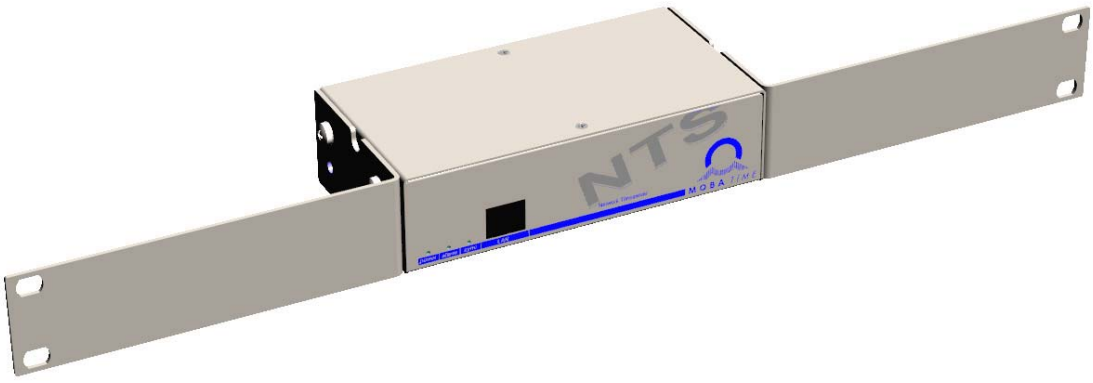
MOUNTING AND INSTRUCTION MANUAL

Network Time Server NTS

Network Time Server



Certification of the Producer

STANDARDS

The Network Time Server NTS was developed and produced in accordance with the EU Guidelines:
2006 / 95 / EC
2004 / 108 / EC
96 / 48 / EC

CE

This product belongs to Class A in accordance with EN 55022.
This equipment can lead to radio interference. In this case, actions must be taken by the user.

References to the Instruction Manual

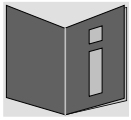
1. The information in this Instruction Manual can be changed at any time without notice.
   The current version is available for download on www.mobatime.com.
2. The device software is continuously being optimized and supplemented with new options. For this reason, the newest software version can be obtained from the Mobatime website.
3. This Instruction Manual has been composed with the utmost care, in order to explain all details in respect of the operation of the product. Should you, nevertheless, have questions or discover errors in this Manual, please contact us.
4. We do not answer for direct or indirect damages, which could occur, when using this Manual.
5. Please read the instructions carefully and only start setting-up the product, after you have correctly understood all the information for the installation and operation.
6. The installation must only be carried out by skilled staff.
7.

Overview

Table of contents

1 Safety

1.1 Safety instructions



Read this chapter and the entire instruction manual carefully and follow all instructions listed. This is your assurance for dependable operations and a long life of the device.

Keep this instruction manual in a safe place to have it handy every time you need it.

1.2 Symbols and Signal Words used in this Instruction Manual

	**Danger!** Please observe this safety message to avoid electrical shock! There is danger to life!
	**Warning!** Please observe this safety message to avoid bodily harm and injuries!
	**Caution!** Please observe this safety message to avoid damages to property and devices!
	**Notice!** Additional information for the use of the device.

1.3 Intended Use

The **Network Time Server NTS** is a time server for the use in network environments. It can be synchronized from NTP and be used as NTP server. In addition, it can read the time from DCF or GPS (e.g. from GPS 4500).

For additional functions, see the device descriptions in chapter 3.4.

The device is designed for stand-alone use; optionally, 2 mounting brackets allow installation into a 19" rack.

1.4 Observe operating safety!

Caution!

- Never open the housing of the device! This could cause an electric short or even a fire, which would damage your device. Do not modify your device!
- The device is not intended for use by persons (including children) with limited physical, sensory, or mental capacities or a lack of experience and/or knowledge.
- Keep packaging such as plastic films away from children. There is the risk of suffocation if misused.

1.5 Consider the installation site!

Caution!

- To avoid any operating problems, keep the device away from moisture and avoid dust, heat, and direct sunlight. Do not use the device outdoors.

Danger! Make sure
that you wait before using the device after any transport until the device has reached the ambient air temperature. Great fluctuations in temperature or humidity may lead to moisture within the device caused by condensation, which can cause a short.

1.6 Please observe the electromagnetic compatibility!

Caution!

- This device complies with the requirements of the EMC and the Low-voltage Directive.

2 Maintenance

2.1 Troubleshooting: Repairs

Please read carefully Appendix "D Troubleshooting" if your device does not work properly.

If you cannot rectify the problems, contact your supplier from whom you have purchased the device.

Any repairs must be carried out at the manufacturer's plant.

Disconnect the power supply immediately and contact your supplier, if …

- liquid has entered your device
- the device does not properly work and you cannot rectify this problem yourself.

2.2 Cleaning

- Please make sure that the device remains clean especially in the area of the connections, the control elements, and the display elements.
- Clean your device with a damp cloth only.
- Do not use solvents, caustic, or gaseous cleaning substances.

2.3 Disposing

Device
At the end of its lifecycle, do not dispose of your device in the regular household rubbish. Return your device to your supplier who will dispose of it correctly.

Packaging
Your device is packaged to protect it from damages during transport.
Packaging is made of materials that can be disposed of in an environmentally friendly manner and properly recycled.

3 General Information: Introduction

3.1 Scope of Delivery

Please check your delivery for completeness and notify your supplier within 14 days upon receipt of the shipment, if it is incomplete.

The package you received contains:

- Network Time Server NTS
- Connector set
  - spring terminal 6-pole orange
- wall power supply 230 VAC – 24 VDC
- 2 mounting tools with spring terminals

Optional

- Mounting set for rack mounting consisting of:
  - 2 brackets
  - 4 mounting screws for bracket to housing
  - 4 nuts for 19" housing
  - 4 screws M6 for the nuts
  - 4 plastic discs for screws M6

3.2 Technical Data

See Appendix "G Technical data".

3.3 Device Description in this Manual

This instruction manual is for the Network Time Server NTS.

3.4 Introduction

The **Network Time Server NTS** is a NTP Time Server for use in network environments. It can be synchronized by DCF or GPS (e.g. from GPS4500), AFNOR-A/C, IRIG-B and NTP, and act as a NTP server in a network.

The NTS can provide NTP clocks with NTP and time zone tables via multicast or unicast.

As the "main“ master clock, the NTS can synchronize other master clocks or other equipment with DCF or optionally with synchronization impulses.

The NTS can send both e-mails and SNMP traps for alerting purposes.

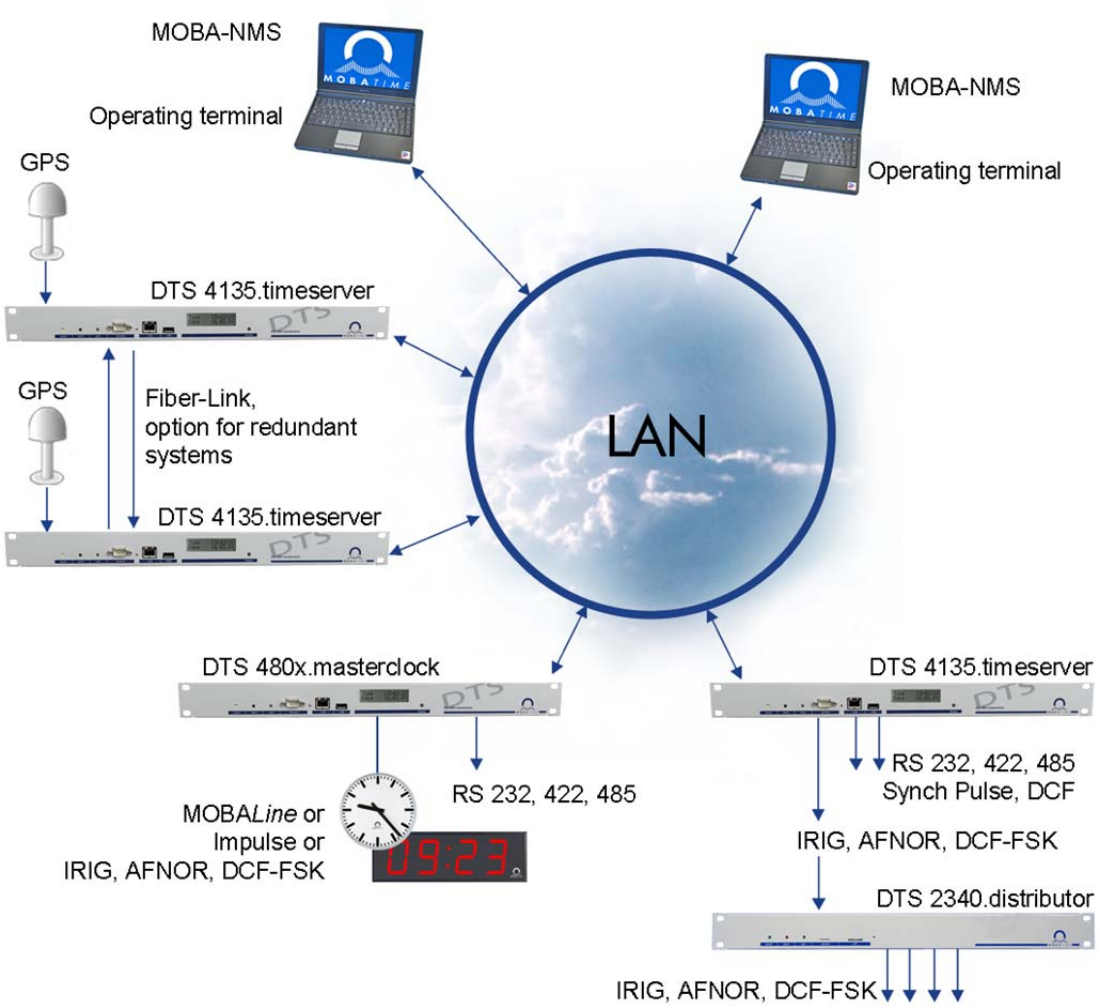
Using MOBA-NMS and SNMP, the NTS can be fully operated and its configuration and system status can be requested.

3.5 Device types

Model:	Features:	Product no.:
Network Time Server NTS	According to above description	**205650 / 117990**
Mounting bracket	Including mounting accessories	**205897**

3.6 DTS distributed time system

The DTS (Distributed Time System) is a system developed by Moser-Baer AG to connect decentralized master clocks, slave clock lines and time servers. For communication, standard LAN (Ethernet) is used. The DTS can be centrally operated and monitored.



3.7 MOBA-NMS - Network Management System

MOBA-NMS is a software used for central management and inquiry of state and alarm information. It supports DTS / NTS devices as well as all MOBATime analog and digital network clocks and can handle a network with more than 1000 devices. This software provides extensive functions for the configuration, installation, back-up / recovery etc. especially for DTS devices.

Due to the DTS concept, MOBA-NMS can be installed multiple times in one network. With different user rights on the device and software level, the configuration abilities of different users can be set as required.

For DTS / NTS devices, all communication is conducted over SNMP V3. The SFTP protocol is used for broadcasting files.

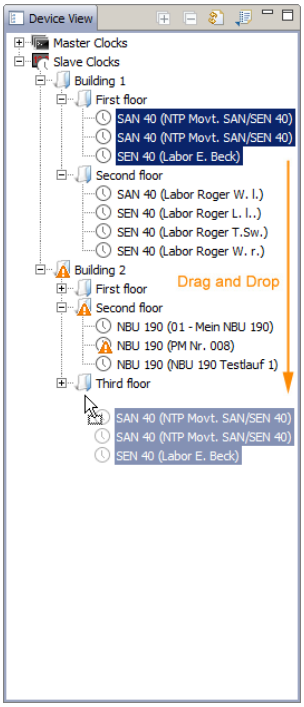
3.7.1 Overview of the main functions

The main MOBA-NMS functions for DTS / NTS devices and network clocks are listed below:

- automatic device scan over multicast or IP range
- device management using user-defined device groups ➔ see chapter „3.7.2 Device management“
- intuitive user interface with input check for the device configuration
- status / alarm request and display on the device group level
- device firmware update for one or several devices (parallel)
- support for device commands, e. g. reset, restart etc.
- back-up / recovery of DTS / NTS devices
- transfer of the whole DTS / NTS configuration to another device
- user management with different access rights
- monitor for NTP and time zone packages
- editor for time zone files
- online help
- etc.

3.7.2 Device management

All MOBATime network devices are displayed in the so-called device view. Here, the devices can be grouped according to user-defined criteria. For this, the individual devices can simply be moved to the according groups and sorted using drag and drop. There is no limit to the number of groups and sub-groups.



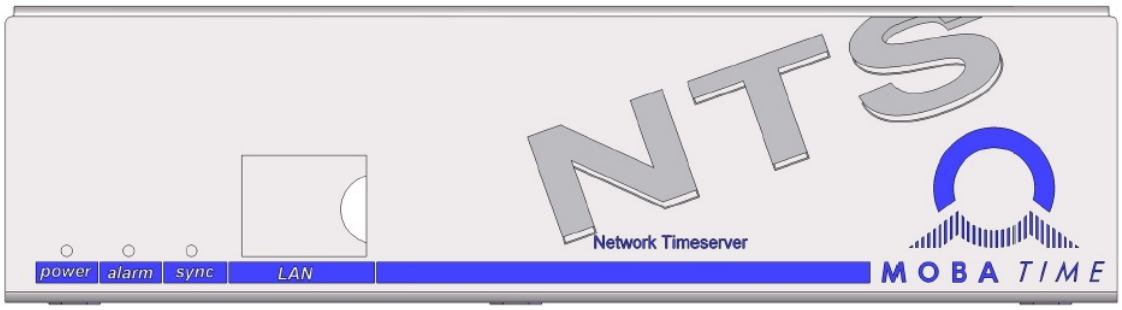
Besides the organizational advantages (easier locating, better overview), a device group has the following advantages:

- commands and device updates can be applied to the whole group (including sub-groups).
- Alarms and errors of included devices are displayed on the group level.
- Complete groups can be moved / sorted among themselves.

The content of the device view can be saved and opened at a later time. The created structure and breakdown into groups is preserved.

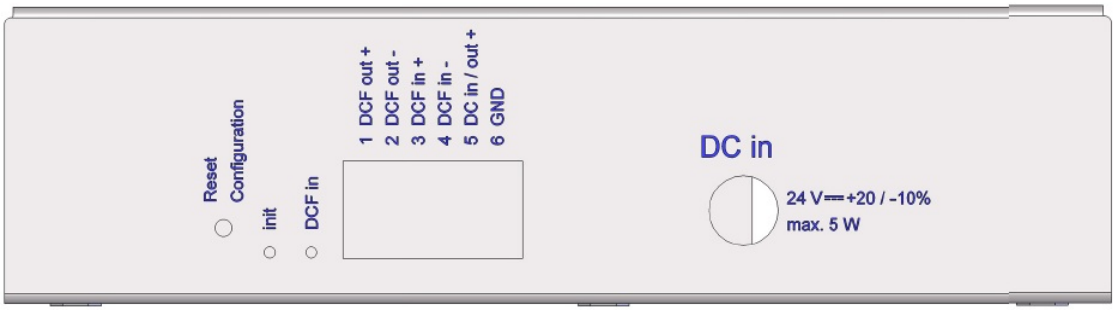
4 Displays

4.1 LED displays front side



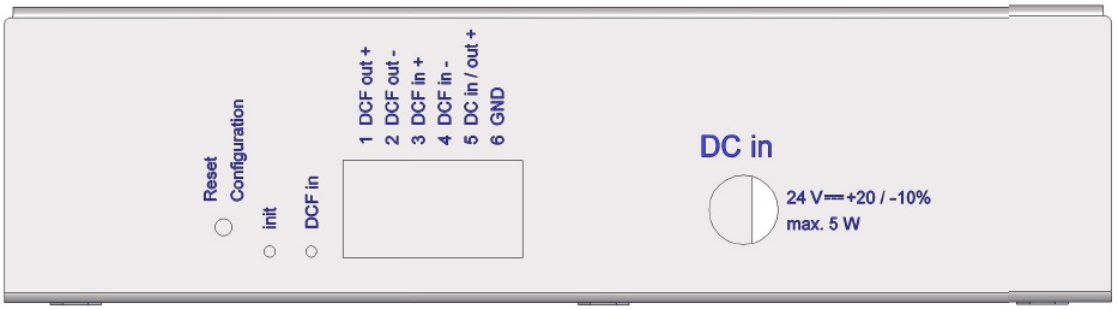
Description	Color	Status	Description
power	green	on	mains or DC power supply is in order
		off	no power supply
alarm	red	on	the alarm relay signalizes an alarm
		off	no active alarms
sync	green	on	NTS can read the time from a synchronization source
		blinking	internal time source (RTC) or manual time-setting (blinking until ‘NTP synch. loss’ alarm appears or external source is available after restart)
		off	synchronization source is not available off if the alarm “loss time source str” appears. see chapter 6.5.5, menu 1: “stratum limits for synch alarm” for DCF time sources, the delay for this alarm is defined in chapter 6.5.6, menu 6: stratum TO (0-16) DCF/GPS loss”
LAN control lamps:			
left	green	blinking	Network activity
	orange	blinking	No connection to network
right	yellow	off	10 Mbit
		on	100 Mbit

4.2 LED indication back side



Description	Color	Status	Description
Init	green	blinking	default configuration set
		on	start-up process
		off	normal operation
DCF reception	red	blinking	DCF (GPS reception)

4.3 Operation elements



If the button is pushed for a long duration (min. 30 sec) during start-up or operation, the default configuration is set. Setting the default configuration is signalized through rapid blinking of the Init LED (>5 Hz) (only let go of the button after this starts).

Attention: The current configuration will be lost.

5 Installation

5.1 Connections

The connections are specified in Appendix "A Connection diagrams".

Only connect the designated devices to the various inputs and outputs.

5.2 Boot procedure of the Network Time Server NTS

The normal booting time of the NTS is approx. 60 sec. with pre-set IP or with DHCP. The end of the booting procedure is signalized by the Init LED. Without connection to a DHCP server, the first start up can take up to 75 seconds.

5.3 Firmware

It is recommended to install the current firmware on your device prior to the definite commissioning. The current firmware can be found under *www.mobatime.com* ➔ *Customer Data* ➔ *Product Ressources* ➔ *Time Server*.

5.4 First configuration

By default, the LAN interface is configured with the fixed IP address 192.168.46.46, the net mask 255.255.255.0 and the gateway 192.168.46.1 .

Caution: The network administrator must be consulted regarding settings on network devices!

Important: The firewall on the PC may have to be deactivated for the first configuration.

In case of problems, first check the connection to the NTS using Ping on the PC. Otherwise, the default configuration must be restored on the NTS according to Chap. 4.3.

5.4.1 First configuration using the default IP

To configure the NTS, a PC must be connected to the NTS either directly or over a switch (LAN / Ethernet cable RJ45). The PC must be brought into the same address range (e.g., 192.168.46.2). After that, the connection to NTS can be established by means of Telnet, SSH or MOBA-NMS.

Configuration IP address Microsoft Windows:
http://windows.microsoft.com/de-ch/windows7/change-tcp-ip-settings

5.4.2 First configuration ARP procedure

If the NTS was never configured before or the default configuration was restored, the ARP procedure can also be used:

1. Opening of a console: Windows with the command *cmd*
2. Assign a new IP address to the MAC address of the NTS (marked on the product label) using the Windows or Linux command **arp -s <IP address> <MAC address>**
   Example for Windows: *arp -s 192.168.0.190 00-0c-c6-77-f5-38*
   Example for Linux: *arp -s 192.168.0.190 00:0c:c6:77:f5:38*

3. The IP address is temporarily adapted to the NTS by means of the Windows command **ping –l 111 –t <IP address>** (l = small L) or the Linux command **ping –s 111 <IP address>**. The NTS should answer at least two ECHO requests.
   Example for Windows: *ping -l 111 -t 192.168.0.190*
   Example for Linux: *ping -s 111 192.168.0.190*
4. Perform the following within 60 seconds after Ping.
   Using the Windows or Linux command **telnet <IP address>**, the Linux command **ssh nts@<IP address>** or the application Putty, change the network settings of the NTS, e.g., *telnet 192.168.0.190*
5. Delete the ARP entry generated above using **arp -d <IP address>**
   Example for Windows or Linux: *arp -d 192.168.0.190*

5.4.3 First configuration IPv6

By default, NTS only has one link-local address that can be derived from the MAC address:
fe80::2[2nd position MAC]:[3rd position MAC]ff:fe[4th position MAC]:[5th position MAC][6th position MAC]

Example: MAC: 00:0c:c6:77:f5:38

IPV6: fe80::20c:c6ff:fe77:f538

Connection construction with Telnet **telnet <IP address>%<interface>**:
Example with Windows: *telnet fe80::20c:c6ff:fe77:f538%11*
Example with Linux: telnet *fe80::20c:c6ff:fe77:f538%eth0*

In Windows, the interface is called the Scope Zone or Scope ID and can be determined with the command "*netsh interface ipv6 show addresses.*"

Putty can also be used with Windows, where the connection can be readily created using the link-local address (Telnet or SSH):

In Linux, the connection with SSH can also be created by means of **ssh nts@<IP address>%<interface>**:
Example: *ssh nts@fe80::20c:c6ff:fe77:Ff38%eth0*

5.4.4 First configuration with MOBA-NMS

Using MOBA-NMS, unconfigurated NTS can be sought in a local net (same subnet) and the network settings can be set by means of the current network.

