber-optic or Twisted Pair cable.

FIRMWARE

Software routines stored and kept in the Read Only Memory (ROM) of the device even when turning off the device.

GATEWAY

Interface for the connection of networks even using different protocols of communication so that information can be sent from one network to the other.

HOST ID

Last part of the IP address to clearly identify a network user.

INTERNIC

Internet Network Information Center: worldwide registration and administration of IP addresses.

IP ADDRESS

32-bit (4-Byte) binary number assigned to each network host for unique identification. Notation: 4 decimals between 0..255 separated from each other by a dot.

LINK-LOCAL

Address space (169.254.0.1 - 169.254.255.254) for automatically assigned private IPv4 addresses for terminals.

LOOPBACK ADDRESS

In all networks reserved address for your local PC: 127.0.0.1. It serves for the simplification of network applications, in which the local PC is addressed in the same way as any outside PC.

NETMASK

The netmask indicates the line between network and host ID of an IP address and therefore the number and range of available user addresses of a network.

NETWORK

Group of computers and connected devices of different size and extent connected with each other by communication systems. The connection is either permanently (e.g. cable) or temporarily (e.g. modem).

NETWORK ADDRESS

Reserved IP address to identify the network. In this case all bits of the host ID are set to 0.

NETWORK CLASSES

They serve for the subdivision of networks into classes of different size. Supported by Windows[®] are the standard classes A, B, and C. The following always applies: the more networks are provided in a class, the smaller they are, i.e. is the number of connectable hosts.

NETWORK ID

First part of the IP address identifying the network itself. All users of a network must have the same network ID.

NTP

Protocol to synchronize devices in a network.

PROGRAM GROUP

Entry in the Windows® start menu at *Start/Programs* containing the software itself, additional programs, and help files.

ROUTER

Relaying appliance in a communication network. Single network: receiving and forwarding of sent data packages, finding out the most effective and correct route to the destination; several connected local networks: linking unit between networks to make communication between different networks possible.

ROUTING

At every network connection, deciding the best and correct route of a data package to its destination address.

SUBNET MASK

In binary notation, it shows the line between network and host ID. The leading digits (1) indicate the bits of the network ID, the following digits (0) the bits of the host ID. With the subnet mask, you can find out how many and which host addresses are available in a subnet.

SUBNETTING

Subdivision of networks in several small networks.

SYNCHRONIZATION

For networks adjustment of the system, time between the individual network hosts for a better communication and coordination.

For DAQ systems, adjustment of the scan time between connected DAQ systems to get a common relation to time.

SYSLOG

Service provided by UNIX to write messages of a network participant into a *.log file stored and visualized on another PC which is especially important for debugging.

TCP/IP

Transmission Control Protocol/Internet Protocol: standard protocol for data transmission via network (internet also).

5 INDEX

A

AMS42-LAN16f 5, 10, 13, 16, 18
 AMS84-LAN16f 5, 10, 13, 16, 18
 Application layer 20

B

Broadcast address 23

C

Class A 23
 Class B 24
 Class C 24
 Class D 25
 Class E 25
 Configuration
 automatic 16, 17, 20, 30, 33
 automatic settings 9
 manual 31
 manual settings 15
 Connection test 9, 34
 Copyrights 7

D

Data package 20
 Data transmission 20
 Data transport 20
 Demultiplexing 21
 Device
 add 16
 change settings 17, 30
 remove 16
 select 16
 select several 16
 Device address 16
 Device information 16
 Device settings 17, 18, 30, 32, 33
 Device software 40
 Device statistics 36, 39
 Device test 5, 15, 34

Device type 16
 DHCP 17, 20, 30
 DHCP server 37
 Directory path 11
 DNS 20
 Duplex 33

E

Encapsulation 21
 Error 36
 Ethernet 5, 19, 33, 34
 Example 31
 Example configuration 9, 18
 Exit program 8

F

Firewall 5, 9
 Firmware 5, 9, 17
 update 41
 version 16
 Fragmentation 20
 FTP 20

G

GPS 38

H

Header 21
 Host 22
 Host ID 22, 28
 HTTP 20

I

Installation
 device 13
 internal software 17
 software 8, 10
 Installation folder 11

Installation path 11
 Internet 18, 22, 25, 26, 28
 Internet address 6
 Internet layer 20
 IP 20
 IP address 5, 20, 22, 31, 32
 assignment worldwide 22
 available 28
 dynamic 22
 link-local 9, 16
 notation 22
 PC 9, 29
 private 28
 static 22
 ipconfig command 29

L

LAN 28
 LAN-AD16f 5, 10, 13, 16, 18
 Layer system 19
 Layers 19
 Link-local 9

M

Multicast group 25
 Multicast ID 25

N

Netmask 16, 31
 Network 16, 18, 20
 class A 23
 class B 24
 class C 24
 class D 25
 class E 25
 subnetting 26
 supernetting 27
 Network address 23
 Network class 23
 standard 23
 Network DAQ system 5
 Network ID 22, 28
 Network layer 19
 Network settings 30
 NTP 20, 32

NTP server 32, 37, 39

P

ping command 29
 Private IP addresses 28
 Processor 16
 Program group 8, 11
 Program start 14, 16

Q

Quickstart 8

R

Routing 20

S

Serial number 5, 8, 14, 16
 SMTP 21
 SNMP 21
 Software Collection 8, 10
 Speed 33
 Start menu 11
 Statistics 36
 Subnet 26
 Subnet mask 26
 standard class 26
 Subnetting 26
 Supernetting 26, 27
 Synchronization 20, 37
 check 39
 System requirements 10

T

TCP 20
 TCP/IP 5, 10, 18, 19, 21, 23, 30
 basics 18
 structure 19
 test installation 29
 Telnet 21
 Test
 IP connection 29
 Time 32

INDEX

Time-synchronous 37
Transmission 33, 36
Transport layer 20

U

UDP 20
Update 40