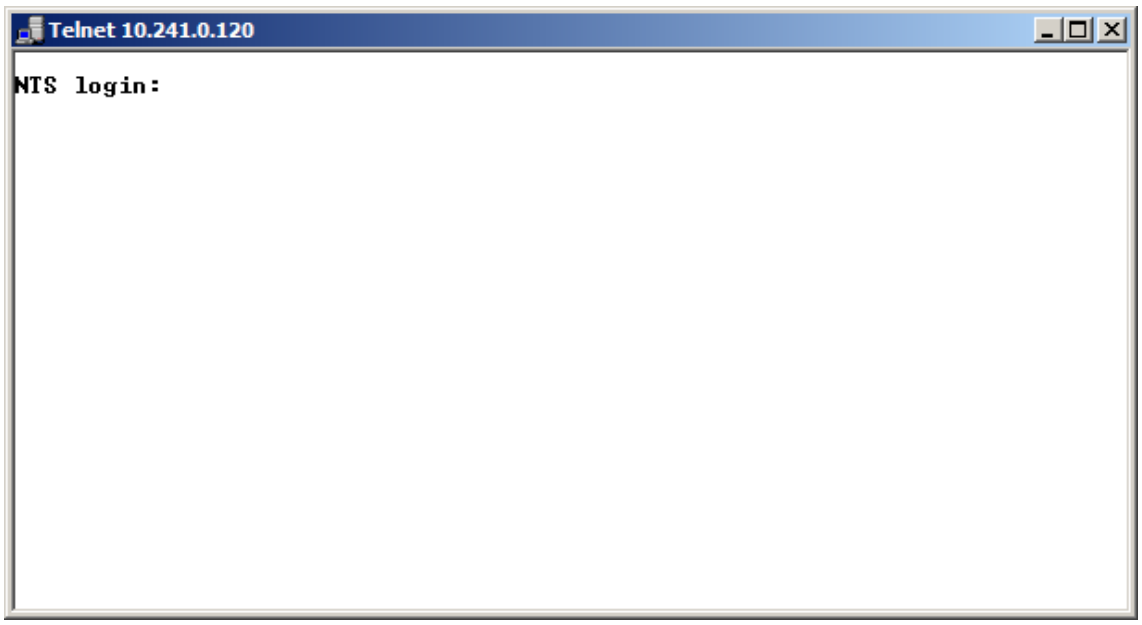
5.5 Basic settings (factory settings)

The basic settings can be found in the table in the attachment "F Parameters"

6 Operation

6.1 General

Operation occurs via MOBA-NMS, a terminal menu or SNMP. SNMP operation is explained in chapter “9 SNMP“. Operation with the terminal menu takes place either via Telnet or SSH. After a connection has been set up, the login screen is displayed:



To start the menu, n*ts* must be logged in as user. The standard password is *nts*. (Changing the password ➔ see chapter “6.5.13 General Settings“).

Only one menu can be open at any time. The first menu started has priority. The menu is automatically closed after 15 min. without operation, and any connection via Telnet or SSH is interrupted.

Backspace:

Backspace must be set to "delete“ with the serial terminal:

For example, for **Hyperterminal** under "File ➔ Properties ➔ Settings - Backspace sends DEL" must be selected.

Local echo:

Some terminals (serial or Telnet) do not display the characters entered. It is, therefore, necessary to switch on the "local echo" in the terminal.

6.1.1 Telnet

Windows 98, 2000, XP, Vista, Windows 7: Start ➔ Run ➔ *telnet [IP address]*
Password: **nts**
NetTerm (Shareware)

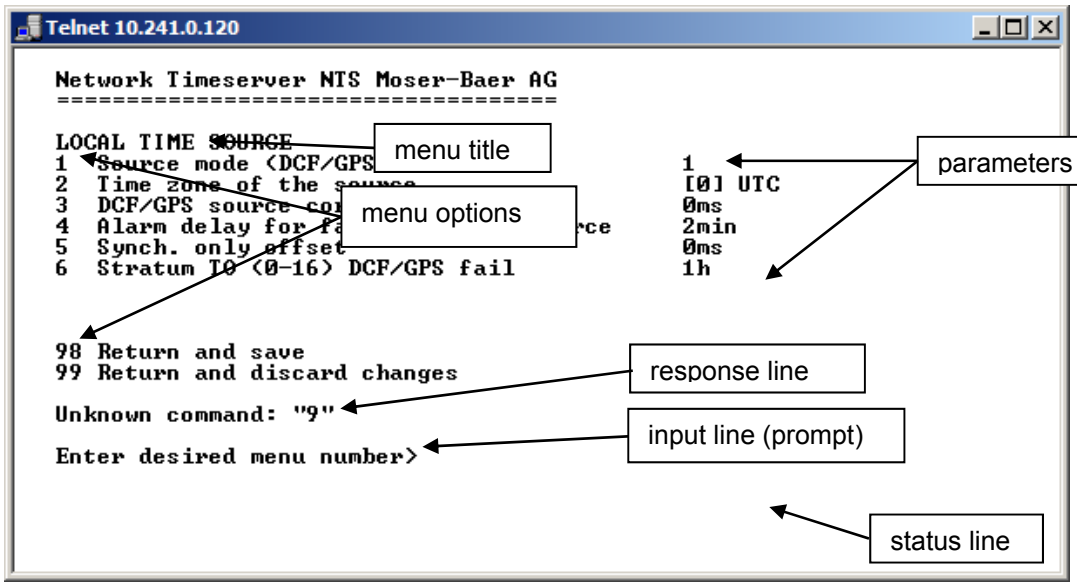
Linux: Start console and enter "*telnet [IP-address]*

6.1.2 SSH

Windows 98, 2000, XP, Vista, Windows 7: e.g. with Putty

Linux: Start console and enter "*ssh nts@[IP address]*"
Password: **nts**

6.1.3 Menu structure



The current menu is always displayed in the **menu title**. The **menu options** show all the selectable menu functions. Provided the menu item is not a further menu, the set **parameters** are displayed. Error messages (e.g. invalid entries) or additional information to the selected menu items are displayed in the **response line.** The **input line** shows the current input values or options possible. The **status line** only appears, when an information has to be displayed, e.g. "An alarm is active".

All entries must be completed with ENTER (Return) (e.g. also ESC).

The menu window can always be exited with *Ctrl-C* (incl. termination of the Telnet and SSH connection).
The desired menu can be selected with the relevant number.

The numbers 98 and 99 are always used identically:

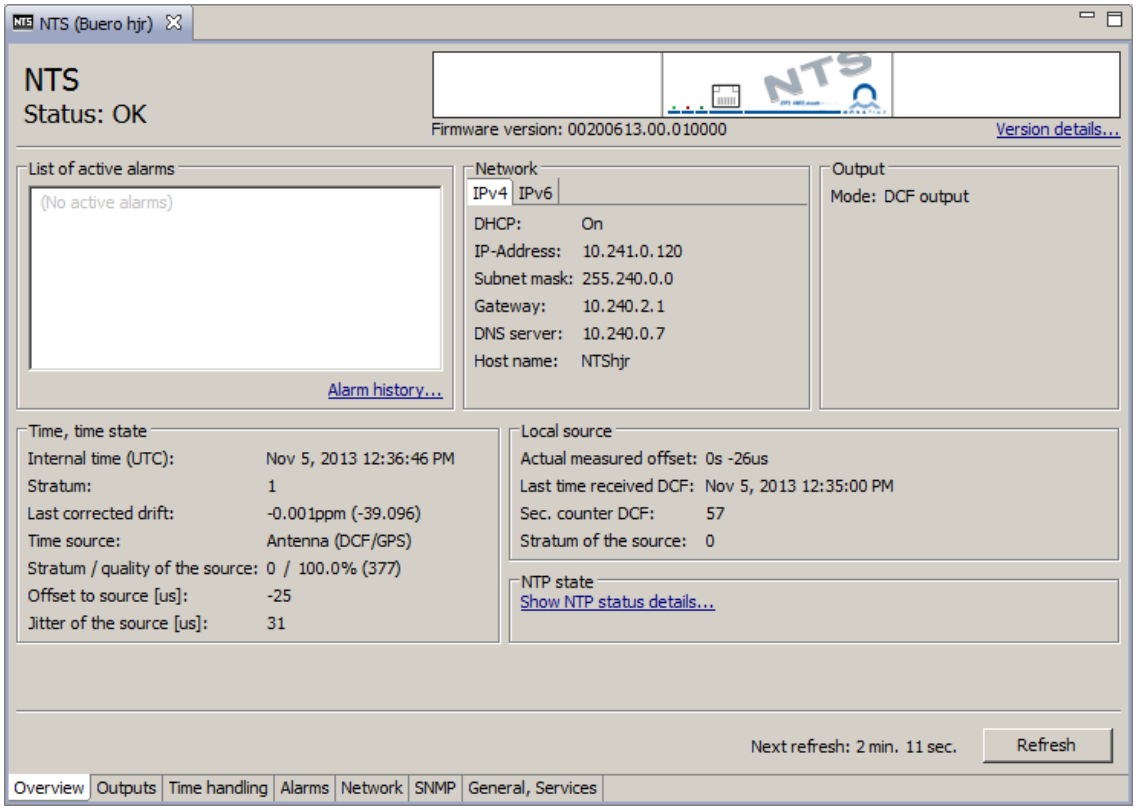
- With 98, the settings entered are saved and the menu exited. Depending on the change, the NTS, or only partial functions, are rebooted.
- With 99, all changes to the menu are reversed and the menu exited.
  In the menus where data cannot be saved (command 98), the menu is only exited with 99, but any changes are not saved.

The current menu is updated, without any further entry, with ENTER.

6.2 MOBA-NMS operation

For the configuration of NTS devices via GUI, MOBA-NMS (see chapter „3.7 MOBA-NMS - Network Management System“) can be used. All configuration possibilities are subordinated in different configuration pages (called „tabs“). These tabs are connected to the terminal menu and designated accordingly. Example: The terminal menu „Configuration ➔ Alarms“ can be found in MOBA-NMS under the tab „Alarms“.

Configuration example of a Network Time Server NTS:

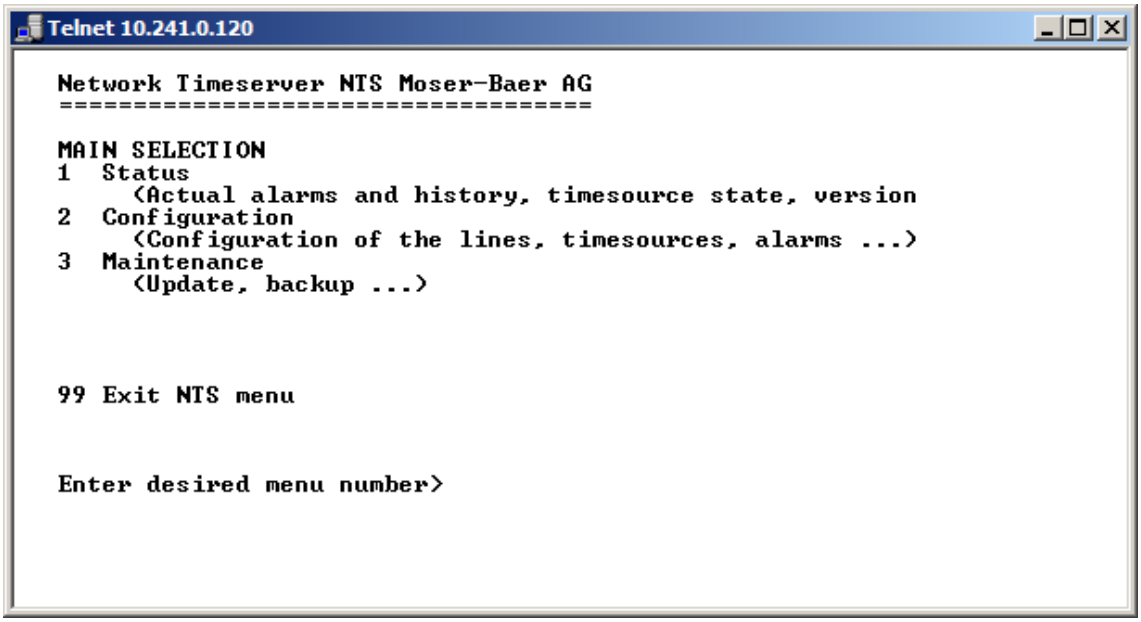


configuration pages (tabs)

For further details on the general MOBA-NMS operation, check the integrated online help (menu „Help ➔ Show help“).

Important: To enable the communication between MOBA-NMS and the NTS devices, SNMP must be activated! Set terminal menu „Configuration ➔ SNMP ➔ SNMP Mode“ to „on“. SNMP is activated by default.

6.3 Main menu



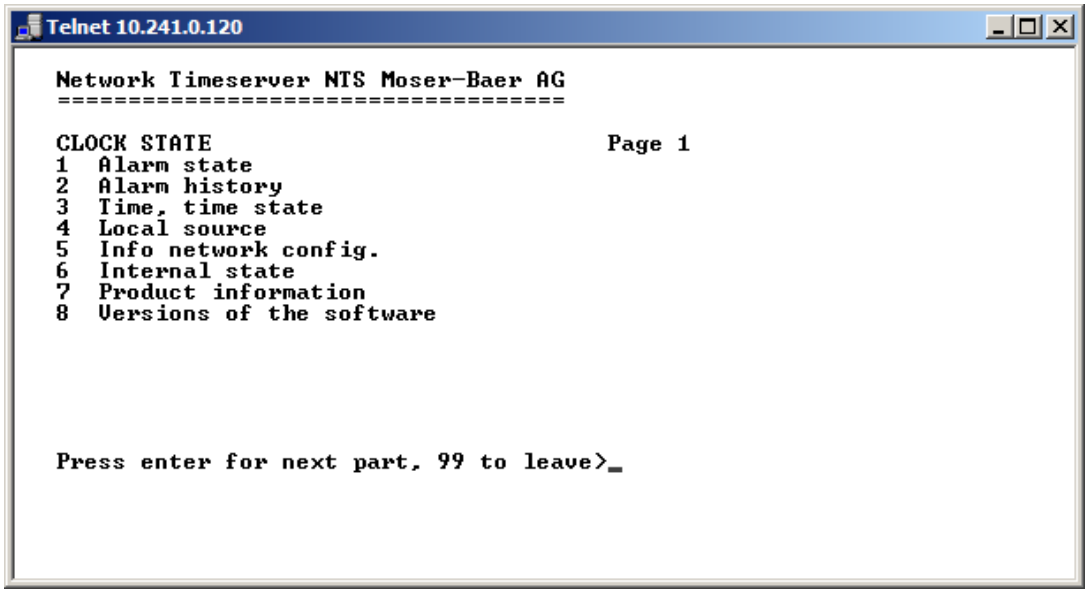
Menus:

Status:	Display of various information regarding operation and environment See chapter “6.4 Status Menu“
Configuration:	Configuration of the NTS See chapter “6.5 Configuration Menu“
Maintenance:	Software update, backup and restore See chapter “6.6 Maintenance Menu“

6.4 Status menu

The status menu consists of 2 pages.

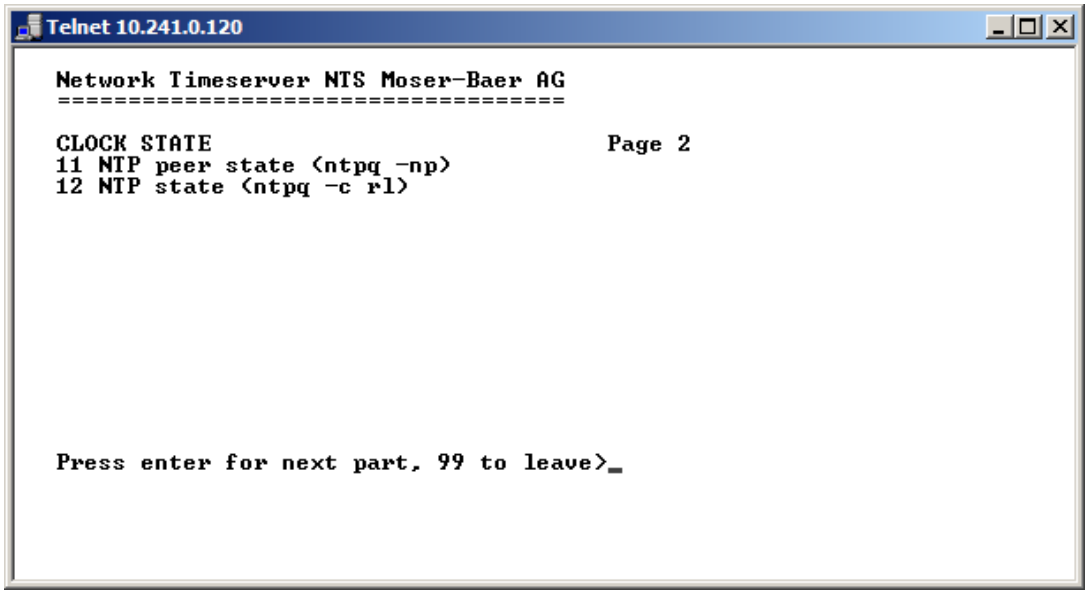
Status menu page 1:



The menu shows various information on the current operating status.

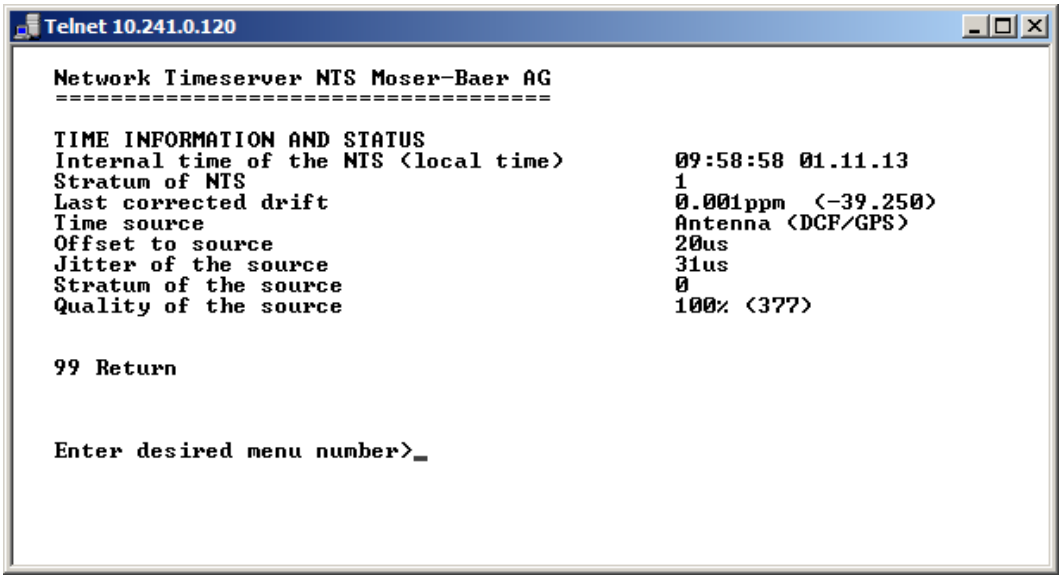
1. Requesting alarm status, display of all the NTS active errors.
   Display of the NTS alarms (64) on 4 pages. The ALARM DETAIL menu pages can be scrolled through with ENTER. Active alarms are displayed with a *. The ALARM DETAIL menu page can be exited with 99. All NTS active alarms are displayed, masking (e-mail, traps, relay) only occurs later.
2. Alarm history display.
   Display of the NTS alarm record, newest alarm first. The ALARM RECORD menu pages can be scrolled through with ENTER. The ALARM RECORD menu page can be exited with ESC.
3. Current time and status display. See chapter 6.4.1 Time Information and Status"
4. Time source information display. See chapter "6.4.2 Time Source Information"
5. Current network configuration display. With ENTER, a second page can be displayed with network information.
6. NTS system information display (internal status, regulation voltage of the quartz..). This information is for support purposes only.
7. Product information's like serial number, firmware version etc.
8. All several software versions of the NTS.

Status menu page 2:



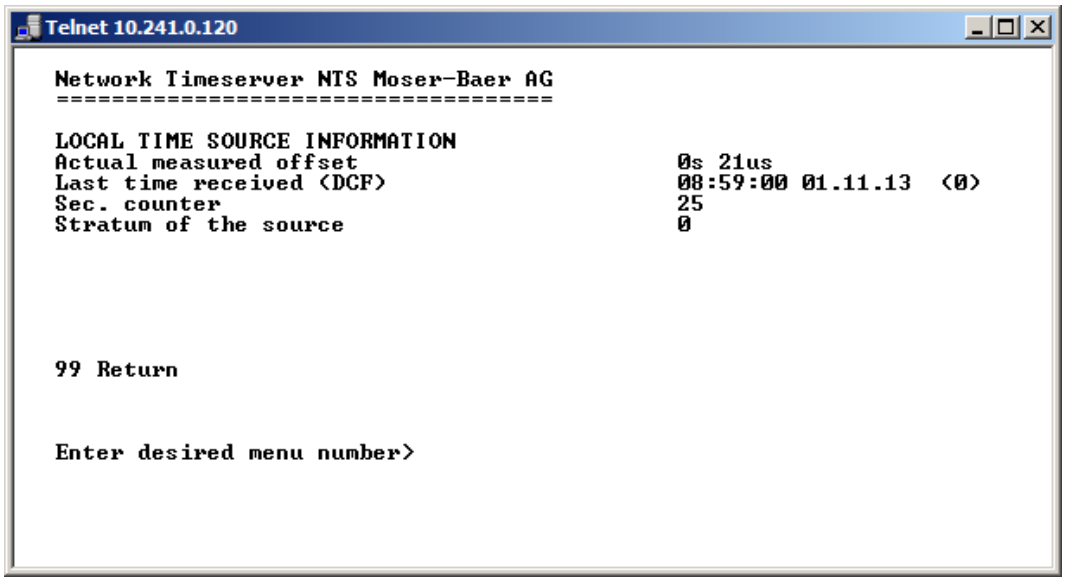
Display of information with regard to the internal state of the NTP server.

6.4.1 Time information and status



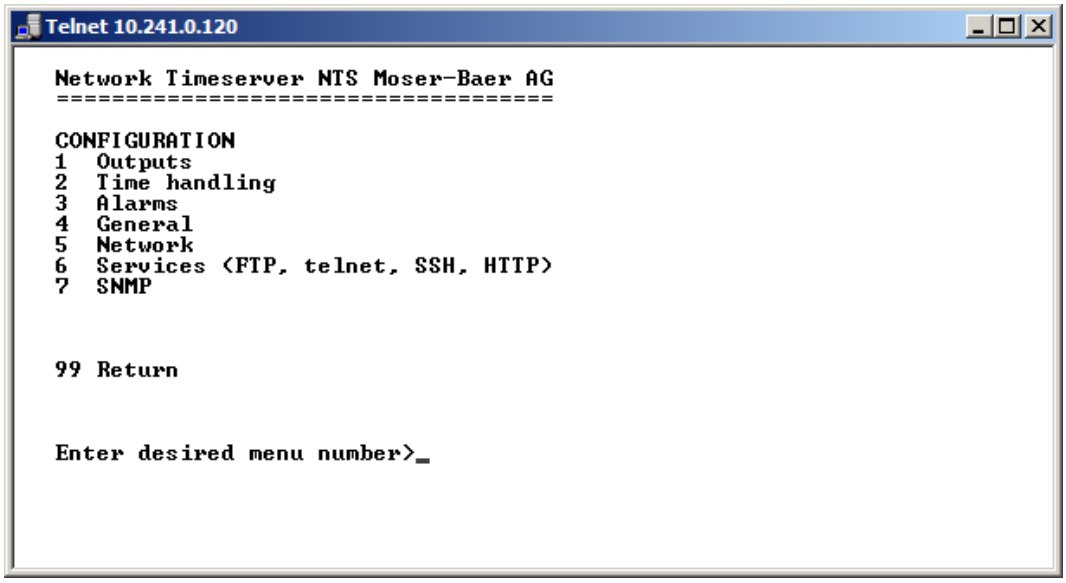
-Internal time of the NTS:	local time
-Stratum of the NTS:	current stratum
-Last measured drift:	drift before the last quartz correction in () frequency of NTP (for support only)
-Time source:	current time source
-Offset to source:	offset to source (source – system time)
-Jitter of the source:	current jitter
-Quality of the source:	quality of the source

6.4.2 Time source information



- Currently measured offset:	last measured offset
- Last time received DCF:	last time received from DCF source In () information about number of available satellites (only with GPS 4500 or GNSS 3000). With DCF, this value is random.
- Sec. counter DCF:	the counter is incremented by 1 with each DCF pulse. For the minute marker, the counter is set to 0.
- NTP source stratum:	stratum of the current source

6.5 Configuration menu



Configuring the NTS through various submenus:

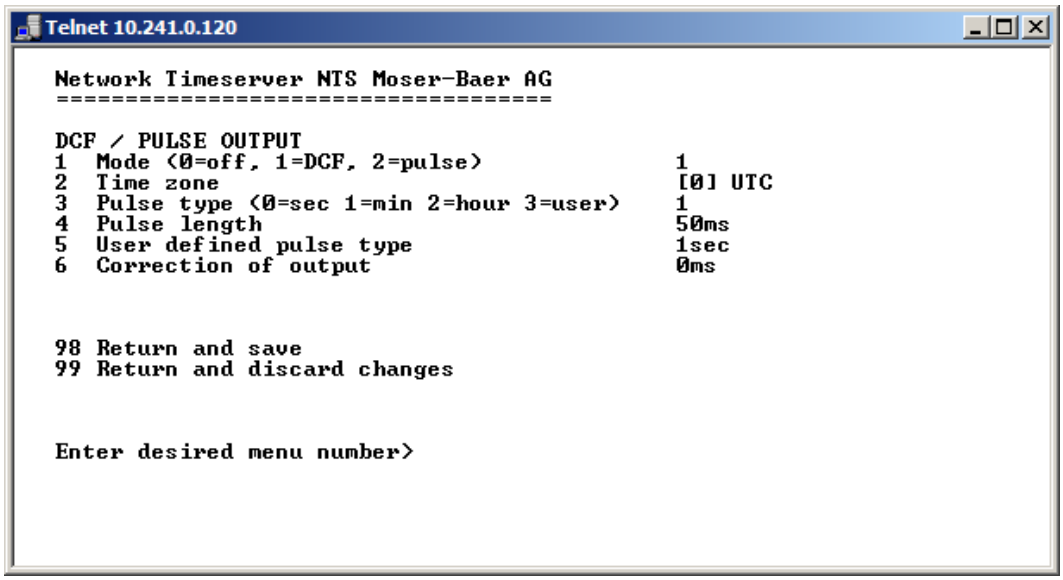
1. Configuring the lines / outputs (DCF out, RS 485 line and NTP slave clock line)
   See chapter "6.5.1 Lines"
2. Configuring the time source, time-keeping etc.
   See chapter "6.5.4 Time Administration"
3. Alarm settings (e-mail, SNMP)
   See chapter "6.5.9 Alarms"
4. General settings of the NTS (language, time zone for alarms and display, password for menu...)
   See chapter "6.5.13 General Settings"
5. Network Settings
   See chapter "6.5.14 Network"
6. Services (switching network services such as FTP, Telnet, SSH on or off)
   See chapter "6.5.15 Services (Network services FTP, Telnet, SSH....)"
7. SNMP Configuration for GET/PUT.
   See chapter "6.5.16 SNMP" (Traps are dealt with in menu ’2. Configuration’ ➔’3. Alarms’ ➔ ’3. Traps’. See also chapter 6.5.12 SNMP Traps)

6.5.1 Lines

Under lines, settings can be undertaken for the following functions:

- DCF / Pulse output 1 ➔ see chapter 6.5.2
- NTP slave clocks / time zone server ➔ see chapter 6.5.3

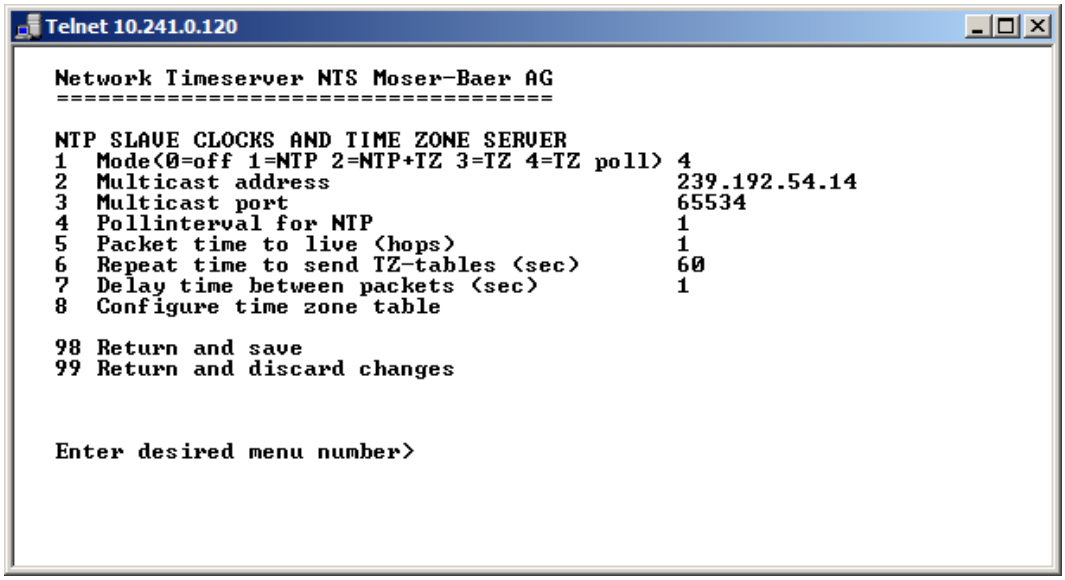
6.5.2 DCF / Pulse output



1. Select line function: Line switched off, line DCF output, line pulse output
2. Select time zone -> see chapter "6.5.19 Time zone selection"
3. Select pulse mode: every second, minute, hour or user-defined.
   (Only active with the pulse output function)
4. Select pulse length in ms (20-500ms)
   (Only active with the pulse output function)
5. User-defined pulse interval (1-3600 sec) only active with pulse type 3 (=user) (the value is also only then displayed). The pulse always occurs after a multiple of the pulse interval from the 0 second in the 0 minute, e.g.:
   – Pulse interval 960 sec. (16 min.)
   ➔ Pulse occurs: 00:00:00, 00:16:00, 00:32:00, 00:48:00, 01:00:00, 01:16:00 ...
   – Pulse interval 25sec
   ➔ Pulse occurs: 00:00:00, 00:00:25, 00:00:50, 00:01:15, 00:01:40, 00:02:05 ...
   ... 00:59:35, 01:00:00, 01:00:25 ...
6. Output correction (-500ms...+500ms)
7. Frequency (1…5000Hz)

6.5.3 NTP slave clocks / time zone server

NTP slave clock line for operating slave clocks on the LAN (Ethernet). With this clock line, a world time function can be realized.



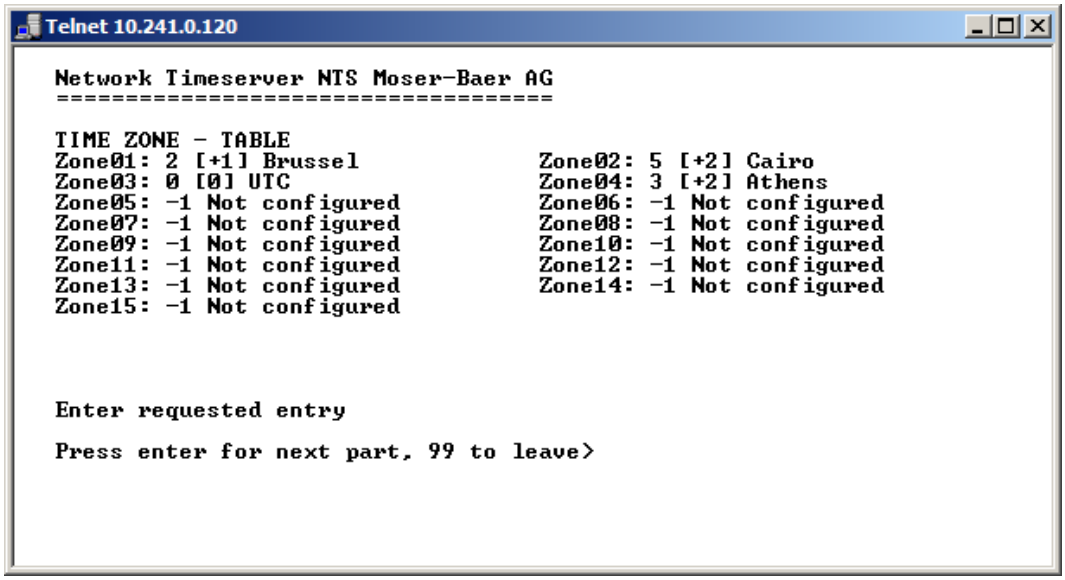
1. Mode of clock line: 0 = off, 1 = Send NTP multicast, 2 = Send NTP Multicast and Time zone table, 3 = Send Time zone table, 4 = Time zones on request, 5 (only for maitenance) = Send an empty Time zone table and return to previous mode.
2. Multicast adress for NTP and time zone server: **239.192.54.x**
   Group address: x = 1..15 for MOBATIME devices, e.g. NCI, SEN 40.
3. Multicast port for Time zone server (enter an arbitrary value, empty is not allowed ! Value e.g.: 65534). The port is also needed for requesting Time zone entries (mode 4).
4. Poll-interval for NTP Multicast in 2^**poll-values** in seconds (range: 1 – 16).
   E.g. poll-value = 2 ➔ interval: 2^2 = 4 sec., poll-value = 5 ➔ interval: 2^5 = 32 sec.
   For redundant Multicast time servers see remark next page.
5. Packet time to Live (TTL) for NTP- and time-zone-Multicast-packets in hops. (Number of Routers in a network to transfer the packets through; for simple network without routing, enter value "1", for 1 Router enter "2").
6. Repeat time to send time zone table: 10 – 86400 sec
7. Delay time between the sending of the individual time zone entries (one entry per Multicast packet) of the table: 1 – 60 sec.
8. Configuration of individual time zone entries. Displays menu “TIME ZONE TABLE“.

Notice: Changes of multicast-address, pollinterval and TLL lead to a **restart** of the NTP server.

Notice: For the operation of a **Multicast** communication (NTP and Time Zone Server) **the configuration of a gateway is required** (see chapter 6.5.14 Network). The gateway can be set manually or by using DHCP.
If there’s no gateway available, it’s possiible to set the own IP as gateway.

Notice: **Redundant Multicast time server:**
If in the same network two NTP server should send NTP with same Multicast IP address (redundancy), then the first time server has to be configured with a small **pollinterval** (e.g. 2 ➔ 4 sec.) and second time server with a large pollinterval (min. 100 x larger, e.g. 9 ➔ 512 seconds). As long as the first time server is sending NTP Multicast packets, the packets from second time server are ignored. This configuration is needed, to reach a defined situation for the end devices (the NTS with the more frequently NTP send rate gets higher priority for time reception).

Time zone table for the NTP slave clock line:



Display of all time zone entries (15) of time zone servers for NTP slave clock lines.

Choose a zone number to change selected zone.

Time zone selection (see chapter 6.5.19 Time zone selection).

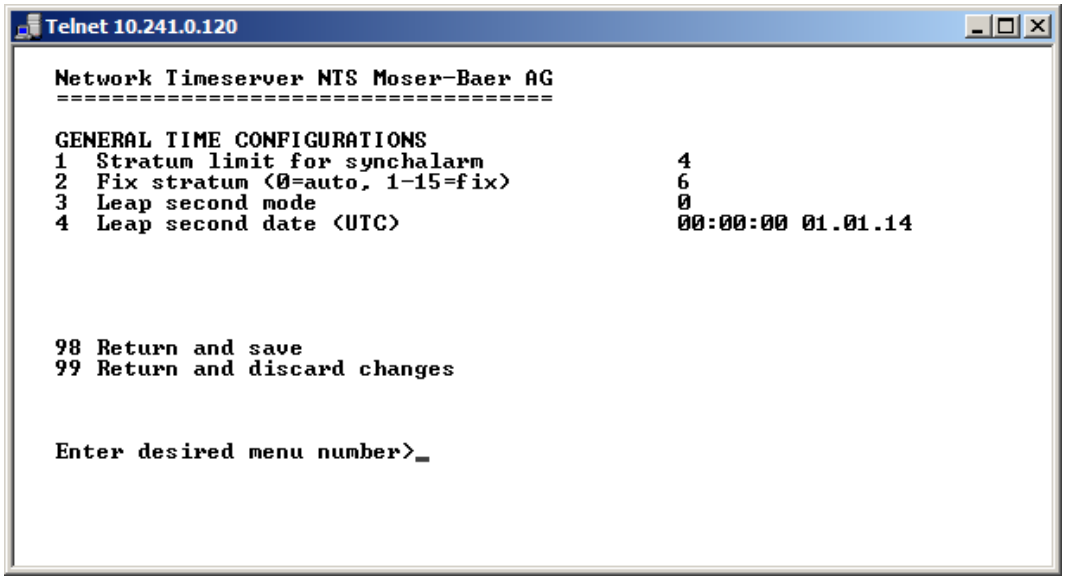
The page can be exited with 99. Changes are first stored or reset on the overlying menu page.

6.5.4 Time administration

Under time administration, settings can be undertaken for the following functions:

- General settings ➔ see chapter 6.5.5
- Local time source configuration ➔ see chapter 6.5.6
- NTP server / NTP sources ➔ see chapter 6.5.7
- For setting the time manually ➔ see chapter 6.5.8

6.5.5 General time settings



1. Stratum limits for Synchalarm:

   Stratum limits (1-16) for generating the alarm “Loss of time source str.”
   Standard value: 5
   Explanation:
   If the **stratum** of the NTS **equals** or is **larger** than the value “**Stratum limits for Synchalarm**,” the alarm “**Loss of time source str”** occurs after a fixed delay of 1 min. ➔ **Synch LED is turned off!**

2. Fixed stratum: 0 = Stratum is automatically calculated using the time source
   1 – 15 = Stratum of the NTS is set by means of the description in the table in Chapter “8.3 Fixstratum for local time source“

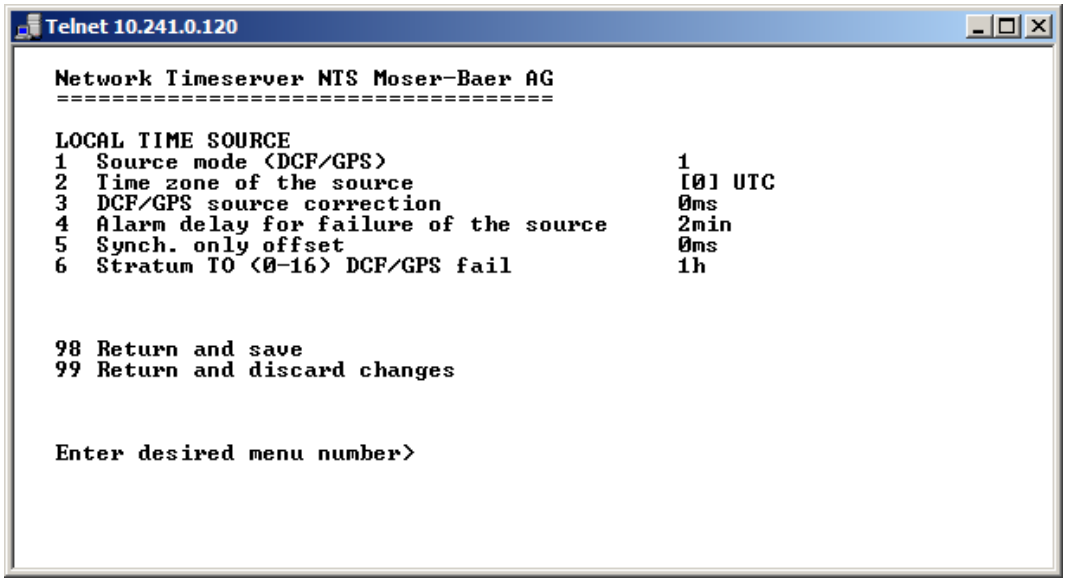
3. Leap second mode:
   0 off
   1 Additional second is inserted at the set point in time. Is set to 0=off after insertion of the leap second.
   -1 A second is left out at the set point in time. Is set to 0=off after insertion of the leap second.
   2 Recognize the leap second automatically. Only possible with a source with announcement of the leap second!

4. Set the point of time of the leap second in UTC using the format: “hh:mm:ss TT.MM.JJ“. The next conventional time is shown as a suggestion.

For a description of the leap second, see chapter “8.6 Leap second“.

6.5.6 Time source

Time source configuration "2 Configuration ➔ 2 Time management ➔ 2 Local time source".



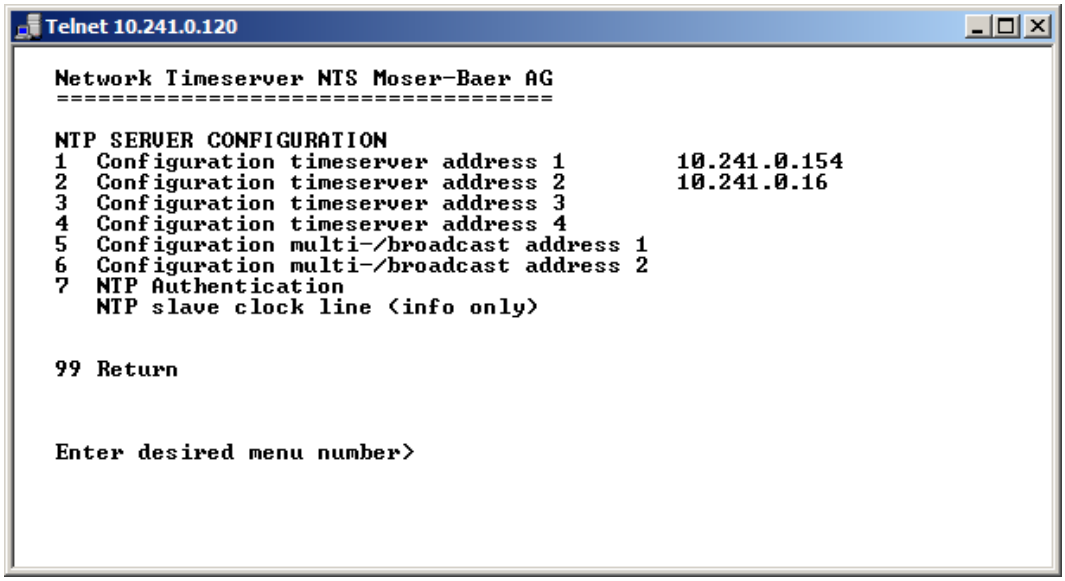
1. Type of time source: 0=off, 1=on
2. Time zone of the source: see chapter 6.5.19 Time zone selection
3. DCF/GPS source correction: (-60000ms..+60000ms)
4. Alarm delay at failure of time source (minutes):
   0 = off, 1-2'160min, default = 0
   Error: “loss of time source TO”
5. Synch. only Offset: 0=off
   100 – 5000ms=Limit from which the time is no longer transferred ➔ alarm “Syn only Diff too big”
6. Stratum TO (Timeout):
   Duration of stratum change 1 to 16 in the case of time loss (1-999h),
   e.g. 24 hrs ➔ stratum counts up from 1 to 16 within 24 hrs.
   Default value: 12h

For description of time source see chapter “8 Time Administration“

6.5.7 NTP server

NTP can run as server or combined as server/client.
To run NTP as source (NTP as client), in the menu ’2. Configuration’ ➔ ’2. Time handling’ ➔ ’1. Time source setting' choose NTP and set at least one server.
The exact behavior of NTP time sources is described in chapter "8.2 Time acceptance from NTP".

Further two multicast or broadcast addresses can be configured.



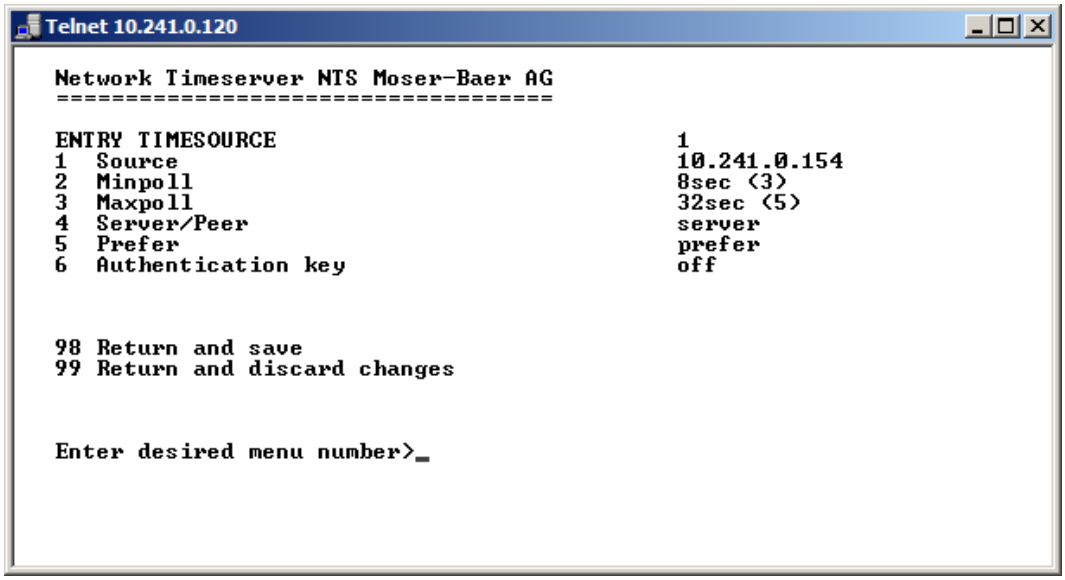
1.-4. Summary about configured NTP – time sources. Select to configure. Changes to the menu “TIME SOURCE ENTRY”.

5.-6. Summary about configured NTP – broadcast addresses. Select to configure. Changes to the menu “NTP MULTI-/ BROADCAST ENTRY”.

7. NTP Authentication: Changes to the menu “NTP AUTHENTICATION"

Information about a multicast – address, configured for NTP slave clocks.

Configuration of the individual server/peer address is as follows:



1. Insert time sources (IP address or name e.g. “ntp.metas.ch”
   ENTER without entry of an address will delete value.

2.-3. Configurations of Minpoll and Maxpoll: Inquiry interval 2^**poll value** in seconds.

   0 = automatically
   e.g. poll value=2 ➔ intervall 2: 2^2 = 4sec., poll value=5 ➔ intervall 5: 2^5 = 32sec.
   Range of poll values (exponent): 1 – 16
   To get a exact synchronization it’s better to limit Maxpoll to 6 (64 sec.).

4. Set type of inquiry: server or peer

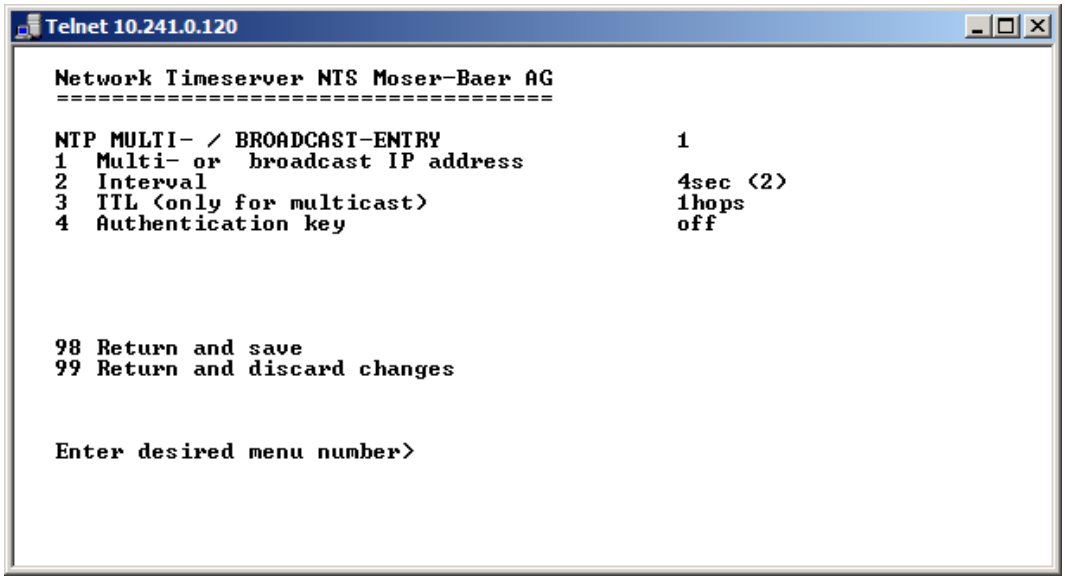
5. Preferred source: on or off
   If possible, a source is to be preferred (even if only one source is defined), unless DCF is active

6. Authentication key: off, key number, autokey

Notice: All changes lead to a restart of the NTP server.

Notice: Maxpoll should not be selected under 4 (16 sec), as otherwise, internal trimmung may be inaccurate.
Maxpoll and Minpoll on automatic can lead to insufficient synchronization accuracy. The specified accuracies were measured with Minpoll = 3 and Maxpoll = 6.
The configuration server should be used whenever possible.

Configuration of the Multi- / Broadcast address is as follows:

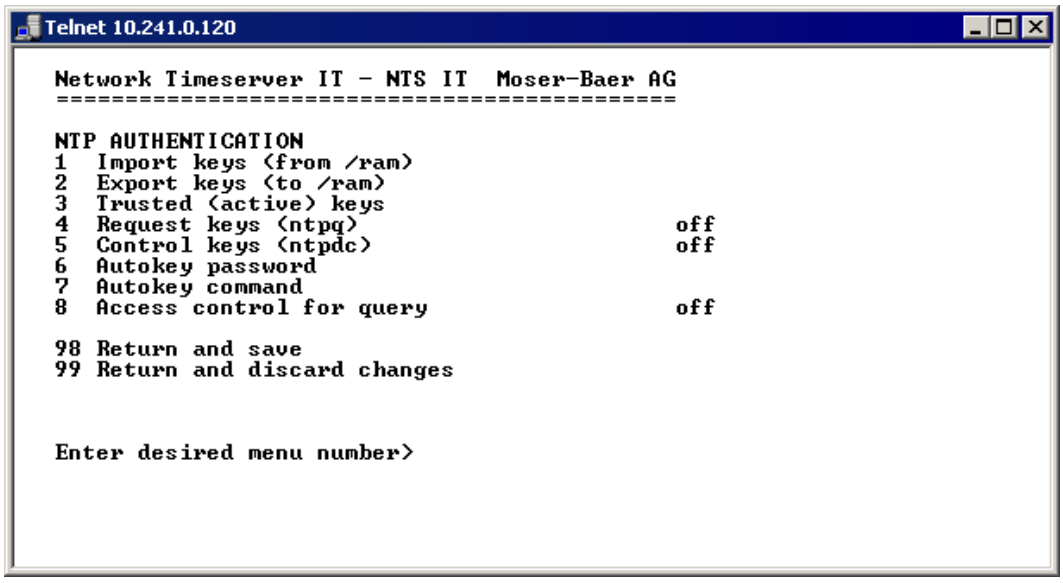


1. IP address of the destination network (multicast or broadcast).
   ENTER without entering an address will delete the entry.
2. Interval for sending out the NTP information in seconds.
   The interval is rounded after the entry to NTP standard, which only permits values of format 2^x: 1,2,4,8,16,32,64. Maximum 65536 seconds.
3. TTL (time to live) in hops. Only required for multicast.
   Number of routers over which the multicast packet should be transmitted: for simple networks without a router - enter 1, for 1 router - enter value 2.
4. Authentication key: off, key number, autokey

Notice: All changes lead to a restart of the NTP server.

Configuration of the NTP authentication:

The NTP authentication is described in chapter “8.7 NTP authentication“.



1. Import keys (from/ram directory)
   The file ntp.keys must first be copied into the directory /ram.

Notice: The file must be named exactly in this way and written entirely in small letters.

2. Export keys (to /ram directory)
   The current ntp.keys file is written in the directory /ram.
3. Select the trusted keys separated by commas or space
4. Select the request key
5. Select the control key
6. Set the auto key password
7. Execute for auto key commands:

gen_iff	generate the IFF certificate
gen_gq	generate the GQ certificate
gen_mv	generate the MV certificate
gen_all	generate all (IFF,GQ,MV) certificates
gen_client	generate the client certificate
update_server	update the server certificate
update_client	update the client certificate
export_iff	export the IFF server certificate to /ram. Parameter password of the client
export_gq	export the GQ server certificate to /ram.
export_mv	export the MV server certificate to /ram.
import_iff	import the IFF server certificate from /ram.
import_gq	import the GQ server certificate from /ram.
import_mv	import the MV server certificate from /ram.
clear_ram	delete the certificates in /ram
clear_keys	delete the certificates in the NTP key directory

   Example: *export_iff myPassword* exports the IFF client certificate to /ram.

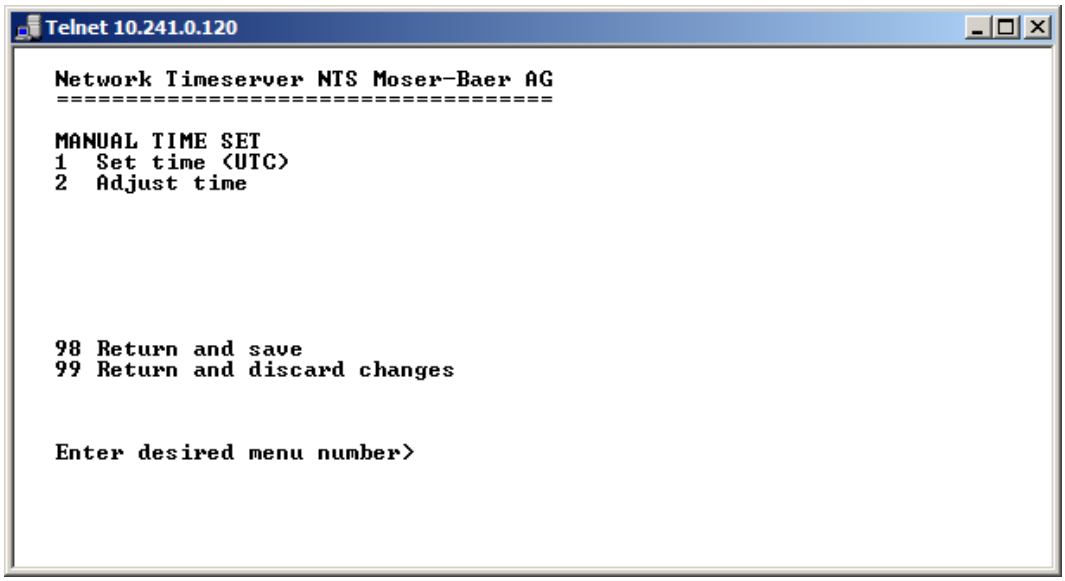
*The MV scheme is not currently available!

8. Access control for query (ntp-query)
   0 = all access (default)

1 = access from local network allowed
2 = all access blocked

6.5.8 Manual time setting

Menu: '2 Configuration ➔ 2 Time management ➔ 4 Set time manually'.



1. Set UTC time in the format “hh:mm:ss DD.MM.YY “.
   Time is set with ENTER!
2. Correct time in ms (- = backwards). Range: +/-10'000ms
   Time is set with ENTER!

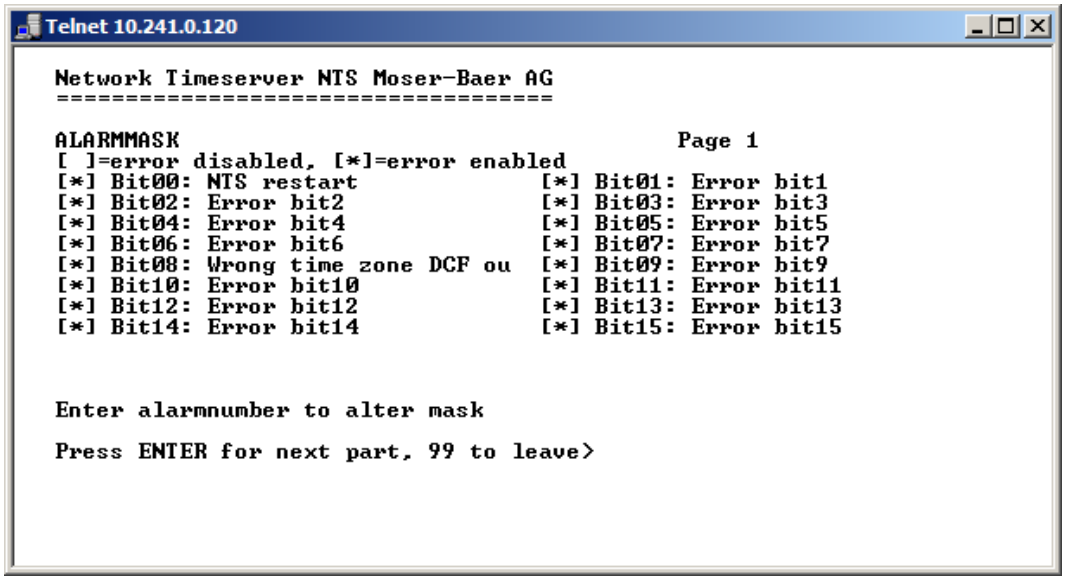
6.5.9 Alarms

Under alarms, settings can be undertaken for the following functions:

- E-Mail ➔ see chapter 6.5.11
- SNMP traps ➔ see chapter 6.5.12

Additionally, the alarm mask for the alarm LED and the alarm display can be configured in the menu.

6.5.10 Alarm mask



Display of all the NTS alarms (64) on 4 pages. Pages can be scrolled through with ENTER.

An alarm on the current page can be switched on or off by entering an error number. The page can be exited with 99. The modifications will be saved or restored one menu level higher in “ALARM CONFIGURATION“. All Alarms with “error bitxx“ are not yet used.

A description of individual errors can be found in appendix "C Alarm list".

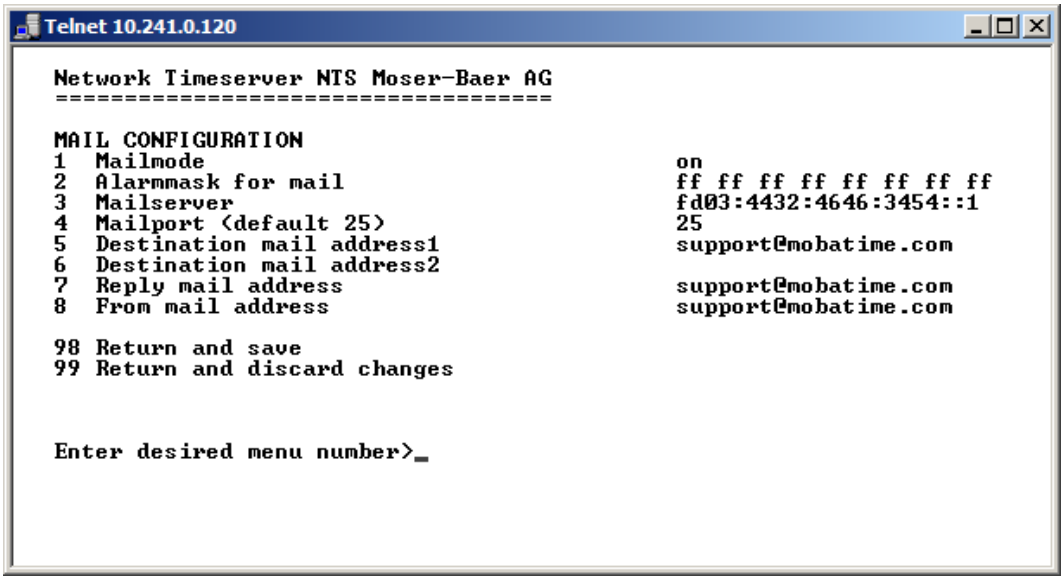
The alarm masks for the various applications (E-Mail, SNMP, SNMP Traps, alarm relay) can differ.

The alarm masks are only valid for the corresponding function, but not for the internal alarm record (menu ‘1 Status’ ➔ ‘1 Alarm status’ and menu ‘1 Status’ ➔ ‘2 Alarn record’).

6.5.11 E-mail

E-mail alarm notifications over SMTP .

E-mail configuration page 1:



1. E-mail function on or off.
2. Alarm mask for e-mail notifications (see chapter "6.5.10 Alarm Mask") Changes are stored or reset on the overlying menu page “MAIL CONFIGURATION“.
3. IP address of the mail server e.g. 10.249.34.5
   ENTER without entering an address will delete the entry.
4. Mail server port (often 25)

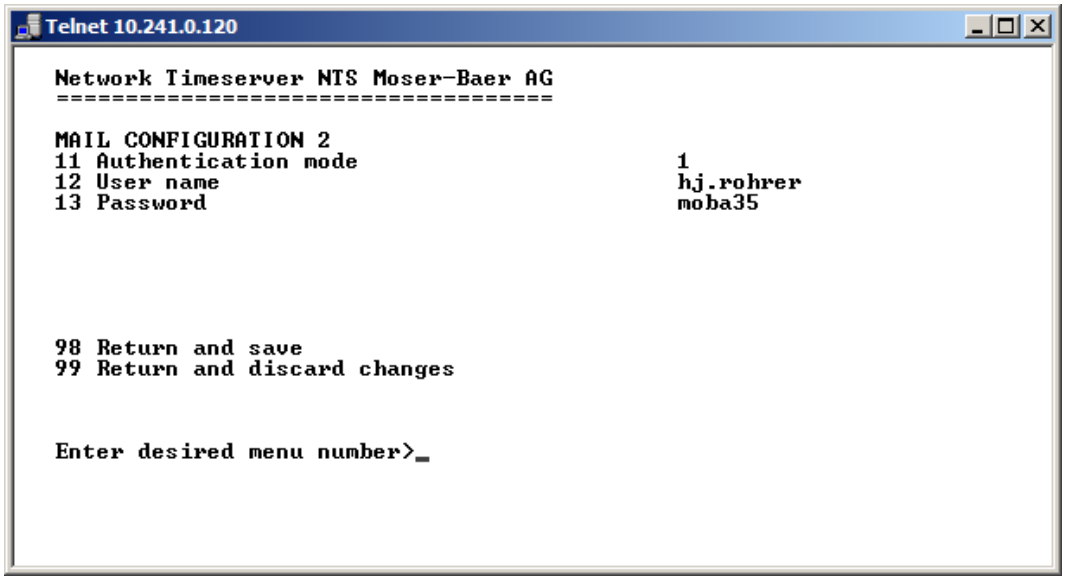
5.-6. Destination e-mail address.
   ENTER without entering an address will delete the entry.

7. Reply address (e.g. support, administrator...)
   ENTER without entering an address will delete the entry.
8. Sender address (important for authentication through the mail server)
   ENTER without entering an address will delete the entry.

Press ENTER to change to page 2.

Notice: Configuration of a gateway is required for sending e-mails (see chapter "6.5.14 Network"). This can be set via DHCP or manually.

E-mail configuration page 2:



11. Authentication mode:
    0=off (sender e-mail address used for authentication)
    1=auto (tries CRAM-MD5, LOGIN- PLAIN in this sequence)
    2=PLAIN
    3=LOGIN
    4=CRAM-MD5
12. User name (only for authentication mode 1-4)
13. Password (only for authentication mode 1-4)

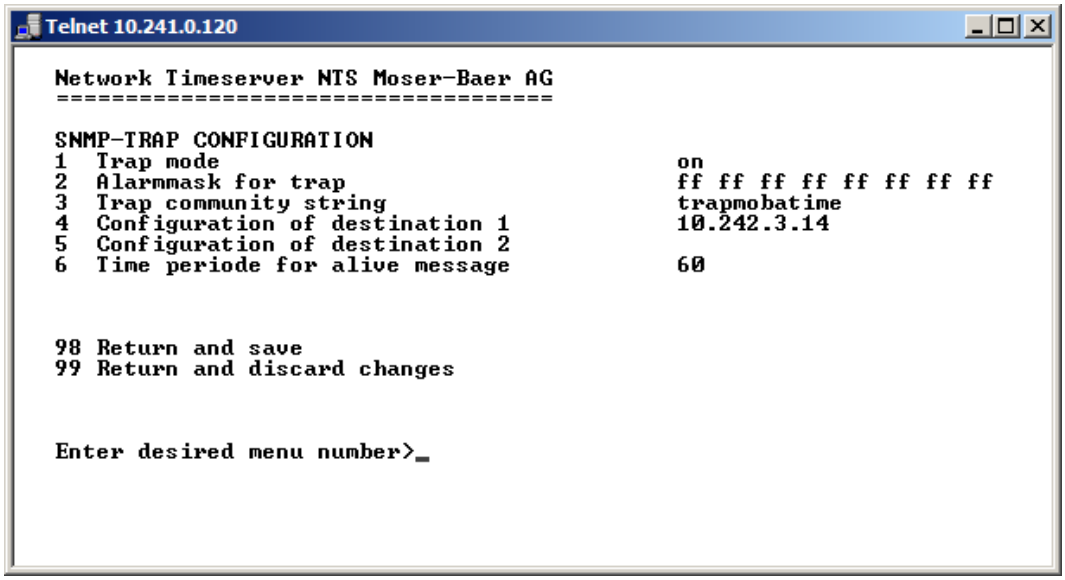
Press ENTER to change to page 1.

Format of an error message via e-mail:

```
Event <Alarm 03 set: Power failure 1>
Time <11:26:45 10.01.07>
Hostname <NTS (10.241.0.30)>
```

6.5.12 SNMP traps

For a description of SNMP functionality, see also chapter “9 SNMP“.



1. Trap mode on or off
2. Alarm mask for SNMP trap messages (see chapter "6.5.10 Alarm Mask") Changes are first stored or reset on the overlying menu page “SNMP TRAP CONFIGURATION“.
3. Trap community string (group membership for traps). Standard: *trapmobatime*.
4. Configuration of the receiving system (trap sink) 1
5. Configuration of the receiving system (trap sink) 2
6. Time period for alive messages in seconds. 0 = no alive traps are sent Range: 1-7'200sec

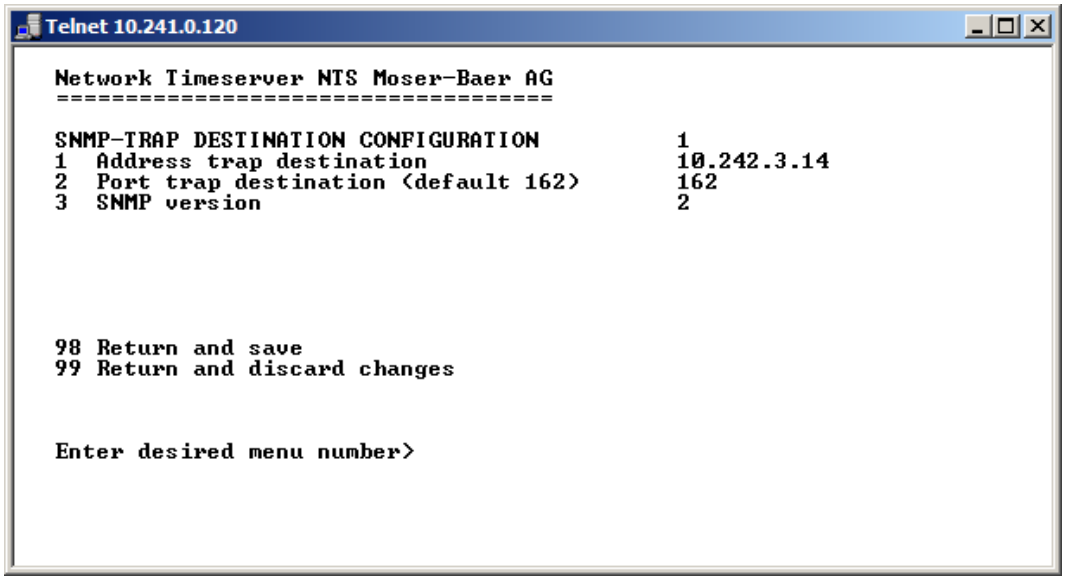
Notice: General settings for SNMP can be found in menu ’2. Configuration’ ➔ ’7. SNMP’. See also chapter "6.5.16 SNMP").

Notice: Configuration of a gateway is required for sending SNMP traps (see chapter "6.5.14 Network"). This can be set via DHCP or manually.

Notice: Each configuration change leads to a restart of the SNMP NTS Agent.

Notice: In order to send traps, SNMP must be activated!

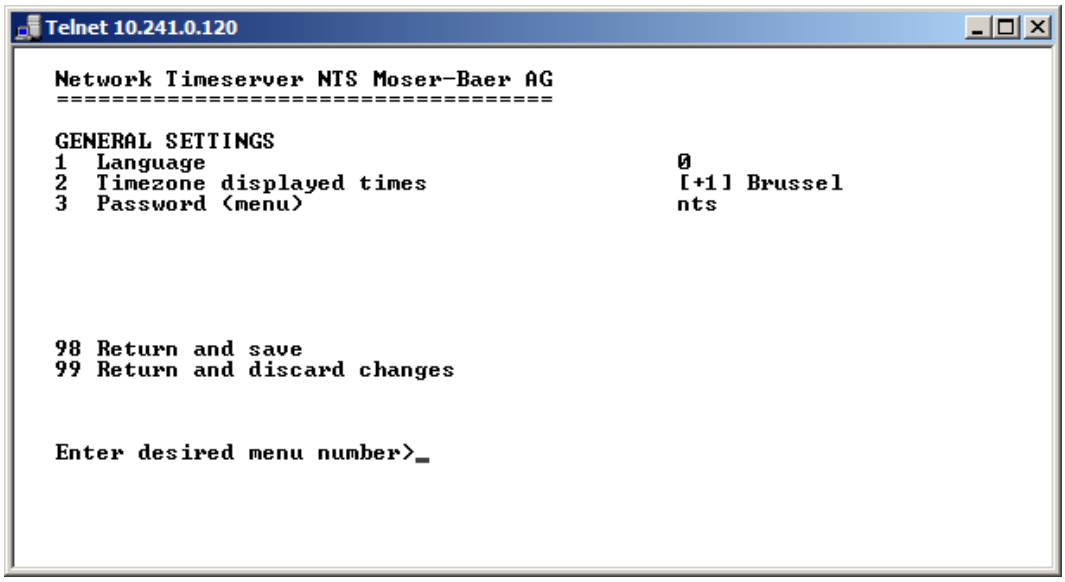
Configuration of the receiving systems



1. Address of the evaluation system e.g. 10.240.2.14.
   ENTER without entering an address will delete the entry.
2. Port of the evaluation system (usually 162).
3. SNMP Version: 1=SNMP V1, 2=SNMP V2c

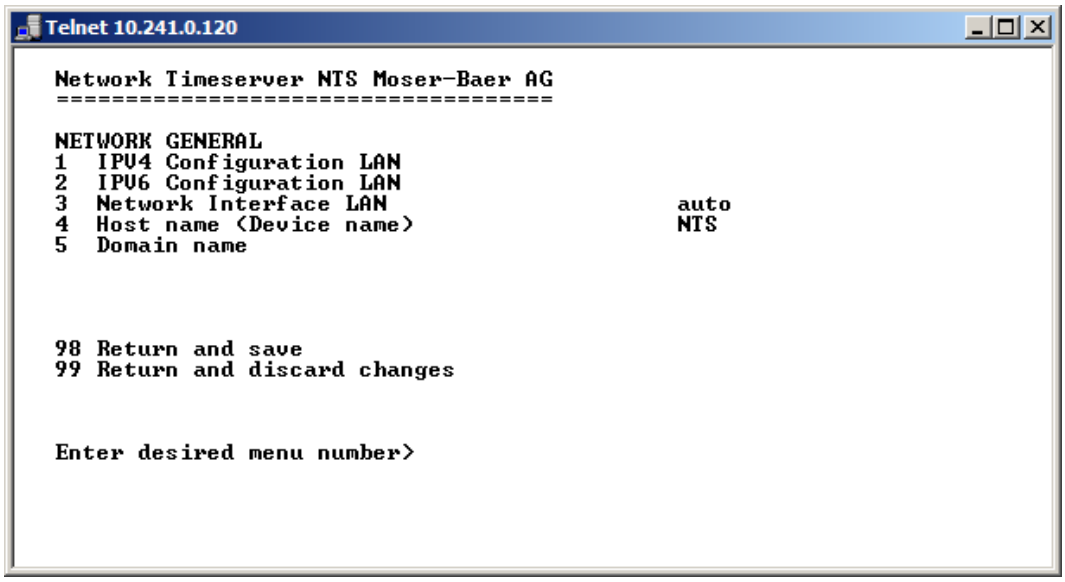
Notice: Each configuration change leads to a restart of the SNMP NTS Agent.

6.5.13 General settings



1. Setting the display language
2. Setting the time zone for the display, and also all alarm logs, e-mail and SNMP. (See chapter 6.5.19 Time zone selection)
3. Enter password for the menu (user ***nts***) (max. 15 characters).
   A password must be configured.

6.5.14 Network



1. Configuration of IPV4 parameters
2. Configuration of IPv6 parameters
3. Set network interface: auto, 100/10Mbit, half, full duplex
4. Set host name.

Notice: **A host name must always be configured.**
Host names and their format are described in the Internet standards RFC 952 and RFC 1123:
Domains and host names may only contain letters (capitals or small letters) and numerals ("0-9"). In addition, the minus sign ("-") may also be used, as long as it is not at the end.
Everything else is not permitted!

5. Set domain e.g. test.org

View of the current network state in Menu: '1 Status' ➔ '6 Info network config.'

Notice: The menu is closed upon modifying the IP or the DHCP mode.

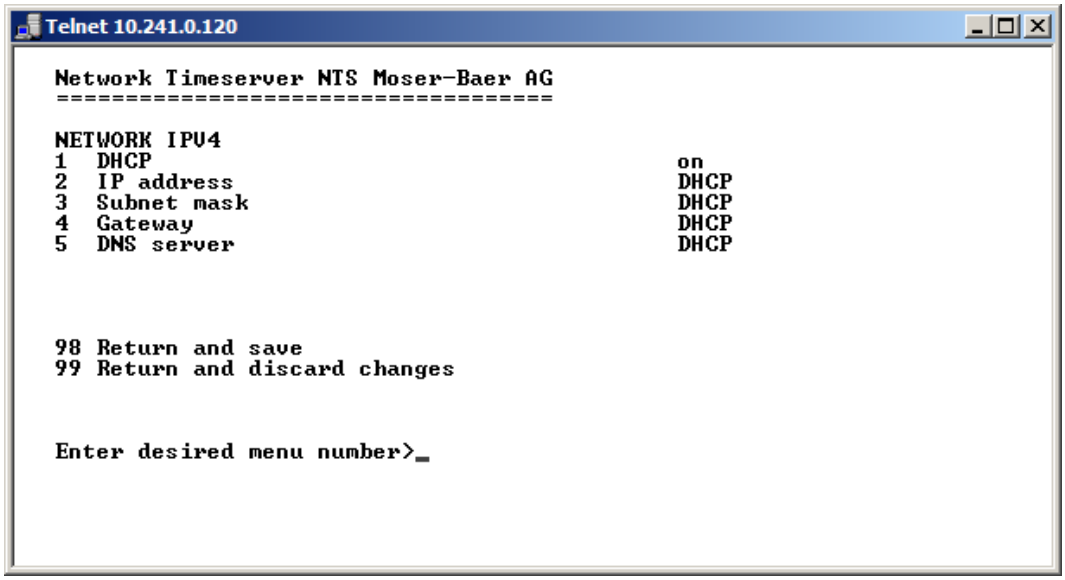
Notice: DHCP on/off, each change of this setting will result in a **restart** of the NTP server!

Notice: For the operation of a **Multicast** communication (NTP and Time Zone Server) **the configuration of a gateway is mandatory**. The gateway can be set manually or by using DHCP. If no gateway is available, the own IP address can be used.

Notice: Only one DNS server should be configured (IPv4 or IPv6).

Notice: Modifications to the network must be coordinated with the network administrator!

Network configuration IPv4:

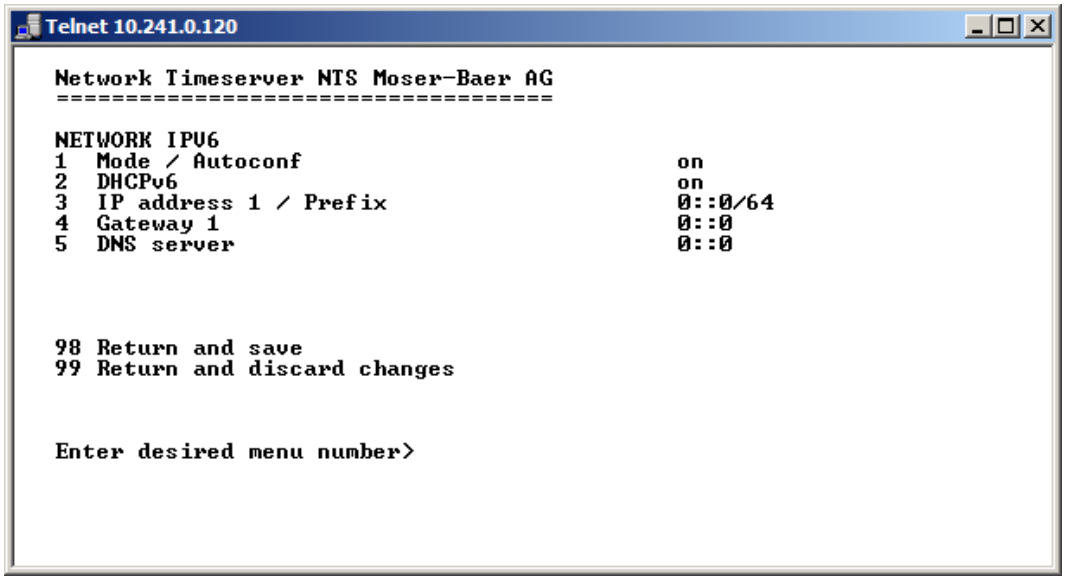


1. DHCP on or off, the following fields are not available in case of DHCP = on.
   A DHCP **renew** can also be triggered via this point.

Notice: DHCP on, if no DHCP server is available, leads to longer start-up time (<75 sec.) of the NTS.

2.-5. Set IP address, subnet mask, gateway and DNS-Server. Format = 10.240.98.7

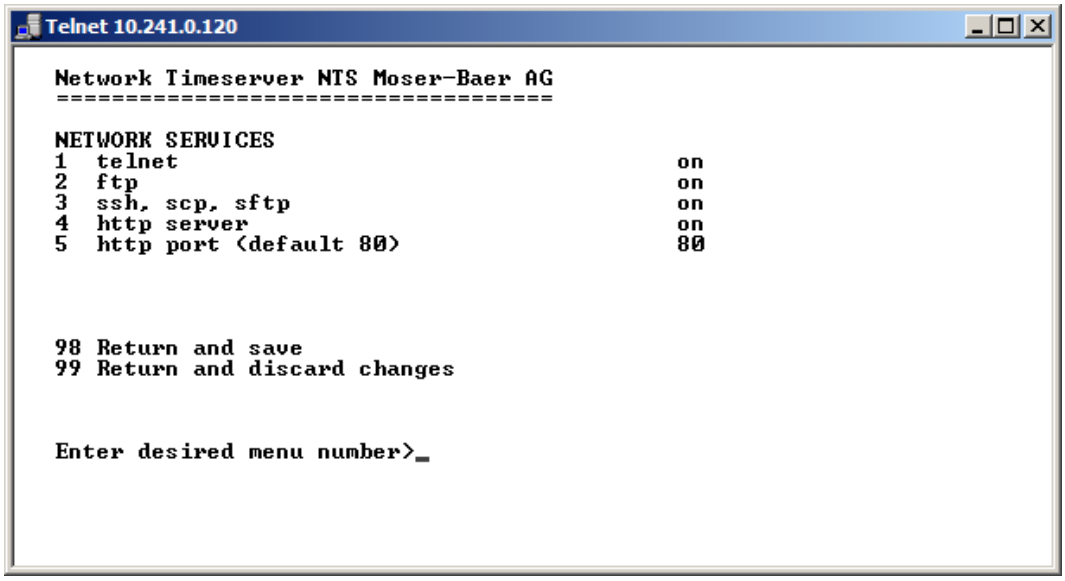
Network configuration IPv6:



1. Autoconf on or off
2. DHCPv6 on or off
3. IP address with prefix in IPv6 format
   e.g. 2001:2345:6789::12:1:34/64
4. Gateway in IPv6 format
5. IPv6 DNS server

6.5.15 Services (network services FTP, telnet, SSH...)

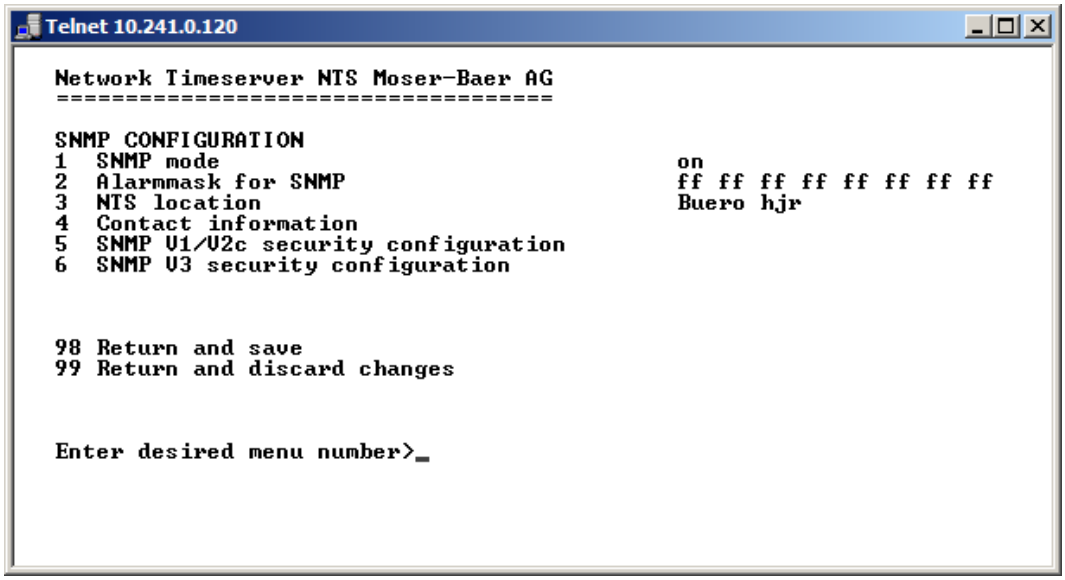
Network services configuration:



1.-4. Switch the individual services off or on.

6.5.16 SNMP

For a description of SNMP functionality, see also chapter “9 SNMP“.



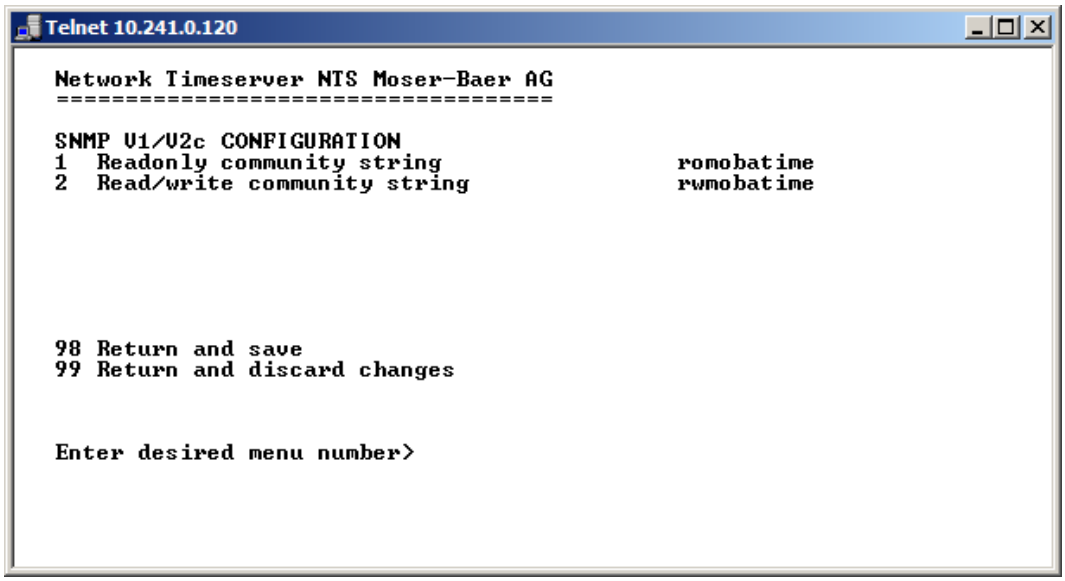
1. Mode. 0=off, 1=on. SNMP information of MIB 2 is always available.

Notice: To send out MIB-2 traps, the trap community and the destination address must at least be configured in menu ’2. Configuration’ ➔ ’3. Alarms’➔ ’3. Traps’. See also chapter “6.5.12 SNMP Traps")

2. Alarm mask for SNMP status (see chapter "6.5.10 Alarm mask"). The modifications will be saved or restored one menu level higher in “SNMP CONFIGURATION“.
3. Location information, which is displayed in SNMP management tool.
4. Contact information, which is displayed in SNMP management tool.
5. Configuration of SNMP V1 / V2c (specific settings). See chapter "6.5.17 SNMP V1 / V2c"
6. Configuration of SNMP V3 (specific settings). See chapter "6.5.18 SNMP V3"

Notice: Each configuration change leads to a restart of the NTS SNMP Agent.

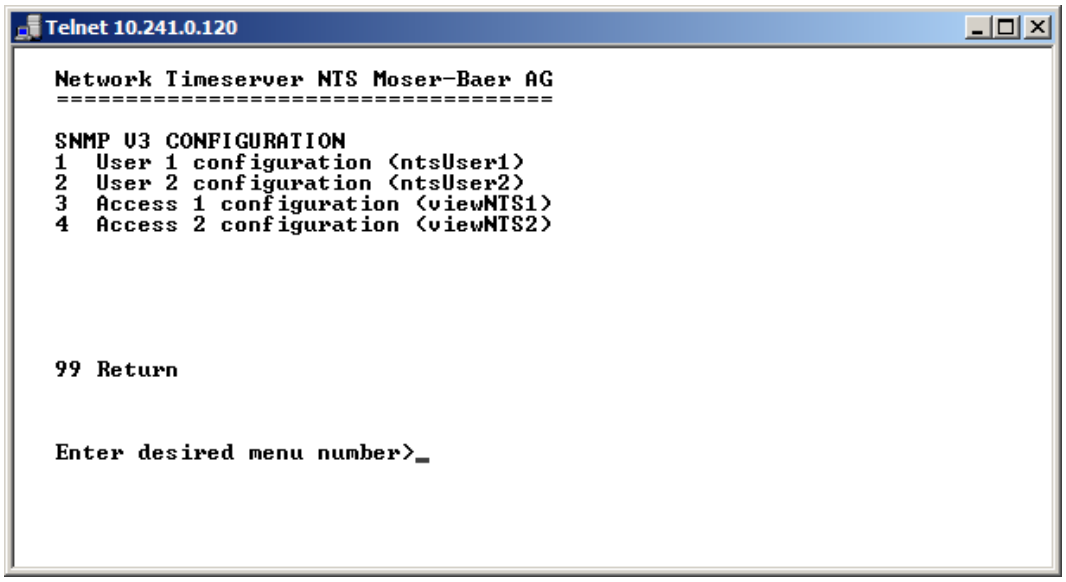
6.5.17 SNMP V1 / V2c



1. Community string for **read only** (Group membership for GET).
   Standard: *romobatime.*
2. Community string for **read/write** (Group membership for GET/PUT).
   Standard: *rwmobatime.*

Notice: Each configuration change leads to a restart of the NTS SNMP Agent.

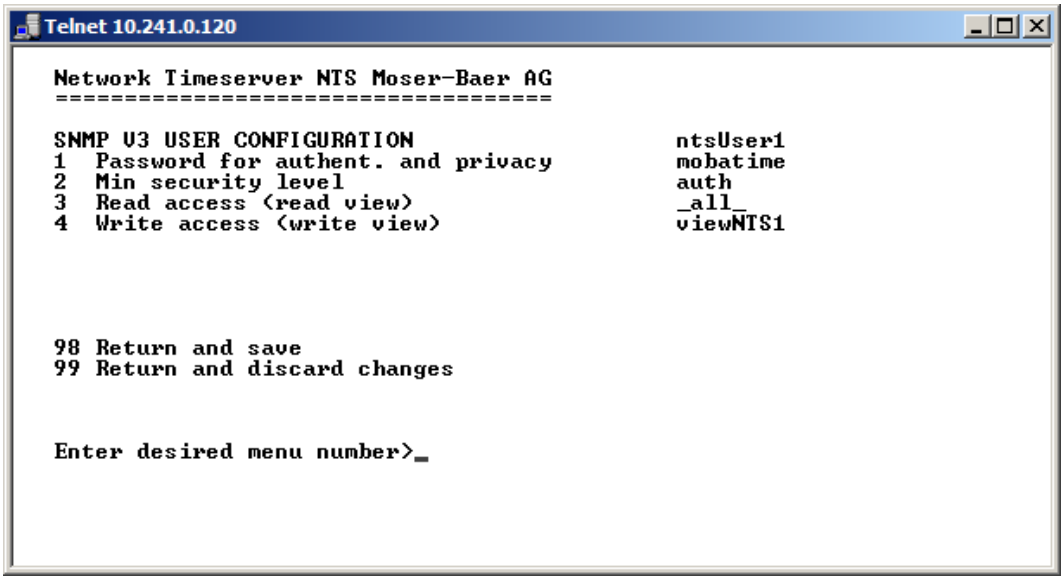
6.5.18 SNMP V3



1. – 2. Configuration of user-defined SNMP accounts ntsUser1 and ntsUser 2
3. – 4. Configuration of user-defined SNMP access rights viewNTS1 and viewNTS2

Notice: Each configuration change leads to a restart of the NTS SNMP Agent.

User configuration SNMP V3:



1. Password for authentication (MD5) and privacy (DES). 8 – 40 characters.

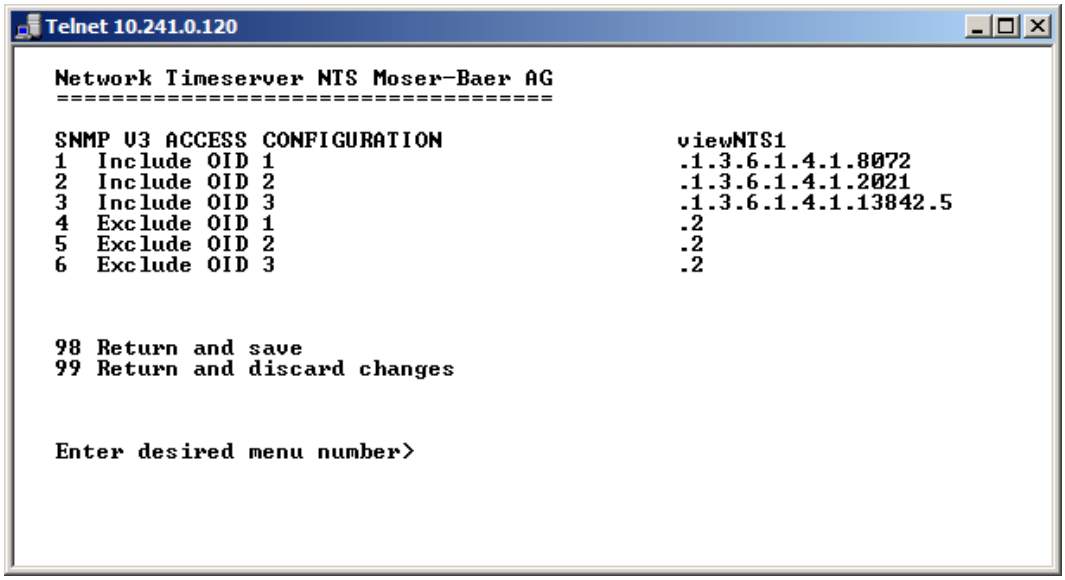
2. Minimal security level: 1=noauth (no authentication)
   2=auth (only authentication)
   3=priv (authentication and privacy)

3. SNMP read access: 0=none (no access)
   1=all (full access)
   2=NTS info (only NTS specific information)
   3=user defined 1 (viewNTS1)
   4=user defined 2 (viewNTS2)

4. SNMP write access 0=none (no access)
   1=all (full access)
   2=NTS info (only NTS specific information)
   3=user defined 1 (viewNTS1)
   4=user defined 2 (viewNTS2)

Notice: Each configuration change leads to a restart of the NTS SNMP Agent.

Access configuration SNMP V3:

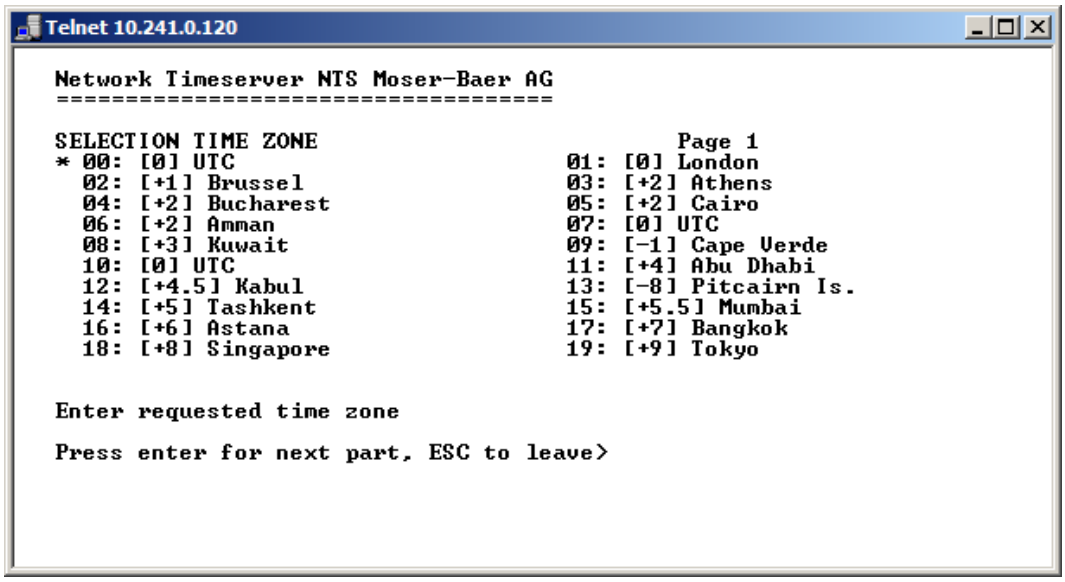


1. – 3. Include View path, form: *.1.3..6.1.4.1.13842.4* (e.g. NTS) or *.iso* (complete SNMP ISO path).

4. – 6. Exclude View path: analogue include.

Notice: Each configuration change leads to a restart of the NTS SNMP Agent.

6.5.19 Time zone selection



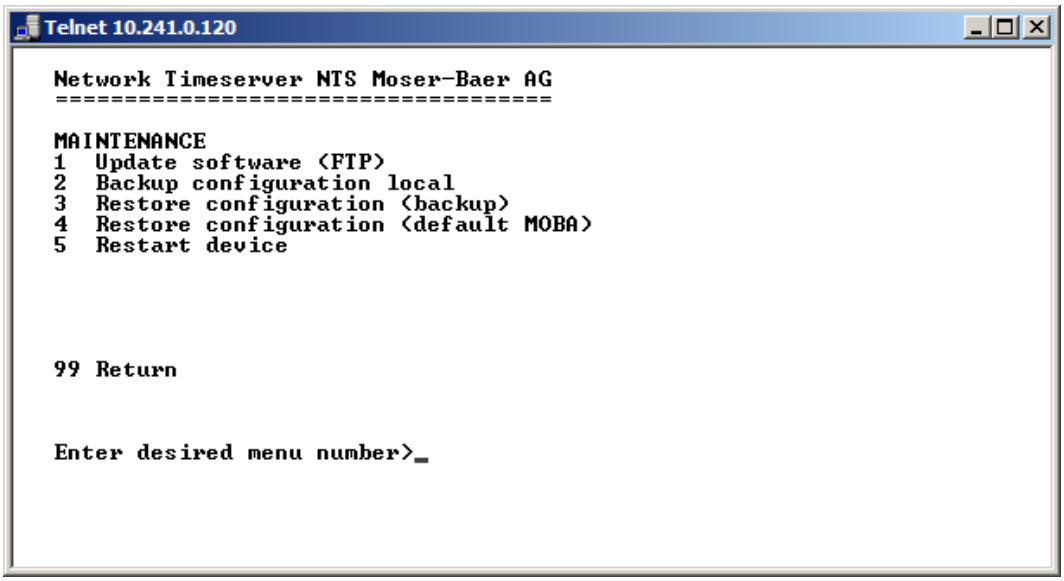
Display of all the NTS time zones (100) over several pages. The pages can be scrolled through with ENTER.

A time zone can be selected on the actual page by entering a time zone number.

Only one time zone can be selected.

Press ESC to leave the page. The modifications will be saved or restored one menu level higher.

6.6 Maintenance menu



1. Initiating a software update (files must have been copied by FTP into the directory */ram* of the NTS before). ➔ See chapter "7 Updates".
   The command always leads to a restart of the NTS (even if no files were copied for update)

Notice: Possibly save configuration first.

2. Backup the entire configuration locally (backup on the NTS).
3. Restore the entire configuration from a backup stored locally. This leads to an automatic restart of the NTS.
4. Restore the entire configuration to factory settings. This leads to an automatic restart of the NTS.
5. Restart NTS.

See also chapter "7 Updates".

7 Updates

7.1 Updating images with MOBA-NMS

Steps for updating images using MOBA-NMS:

1. Select NTS device(s) in the device view.
2. Menu ‘Edit‘ ➔ ‘Commands‘ ➔ Select ‘Firmware Update…‘.
3. Enter the path to the file ‘ntscheck.md5‘ or select it using the ‘Browse…‘ button.
4. Enter further paths to images or select them using the ‘Browse…‘ button.
5. Optionally: Check the box ‘Backup device(s) configuration before update‘ and enter the destination directory for the backup file(s). If a destination folder is selected, the whole device configuration will be saved before the backup. Additionally, if the image ‘ntscfg.img‘ is written too, the saved configuration can be automatically restored after the update. For this, check the box ‘restore configuration after update‘.
6. By clicking the ‘OK‘ button, the update is initiated.

Important: The update procedure (item 6) can take some time (<5 min.) and may not be interrupted under any circumstances. In case of an interruption, the software on the NTS is destroyed and it can only be repaired in the factory.

7.2 Updating images with FTP

Possible images are: u-bootNTS, rootfsNTS.img, uImageNTS, ntsapp.img, ntscfg.img. Additionally the file ntscheck.md5 must exist.
➔ **all file names are case-sensitive.**

Steps for updating images:

1. Connect a FTP client software to the NTS e.g. with Internet Explorer enter: ***ftp://nts@[IP address]***) (as user nts).
   See also chapter "7.4 FTP-Connection"
2. If an update of the image **ntscfg.img** is made, the configuration of the NTS and the telegram files are overwritten. In order to store the configuration, the file *nts.conf* from the directory ***/*etc**. After the update, the file can again be written on the NTS in accordance with chapter “7.3 Updating applications or configurations via FTP“.
3. Change to the directory */ram*.
4. Copy the image into the directory */ram*.
5. Close FTP connection.
6. The update procedure can be started on NTS by selecting the menu '3. Maintenance' ➔ ’1. Update software (FTP)’ and press ENTER.
   The message "Update in progress" appears and at the same time, “Please wait!>“ is shown in the command line. All images are copied. The NTS is automatically restarted upon completion of the update. The Telnet or SSH session has to be restarted.

Notice: The update procedure (point 6) may take longer time depending on the type and number of images (<5 min) and must not be interrupted under any circumstances. If interrupted, the software on the NTS will be destroyed and it has to be returned to the manufacturer for repairing.

Starting up after an update can also take some minutes (<10 min), or it can result in an additional restart, as the file systems have to be checked first.

To eliminate any mistakes during update procedure, the versions should be verified after the update.

7.3 Updating applications or configurations with FTP

To update individual files such as, e.g. ntsapp, ntsmenu, ntpd, nts_time.ko, nts.conf, etc. on the NTS, the following steps are carried out
➔ **all file names are case-sensitive**:

1. Connect a FTP client software to the NTS e.g. with Internet Explorer enter: ***ftp://nts@[IP address])*** (as user nts). See also chapter 7.4 FTP-Connection
2. Change to the directory */ram*.
3. Copy all the files to be updated into the directory */ram*.
4. Close FTP connection.
5. The update procedure can be started on NTS by selecting the menu '3. Maintenance' ➔ '1. Update software (FTP)' and press ENTER.
   The message "Update in progress" appears and at the same time, "Please wait!>" is shown in the command line. All images are copied. The NTS is automatically restarted on completion of the update. The Telnet or SSH session has to be restarted.

Notice: The update procedure (point 5) may take longer time depending on the type and number of images (<5 min) and must not be interrupted under any circumstances. If interrupted, the software on the NTS will be destroyed and it has to be returned to the manufacturer for repairing.

To eliminate any mistakes during update procedure, the versions should be verified after the update.

7.4 FTP connection

Establish anonymous connection:
ftp:///[IP address of NTS]
to directly reach the sub-directory ***/*ram**, e.g. Explorer *ftp://10.241.0.5*

Establish connection as/with a user:
ftp://nts@[IP address of NTS].
e.g. with Internet Explorer enter: *ftp://nts@10.241.0.5*
Password: **nts** resp. the defined password for the menu.
To directly reach the sub-directory */ram*, you can also enter *ftp://nts@10.241.0.5/ram*.

Establish connection with IPv6:
The address **must** be written in brackets [ ]:
e.g. with Internet Explorer enter: *ftp://nts@[fd03:4432:4646:3454::2000]*

Notice: The file has to be copied in binary mode (not ASCII).

FTP tools

	Windows 98, ME, 2000, XP, Vista, Windows 7	**Linux (Suse, Redhat)**
Integrated in the system (file manager):	Windows Explorer Start ➔ Execute: Explorer	Konqueror / Dolphin
Programs (examples)	CuteFTP	Kbear

7.5 SFTP connection

SFTP= SSH File Transfer Protocol

SFTP-Tools

	Windows 98, ME, 2000, XP, Vista, Windows 7	**Linux (Suse, Redhat)**
Integrated in the system (file manager):	-	Konqueror / Dolphin
Programs (examples)	WinSCP	-

7.6 SCP connection

SCP = Secure Copy Protocol

Notice: SCP connection can only be established when no menu (operation) is open.

The following error message can be ignored. There is no influence in the functionality of the operation:

```
Command 'groups'
failed with termination code 127 and error message
-sh: groups: not found.
```

SCP tools

	Windows 98, ME, 2000, XP, Vista, Windows 7	**Linux (Suse, Redhat)**
Integrated in the system (file manager):	-	With command line
Programs (examples)	WinSCP	-

7.7 Save configuration externally

(for backup or copy to another NTS)

Save the current configuration via MOBA-NMS:

1. Select NTS device in the device view.
2. Menu ‘Edit‘ ➔ Select ‘Backup configuration…‘.
3. Select the elements that are to be saved. (In case of doubt, select everything)
4. Click button ‘Next >‘.
5. Indicate destination file by clicking the ‘Browse…‘ button.
6. Optionally: enter a free backup comment. E.g. reason for the backup, use, etc. This comment will then be shown during the restoration of the backup.
7. By clicking the ‘Finish‘ button, the backup is created.
8. At the end of the backup, an overview of the process is shown. It shows which elements were saved and which ones are not available or could not be saved.

Save the current configuration via FTP:

1. Connect a FTP client software to the NTS (with Internet Explorer enter: ***ftp://nts@“IP address“***) (as user nts).
2. Change to the NTS directory ***/etc***.
3. Save the file ***nts.conf*** (configuration) to the user PC (e.g. copy the file to the Desktop or to the directory *My Documents*).

Copy configuration to another NTS:

In order to copy the entire configuration or elements of it from a NTS device to another, the according assistant in MOBA-NMS can be used. For this, select the source device (from which the configuration shall be transferred) and start the assistant in the menu ‘Edit‘ ➔ ‘Transfer configuration…‘. It will lead you through the individual steps.

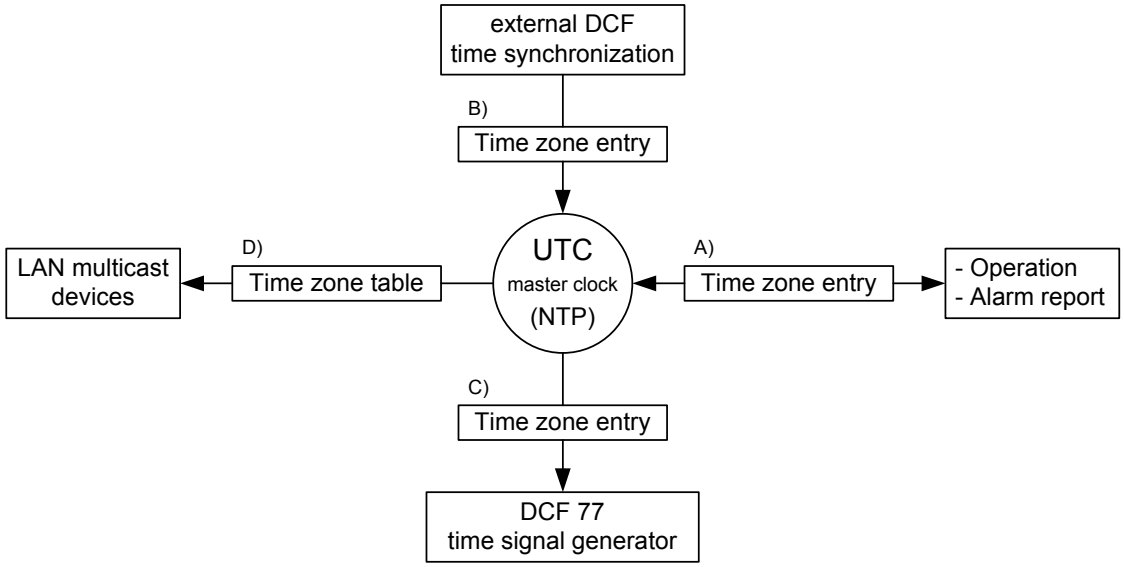
Without MOBA-NMS, perform the procedure explained in chapter 7.3.

Notice: When copying the configuration from one NTS to another, the IP address may have to be changed after the download by serial connection (remove original device from network first).

8 Time administration

8.1 Concept of time administration

The internal master clock as well as the real-time clock runs with UTC (Universal Time Coordinated). The synchronisation inputs, the time shown on the display, as well as all outputs are linked via a time zone entry with the master clock time, i.e. all inputs and outputs can be individually allocated to a specific time zone.



Configurable time zones:

(A) chapter 6.5.13

(B) chapter 6.5.6

(C) chapter 6.5.2

(D) chapter 6.5.3

8.2 Time acceptance from NTP

Always NTP according to RFC 1305.
Maximum of 4 sources.
Reference clock for DCF with selectable time zone.

Acceptance starting at DCF:

- Reference clock for reception starting at DCF. A minimum of 3 minutes of reception is required before the NTP server becomes available.
  Stratum of the time source = 0 ➔ Stratum of the NTS = 1.

Acceptance starting at NTP:

- According to NTP RFC 1305 (www.ntp.org)
  (see http://ntp.isc.org/bin/view/Servers/WebHome for internet servers)

Acceptance starting at RTC (internal time source of the NTS):

- The NTP server is started with Stratum 3 if a DCF source has been configured. As soon as a time source is available, the stratum is reset suitably.
  If no DCF time source has been configured, the NTP server only starts when an NTP source has become available.

Manual setting of time:

- The NTP server is started with Stratum 3 if a DCF source has been configured. As soon as a time source is available, the stratum is reset suitably.
  If no DCF time source has been configured, the NTP server only starts when an NTP source has become available.

Error cases:

- **DCF loss:**
  Conforming to the setting in “Stratum TO,“ the stratum is counted in ascending order to 16.
  When the stratum reaches the value “Stratum limits for Synchalarm,” the alarm “Loss of time source str“ occurs (fixed delay of 1 min.) and the Synch LED turns off.
  When the time source has become available again, the stratum is immediately set according to the source (stratum source + 1).

- **DCF loss with NTP as back-up:**
  According to the setting in “Stratum TO,“ the stratum is counted in ascending order to 16. When the stratum limits have been reached and an NTP server with a better stratum has become available, the NTS synchronizes from NTP.
  When the local time source has become available again, the stratum is immediately set according to the source (Stratum source + 1).

- **NTP loss:**
  Loss of the/all NTP source/s without Fixstratum and without DCF.
  Normally, it takes 8 x the poll interval of the current source until the peer has been recognized as invalid (source no longer recognizable) and NTP loses the synchronization. The duration lies outside the poll interval but also dependent on the measured jitter, number of sources, duration of the synchronization and source deviation. Consequently, it may massively deviate in individual cases.

Exception during time acceptance:
After an update of the software, the first time acceptance may last noticeably longer (>8 min).

8.3 Fixstratum for local time source

During operation with NTP sources and "local source = off," the behavior of the NTP server is equivalent to a standard NTP server: When the sources are no longer available or invalid, the NTP server is unsynchronized after a short time according to NTP algorithms.

So that the NTP slave clock line is supplied with Multicast NTP, the NTP server must remain synchronized. An unsynchronized NTP server does not transmit time. In that case, the clocks in the NTP slave clock line are turned to the 12 o'clock position.

Therefore, it is sensible to set a ***Fixstratum*** value **unequal to 0** in this case.

Time source(s)	**Fixstratum = 0**	**Fixstratum > 0**
Local time source (DCF/GPS) switched on; **with NTP source/s**	DCF ok: Stratum NTS always 1, time always from DCF DCF nok: If NTP is available Stratum NTS = Stratum NTP source + 1 Otherwise: Stratum rises according to set stratum TO value until the NTP server becomes unsynchronized (Stratum = 16)	DCF ok: Stratum NTS always 1, time always from DCF DCF nok: If NTP available Stratum NTS = Stratum NTP source + 1 Otherwise: Stratum rises according to set StratumTO value to stratum source = Fixstratum ➔ NTS now keeps Fixstratum + 1
Local time source (DCF/GPS) switched on; **without NTP source/s**	DCF ok: Stratum NTS always 1, time always from DCF DCF nok: Stratum rises according to the set Stratum TO value until NTP server becomes unsynchronized (Stratum = 16)	DCF ok: Stratum NTS always 1, time always from DCF DCF nok: Stratum rises according to set Stratum TO value to stratum source = Fixstratum ➔ NTS now keeps Fixstratum + 1
Local time source (DCF/GPS) switched off; **with NTP source/s**	NTP ok: Stratum NTS = current NTP source + 1 NTP nok: Normally, the NTP server is very quickly unsynchronized with loss of the NTP source (about 8 x poll intervall of the current source) **Warning:** No sensible configuration with NTP slave clocks	NTP ok: Stratum NTS = current NTP source + 1 except Stratum NTP source > Fixstratum NTP nok: Stratum NTS = Fixstratum + 1
Local time source (DCF/GPS) switched off; **without NTP source/s**	**Warning:** Not a sensible configuration	Only for testing with an NTS without source that should still have an NTP server with valid time. Stratum of the NTS is Fixstratum + 1.

8.4 Time server

- NTP v4 (compatible with v3) as per RFC 1305 (Port 123)
  NTP authentication with MD5 key / autokey
- SNTP (UDP), RFC2030 (Port 123)
- TIME (TCP/UDP), RFC 868 (Port 37)
- DAYTIME (TCP/UDP), RFC 867 (Port 13)

8.5 Time accuracy, time-keeping

See appendix G Technical Data.

8.6 Leap second

Manual mode

The announcement of the switching second is put out by DCF and NTP each time 1 hour before the defined time.

*The announcement is only sent via NTP when the local source or a DCF source is switched on. If only one NTP source is configured, the state of the source is passed on.

Automatic mode

In the automatic mode, the source (DCF or NTP) is checked for a possible announcement for 1 hour before the point in time of the possible leap second. If the announcement is recognized, it is passed on via NTP and DCF output and the leap second is inserted.

8.7 NTP Authentication

NTP provides two variants for authentication in version 4:

- NTP symmetric keys (i.e. symmetric keys)
- NTP autokeys

NTP authentication assures a correct time source and prevents manipulation of NTP information. NTP data itself is, however, not encoded.

8.7.1 NTP symmetric keys

A 32-bit key ID and a cryptographic 64/128-bit check sum of the packet is attached to each NTP IP packet.
The following algorithms are used for this purpose:

- Data Encryption Standard (DES)
  (partly restricted in North America and no longer integrated into new NTP variants (>V4.2))
- Message Digest (MD5)

The NTS only supports the MD5 procedure.

The receiving NTP service calculates the check sum with an algorithm and compares it with the one contained in the packet. Both NTP services must have the same encryption key and the same corresponding key ID for this purpose.
Packets with a wrong key or wrong check sum will not be used for synchronization.
The NTS must be correspondingly configured to be able to use NTP authentication (chapter 6.5.7 NTP Server). The NTP service of the other equipment (e.g. server, PC...) must also be configured. In the case of standard NTP, this occurs via the ntp.conf file:

```
# path for key file
keys /etc/ntp/ntp.keys
trustedkey 1 2 3 4 5 6# define trusted keys
requestkey 4 # key (7) for accessing server variables
controlkey 5 # key (6) for accessing server variables

server ntp1.test.org key 2
server ntp2.test.org key 6
server 192.168.23.5 key 3
```

The description of the ntp.conf file can be accessed via the corresponding man-page, or consulted at http://www.eecis.udel.edu/~mills/ntp/html/authopt.html

The authentication mode is automatically activated when a key is used and the paths for the keys have been correspondingly configured.

`trustedkey` defines all keys currently permitted

`requestkey` defines the key for the ntpq help tool.

`controlkey` defines the key for the ntpdc help tool.

The keys are located in the ntp.keys file defined with `keys`. This has the following format:

```
1   M    TestTest
2   M    df2ab658
15  M    I_see!
498 M    NTPv4.98
```

The key ID is in the first column of the file, the format of the keys in the second defined column, and the key itself in the third. There are four key formats, however, nowadays only the MD5 is still used ➔ M. The letter M is no longer written for new NTP variants (>V4.2) and is only necessary for backwards compatibility.
The signs ' ', '#', '\t', '\n' and '\0' are not used in the MD5 ASCII key! Key 0 is reserved for special purposes and should, therefore, not be used here.

ntp.keys: man page for ntp.keys to be noted (check the internet)

8.7.2 NTP Autokey

The validity of the time received to the NTP clients is assured by symmetric keys. For a higher degree of certainty, exchanging the keys used regularly is, however, necessary to obtain protection, e.g. from replay attacks (i.e. attacks in which recorded network traffic is simply played back).

The autokey procedure was introduced as the exchange is very involved in a large network. A combination of group keys and public keys enables all NTP clients to check the validity of the time information which they receive from servers in their own autokey group.

NTP Autokey is relatively complex in its use and studying the functionality is definitely necessary beforehand.

Autokey is descrbied at *http://www.cis.udel.edu/~mills/proto.html* or on the NTP homepage *http://www.ntp.org*.

Autokey is currently defined in an IETF draft.
http://www.ietf.org/internet-drafts/draft-ietf-ntp-autokey-04.txt

The configuration of Autokey is explained in
http://support.ntp.org/bin/view/Support/ConfiguringAutokey or in
http://www.ntp.org/ntpfaq/NTP-s-config-adv.htm#S-CONFIG-ADV-AUTH.

9 SNMP

9.1 General

The SNMP version **V2c** or **V3** for *Get*, *Put* and *Notification* (Trap) is used.

A full SNMP agent is implemented on the NTS (MIBII, NTS).

For SNMP V2c, following standard *Communities* are used:

Read only :	*romobatime*
Read/write:	*rwmobatime*
Trap:	*trapmobatime*

For SNMP V3, following standard *User I Passwords* are used:

ntsUser1:	*mobatime*	
ntsUser2:	*mobatime*	
ntsInfo:	*mobatime*	*(not changeable, read only)*

The users ntsUser1 and ntsUser2 have full read/write access on all objects. With SNMP V3 rules, access can be reduced. Changes of the rules can only be modified over the NTS menu but not via SNMP.

SNMP V3 agent supports user validation (authentication MD5) and encoding (encryption DES).

MIBII values like sysDescr, sysContact, sysName, or sysLocation can only be modified over the NTS menu but not via SNMP.

The following MIB definitions are used:

SNMPv2-SMI, SNMPv2-MIB, SNMPv2-CONF, SNMPv2-TC, SNMPv2-TM, SNMP-FRAMEWORK-MIB, SNMP-MPD-MIB, SNMP-NOTIFICATION-MIB, SNMP-TARGET-MIB, SNMP-USER-BASED-SM-MIB, SNMP-VIEW-BASED-ACM-MIB, RFC1213-MIB, IF-MIB, IP-MIB, IP-FORWARD-MIB, TCP-MIB, UDP-MIB, HOST-RESOURCES-MIB, HOST-RESOURCES-TYPES, DISMAN-EVENT-MIB, NOTIFICATION-LOG-MIB, UCD-SNMP-MIB, NET-SNMP-MIB, NET-SNMP-TC

SNMP V2c,V3:

MOBA-COMMON (File: MOBA-COMMON-MIB.TXT)
General MOBA definition, always required

NTS (NTS-MIB.TXT)
Device specific NTS definitions

The MIB files can be copied from the NTS with FTP (For FTP use, see chapter “7.4 FTP Connection“):

NTS-MIB:	/etc/snmp/mibs/
Standard MIBS:	/usr/share/snmp/mibs/

9.2 Device configuration with SNMP

If one or several variables are set with *Put* in a configuration group, the variable *nts????ConfigCmd* must be set at the end to 1 in the corresponding group. The values of the entire configuration group are assumed from the NTS with this command (1=accept).

As long as the accept command has not been set, the changed variables can be restored to the old values by setting the *nts????ConfigCmd* variable to 2 (2=undo, restore).

After sending the accept command, an ntsConfigChanged *Notification* is sent.

The definitions of the available variables can be taken from the MIB files.

Example:

Management-System		**NTS**
Put ntsFTPMode=1	→	Variable is set to 1 internally
Put ntsNetServicesConfigCmd=1	→	Configuration group is assumed
	←	Sends ntsConfigChanged *Notification*
		with the new time ntsNetConfigChangedTime

9.3 NTS subagent SNMP notification

Protocol: SNMPv2c Notification

Important: For *Notifications* to be sent out, SNMP must be switched on. In addition, at least one receiver system must be configured.

9.3.1 Start up [ntsStartUp]

Sent out when the subagent for the NTS is started.

This *Notification* is always sent out, as soon as SNMP is activated and a destination address is configured.

9.3.2 Shutdown [ntsShutdown]

Sent out when the subagent for the NTS is stopped.

This *Notification* is always sent out, as soon as SNMP is activated and a destination address is configured.

9.3.3 Status changed [ntsStatusChanged]

Sent out when the subagent detects a status change in the NTS application process. The following variables are monitored for changes:

ntsSysStatus, ntsSysTimeSource, ntsSysStratum, ntsSysMasterMode

This *Notification* is always sent out as soon as SNMP is activated and a destination address is configured.

The *Notification* sent out contains the following data:

Field	Type	Size	Description	Example
ntsSysStatus	Unsigned Int	4 Bytes	Contains the internal system status	`66309`
ntsSysOffset	Integer	4 Bytes	Actual time offset of the system [us]	`-1523` → `-1.523ms`
ntsNTPTInfoCurrentSource	Octet String	63	Actual time source	`192.168.1.55`
ntsSysStratum	Byte	1 Bytes	Actual system stratum level	`1`

9.3.4 Configuration changed [ntsConfigChanged]

Sent out when the subagent detects a configuration change in the NTS application processes.

This *Notification* is always sent out, as soon as SNMP is activated and a destination address is configured.

The *Notification* sent out contains the following data:

Field	Type	Size	Group
ntsSysConfigChangedTime	TimeTicks	4 Bytes	ntsSystem
ntsNetworkConfigChangedTime	TimeTicks	4 Bytes	ntsNetwork
ntsNetServicesConfigChangedTime	TimeTicks	4 Bytes	ntsNetServices
ntsTSConfigChangedTime	TimeTicks	4 Bytes	ntsTimeSource
ntsNTPConfigChangedTime	TimeTicks	4 Bytes	ntsTimeNTPServer
ntsOutDCFPulseConfigChangedTime	TimeTicks	4 Bytes	ntsOutDCFPulse
ntsOutLineTZServerConfigChangedTime	TimeTicks	4 Bytes	ntsOutLineTZServer
ntsRelayConfigChangedTime	TimeTicks	4 Bytes	ntsAlarmRelayConfig
ntsMailConfigChangedTime	TimeTicks	4 Bytes	ntsAlarmMailConfig
ntsSnmpConfigChangedTime	TimeTicks	4 Bytes	ntsSnmpConfig
ntsSnmpV3ConfigChangedTime	TimeTicks	4 Bytes	ntsSnmpV3

The *ConfigChangedTime* variables show the time of the last change of the relevant configuration group as TimeTicks value in 1/100 seconds. The management system can decide on the basis of these time values, which configurations need to be reloaded.

The groups and corresponding parameters are listed in annex F Parameters.

9.3.5 Alive notification [ntsAlive]

Sent out in a configurable interval.

This *Notification* is always sent out, as soon as SNMP and the alarm traps are activated and a destination address is configured.

The *Notification* sent out contains the following data:

Field	Type	Size	Description	Example
ntsSysStatus	Unsigned Int	4 Bytes	Contains the internal system status	66309
ntsSysAlarms	Byte Array	8 Bytes	64 Bit Alarm flags 1.Byte Bit 0..7 2.Byte Bit 8..15 :: 8.Byte Bit 56..63	FFF870FF.FFFFFFFF 1.Byte 2.Byte 5.Byte

9.3.6 Alarm notification [ntsAlarm]

Sent out if alarm status changes, i.e. *Notification* is sent out when an alarm flag is set or deleted.

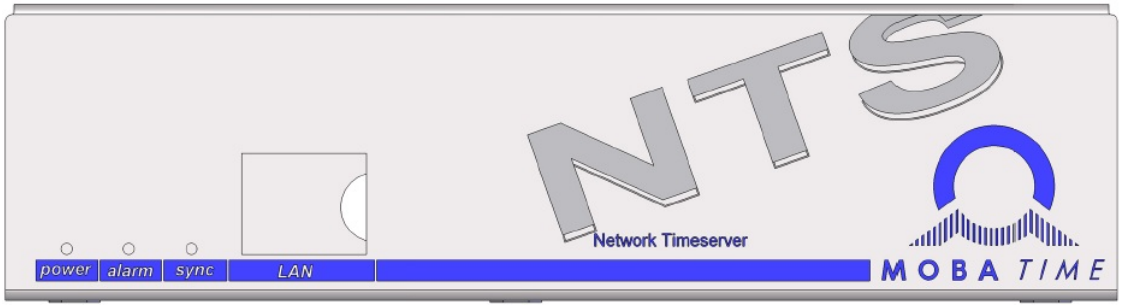
This *Notification* is always sent out, as soon as SNMP and the alarm traps are activated and a destination address is configured.

The *Notification* sent out contains the following data:

Field	Type	Size	Description	Example
ntsTrapAlMsgErrorNr	Byte	1 Byte	No. of the alarm bit (0..63)	3
ntsTrapAlMsgErrorState	Byte	1 Byte	0 = alarm bit was deleted 1 = alarm bit was set	1
ntsTrapAlMsgErrorTime	Unsigned Int	4 Bytes	PC-time in seconds since 01.01.1970 00:00:00	946684805
ntsTrapAlMsgErrorText	Text	59 Bytes	Error text	Failure supply 1

A Connection diagrams

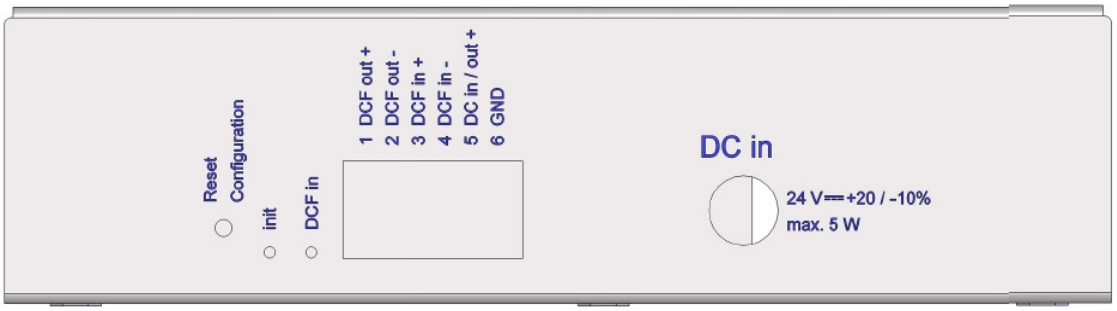
A.1 Front connections



LAN Connection:

Plug: RJ45
Interface: Ethernet, 10/100Mbit half or full duplex
Use only shielded cables!

A.2 Connections (rear view)



NTS connections
For technical data see in Appendix "G Technical data"

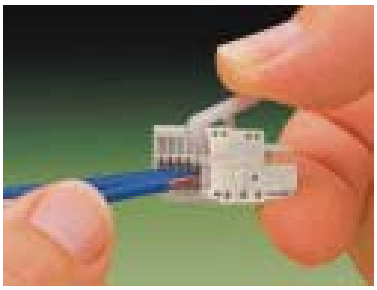
Clamp	Connection	Description
1	DCF output +	DCF or impulse output, “current loop” passive, Umax= 30VDC, I_{on} = 10..15mA, I_{off} < 1mA @20VDC
2	DCF output -	
3	DCF input +	DCF input e.g. for connecting a GPS 4500 or DCF receiver with „current loop“ output
4	DCF input -	
5	DC input / output +	DC power supply at DC in or DC output for GPS receivers 24 VDC, max. 200 mA
6	DC input / output GND	

	DC in	External voltage plug 5.5/2.1+ Input for external DC feed (wall plug transformer) 24 VDC, max. 200 mA

A.3 Plug-in spring terminals

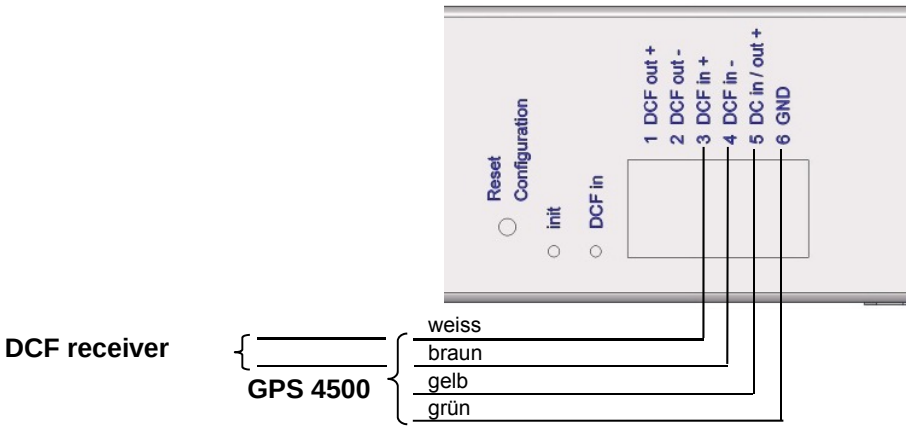
multiple contact strip 100% protected against wrong plug;
WAGO CAGE CLAMP® connection
Cross section of 0,08 mm² to 1,5 mm² (from AWG 28 to AWG 14)
Voltage CSA 300 V / current CSA 10 A
Rated voltage: EN 250 V
Rated surge voltage: 2,5 kV
Nominal current: 10 A
Strip length: 7 mm (0,28 in)

Pulled off spring terminal with operation tool:



2 operation tools are delivered with the accessory bag.

A.4 Connection GPS 4500 or DCF 450



GNSS 3000 according to manual Bx 800813 chap. 9.2 Connection schema DCF current loop.

B Time zone table

Time zone entries in the standard season table (version 10.0).

Time zone	City / State	UTC Offset	DST Change	Standard → DST	DST → Standard
00	UTC (GMT), Monrovia, Casablanca	0	No		
01	London, Dublin, Edinburgh, Lisbon	0	Yes	Last Sun. Mar. (01:00)	Last Sun. Oct. (02:00)
02	Brussels, Amsterdam, Berlin, Bern, Copenhagen, Madrid, Oslo, Paris, Rome, Stockholm, Vienna, Belgrade, Bratislava, Budapest, Ljubljana, Prague, Sarajevo, Warsaw, Zagreb	+1	Yes	Last Sun. Mar. (02:00)	Last Sun. Oct. (03:00)
03	Athens, Istanbul, Helsinki, Riga, Tallinn, Sofia, Vilnius	+2	Yes	Last Sun. Mar. (03:00)	Last Sun. Oct. (04:00)
04	Bucharest, Romania	+2	Yes	Last Sun. Mar. (03:00)	Last Sun. Oct. (04:00)
05	Cairo, Pretoria, Harare	+2	No		
06	Amman	+2	Yes	Last Thu. Mar. (23:59)	Last Fri. Oct. (01:00)
07	UTC (GMT)	0	No		
08	Kuwait City, Minsk, Kaliningrad	+3	No		
09	Praia, Cape Verde	-1	No		
10	UTC (GMT)	0	No		
11	Abu Dhabi, Muscat, Tbilisi, Moscow, St. Petersburg, Volgograd, Samara	+4	No		
12	Kabul	+4.5	No		
13	Adamstown (Pitcairn Is.)	-8	No		
14	Tashkent, Islamabad, Karachi	+5	No		
15	Mumbai, Calcutta, Madras, New Delhi, Colombo	+5.5	No		
16	Astana, Thimphu, Dhaka, Yekaterinburg	+6	No		
17	Bangkok, Hanoi, Jakarta, Novosibirsk	+7	No		
18	Beijing, Chongqing, Hong Kong, Singapore, Taipei, Urumqi, Krasnoyarsk	+8	No		
19	Tokyo, Osaka, Sapporo, Seoul, Irkutsk	+9	No		
20	Gambier Island	-9	No		
21	South Australia: Adelaide	+9.5	Yes	1st Sun. Oct (02:00)	1st Sun. Apr. (03:00)
22	Northern Territory: Darwin	+9.5	No		
23	Brisbane, Guam, Port Moresby, Yakutsk	+10	No		
24	Sydney, Canberra, Melbourne, Tasmania: Hobart	+10	Yes	1st Sun. Oct. (02.00)	1st Sun. Apr. (03:00)
25	UTC (GMT)	0	No		
26	UTC (GMT)	0	No		

27	Honiara (Solomon Is.), Noumea (New Caledonia), Vladivostok	+11	No		
28	Auckland, Wellington	+12	Yes	Last Sun. Sep. (02:00)	1st Sun. Apr. (03:00)
29	Majuro (Marshall Is.), Magadan, Anadyr	+12	No		
30	Azores	-1	Yes	Last Sun. Mar. (00:00)	Last Sun. Oct. (01:00)
31	Middle Atlantic	-2	No		
32	Brasilia	-3	Yes	3rd Sun. Oct. (00:00)	3rd Sun. Feb. (00:00)
33	Buenos Aires	-3	No		
34	Newfoundland, Labrador	-3.5	Yes	2nd Sun. Mar. (02:00)	1st Sun. Nov. (02:00)
35	Atlantic Time (Canada)	-4	Yes	2nd Sun. Mar. (02:00)	1st Sun. Nov. (02:00)
36	La Paz	-4	No		
37	Bogota, Lima, Quito	-5	No		
38	New York, Eastern Time (US & Canada)	-5	Yes	2nd Sun. Mar. (02:00)	1st Sun. Nov. (02:00)
39	Chicago, Central Time (US & Canada)	-6	Yes	2nd Sun. Mar. (02:00)	1st Sun. Nov. (02:00)
40	Tegucigalpa, Honduras	-6	No		
41	Phoenix, Arizona	-7	No		
42	Denver, Mountain Time	-7	Yes	2nd Sun. Mar. (02:00)	1st Sun. Nov. (02:00)
43	Los Angeles, Pacific Time	-8	Yes	2nd Sun. Mar. (02:00)	1st Sun. Nov. (02:00)
44	Anchorage, Alaska (US)	-9	Yes	2nd Sun. Mar. (02:00)	1st Sun. Nov. (02:00)
45	Honolulu, Hawaii (US)	-10	No		
46	Midway Islands (US)	-11	No		
47	Mexico City, Mexico	-6	Yes	1st Sun. Apr. (02:00)	Last Sun. Oct. (02:00)
48	Adak (Aleutian Is.)	-10	Yes	2nd Sun. Mar. (02:00)	1st Sun. Nov. (02:00)
49	UTC (GMT)	0	No		
50	UTC (GMT)	0	No		
51	UTC (GMT)	0	No		
52	UTC (GMT)	0	No		
53	UTC (GMT)	0	No		
54	Scoresbysund, Greenland	-1	Yes	Last Sun. Mar. (00:00)	Last Sun. Oct. (01:00)
55	Nuuk, Greenland	-3	Yes	Last Sat. Mar. (22:00)	Last Sat. Oct. (23:00)
56	Qaanaaq, Greenland	-4	Yes	2nd Sun. Mar. (02:00)	1st Sun. Nov. (02:00)
57	Western Australia: Perth	+8	No		
58	Caracas	-4.5	No		
59	CET standard time	+1	No		
60	Santiago, Chile	-4	Yes	2nd Sun. Oct. (00:00)	2nd Sun. Mar. (00:00)
61	Chile, Easter Island	-6	Yes	2nd Sat. Oct. (22:00)	2nd Sat. Mar. (22:00)
62	Baku	+4	Yes	Last Sun. Mar. (04:00)	Last Sun. Oct. (05:00)
63	UTC (GMT)	0	No		
64	UTC (GMT)	0	No		

In countries where the DST switch date changes annually (e.g. Iran, Israel), the time zone has to be defined manually in the user time zone table (entries 80 – 99).

Legend:

UTC:	Universal Time Coordinate, equivalent to GMT
DST:	Daylight Saving Time
DST Change:	Daylight Saving Time changeover
Standard → DST:	Time change from Standard time (Winter time) to Summer time
DST → Standard:	Time change from Summer time to Standard time (Winter time)

Example:

2nd last Sun. Mar. (02:00) Switch over on the penultimate Sunday in March at 02.00 hours local time.

Notice: The Time Zone Table is usually updated as needed. The current table is available for download under the following address: *www.mobatime.com* ➔ *Customer Area* ➔ *Customer Support* ➔ *Support Resources* ➔ *Time Zone Table*. In case your device is equipped with a newer version than shown in this manual, the current time zone settings should be checked.

Modifications / updating the time zone table:

The time zone tables are filed in the */etc/mbsn.tbl* (standard table) and */etc/usersn.tbl* (user table) files.
The user table can be changed with Moser-Baer AG software such as ETCW or MOBA-NMS.
Using MOBA-NMS, it can be downloaded from there, otherwise, it must be copied on to the NTS in accordance with the update instructions (chapter “7.3 Updating Applications and Configurations“).

Notice: The file names ***mbsn.tbl*** und ***usersn.tbl*** must be written in small letters.

C Alarm list

Number	Error message	Description / Action	Chap.
0	Reboot NTS	NTS restarted, no intervention required	
1	Error bit1	Not used	
2	Error bit2	Not used	
3	Error bit3	Not used	
4	Error bit4	Not used	
5	Error bit5	Not used	
6	Error bit6	Not used	
7	Error bit7	Not used	
8	Wrong time zone DCF out	Check time zone (DCF/impulse output) configuration	6.5.2
9	Error bit9	Not used	
10	Error bit10	Not used	
11	Error bit11	Not used	
12	Error bit12	Not used	
13	Error bit13	Not used	
14	Error bit14	Not used	
15	Error bit15	Not used	
16	Time source lost	Stratum of current time source (DCF/GPS/NTP during loss of time source) too high ➔ check time source. May occur shortly after a restart (approx. 10 min). ➔ synch LED off	6.5.5
17	Failure time source TO	No time information from the selected time source (GPS/DCF) within the configured timeout ➔ check time source. Configuration see chapter 6.5.6, menu 4: “Alarm delay failure time source”	6.5.6
18	No valid time	Set time manually or configure and/or control time source. Occurs after a restart without time information from the source, RTC or manually set time.	
19	NTP synch. lost	Synchronization lost ➔ check time source (DCF/NTP) and settings.	
20	Error bit20	Not used	
21	NTP not working	NTP error ➔ check NTP settings. If no DCF/GPS source: set an NTP source (even if only one available) to “prefer”. May also occur during reconfiguration of time sources or time settings. After a restart of the NTS (<30 min), the alarm may also occur.	
22	Time zone DC in wrong	Check time zone setting (time source)	6.5.6
23	Syn only diff too large	Check synchronization and source	6.5.6
24	Mail config. wrong	Check e-mail configuration. For bug-fixing, see file mailerror.txt in /ram/.	6.5.11
25	SNMP not working	Check SNMP and trap configuration	6.5.12 / 6.5.16
26	Error bit26	Not used	
27	Error bit27	Not used	
28	Error bit28	Not used	
29	Error bit29	Not used	
30	Error bit30	Not used	

31	Error bit31	Not used	
32-63	Error bitxx	Not used	

D Troubleshooting

#	Interference / notes:	Possible causes / measures
1	sync LED flashing:	DCF / GPS source does not supply time –> 2
2	Reception problem with DCF/GPS:	In menu *1 Status –> 4 Source*, check if the DCF second counter regularly counts in ascending order from 0 – 59 (according to the current second, value changes about every 3 seconds). If the counter is not correct ➔ check receiver and wiring. Check "DCF in" LED at the back of the Network Timeserver NTS.
3	No NTP time despite manual time setting ➔ sync LED is off	The local time source **DCF/GPS** or **local** must be set or NTP cannot accept a time.
4	General time acceptance problems	If the Network Timeserver NTS exhibits a major deviation from the source time (NTP or DCF) (> 5 min), the time acceptance by NTP will be longer as a result (> 30 min). As a remedy, the time will be set manually
5	NTS is continuously restarting.	Make sure the network settings are correct, especially the hostname and the gateway have to be configured (if no gateway is available, the own IP address can be used).
6	LAN LED (left) is flashing orange.	No connection to the network. Check network cabling.
7	Opening the menu via Telnet is not possible or NTS is not or no longer reachable via network.	Check network settings in menu 2 Configuration –> 5 Network: - IP-Address, Subnet mask and Gateway must be set correctly - Interface should be set to **Auto** - Check connection with "Ping" - When earlier the menu was not correctly exited (e.g. LAN cable removed), the menu can be blocked up to 15 minutes.
8	System software update	The system software can be updated using FTP client software or MOBA-NMS (s. chapter 7 Updates). Your MOBATIME service informs you of use and necessity of a software update. If necessary, they can provide the needed firmware file.
9	Needed information to contact MOBATIME service	**Device type, part number, production number and serial number:** This details are given on the adhesive type label. **If possible provide the following files for the analysis:** All files from the directories **/var/log/** and **/etc/**. To copy these files use FTP, e.g. Windows Explorer with ftp://[IP-Adresse], see chapter 0 . **If log files cannot be copied, read out current software version:** The software version can be queried in the menu `1 STATUS/9 Versions of the software` **Place and date of purchase and of commissioning of the device.** **Most comprehensive possible details of the malfunction:** Describe the problem, possible causes, measures taken, the system environment / operating mode and configuration, etc.

E Copyright notice

All rights of the software remain the property of Moser-Baer AG.

Parts of existing software (OpenSource) with their own licences were used:

Designation	Description	Version	License	License Description (file)
U-Boot	Boot loader	2012.04	GPL version 2	COPYING
Linux	Operating system	3.2.0-rc3	GPL version 2	COPYING
Busybox	System environment	1.20.2	GPL version 2	LICENSE
NTP	NTP	4.2.6p4	Free	COPYRIGHT
pure-ftp	FTP server	1.0.36	Free, partly BSD	COPYING
NetSNMP	SNMP agent	5.7.1	BSD	COPYING
OpenSSL	SSL Lib.	1.0.16	BSD style	LICENSE
OpenSSH	SFTP server	6.1p1	BSD	LICENCE
dropbear	SSH server	2012.55	MIT style: Free, party BSD	LICENSE
wide-dhcpv6	DHCPv6 client	20080615	Free	COPYRIGHT
flex	Flex Lib.	2.5.37	BSD adapted	COPYING
zlib	Compress lib.	1.2.7	Free	README
mailsend	E-mail client	1.15b5	GPL	-
lighttpd	http Server	1.4.32	Free	COPYING

The complete license descriptions can be referred to in the file indicated in the respective original source code on the corresponding project page.

Licence text GPL, BSD and MIT:

GPL version 2: http://www.gnu.org/licenses/gpl-2.0.html

BSD: http://www.opensource.org/licenses/bsd-license.php

MIT http://www.opensource.org/licenses/with-license.php

The source code of the open source projects running under GPL can be requested from Moser-Baer AG (support@mobatime.com). Handling costs will be charged!

F Parameters

Group	Parameter	Acc	Default	Unit	SNMP
Network	**Network**				**ntsNetwork**
	Mode Interface	*RW*			
	DHCP on/off	RW	off		ntsDHCPMode
	IP address	RW	192.168.46.46		ntsIPAddr
	Network mask	RW	255.255.255.0		ntsIPMask
	Gateway IP	RW	192.168.46.1		ntsIPGateway
	Name server IP	RW	-		ntsIPNameserver
	Autoconf V6	RW	off		ntsIPv6AutoConf
	DHCPv6	RW	off		ntsIPv6DHCPMode
	IP address V6 1	RW	0::0		ntsIPv6Addr1
	IP prefix 1	RW	64		ntsIPv6Prefix1
	Gateway IPV6 1	RW	0::0		ntsIPv6Gateway1
	IP address V6 2	RW	0::0		ntsIPv6Addr2
	IP prefix 2	RW	64		ntsIPv6Prefix2
	Gateway IPV6 2	RW	0::0		ntsIPv6Gateway2
	Name server IPV6	RW	0::0		ntsIPv6Nameserver
	Link 10/100Mbit	RW	auto		ntsEthernetLinkMode
	Device name / host name	RW	Nts + 6 digits of the MAC		ntsHostname, ntsNetInfoHostname
	Domain	RW			ntsDomain
Network Services					**ntsNetServices**
	Telnet	RW	on		ntsTelnetMode
	SSH	RW	on		ntsSSHMode
	FTP	RW	on		ntsFTPMode
	http mode	RW	off		ntsHTTPMode
	http port	RW	80		ntsHTTPPort
General					**ntsSystem**
	Display language	RW	engl.		ntsLanguage
	Password user *nts*	RW	nts		ntsPassword
	Time zone operation and alarm messages	RW	MEZ		ntsTimezone
Lines					**ntsOutputLines**
DCF Out					**ntsOutMainDCF**
	Mode	RW	DCF on		ntsOutMainDCFMode
	Timezone	RW	UTC		ntsOutMainDCFTimezone
	Pulse Mode	RW	sec		ntsOutMainDCFPulseType
	Pulse Length	RW	500	ms	ntsOutMainDCFPulseTime
	Pulse Period	RW	1	sek	ntsOutMainDCFPulsePeriod
	Pulse Offset	RW	0	ms	ntsOutMainDCFPulseCorrection
NTP slave clocks					**ntsOutLineTZServer**
	Mode	RW	off		ntsOutLineTZServerMode
	Multicast IP	RW			ntsOutLineTZServerMCastAddr
	Multicast Port	RW	65534		ntsOutLineTZServerMCastPort
	Poll Intervall NTP	RW	0 -> 1sec	2^x sec	ntsOutLineTZServerNTPInterval
	Multicast TTL	RW	1		ntsOutLineTZServerTTL
	Table interval	RW	60	sec	ntsOutLineTZServerTableInterval
	Entry interval	RW	1	sec	ntsOutLineTZServerEntryInterval
	Table time zone entries	RW	-1		ntsOutLineTZServerTable (TZ entry number)
E-mail					**ntsAlarmMailConfig**
	Mode	RW	Off		ntsMailMode
	IP addr. mail server	RW			ntsMailServerIPAddress
	Port mail server	RW	25		ntsMailServerPort
	Destination address 1	RW			ntsMailAddrDestination1
	Destination address 2	RW			ntsMailAddrDestination2
	Sender address (“login to mail server“)	RW			ntsMailAddrFrom
	Reply address	RW			ntsMailAddrReply
	Alarm mask	RW	All set: FF FF FF FF FF FF FF FF		ntsMailAlarmMask
	Auth. mode	RW	off		ntsMailAuthMode
	User name	RW			ntsMailUser
	Password	RW			ntsMailPassword
SNMP / traps					**ntsSnmpConfig**
	Trap mode	RW	off		ntsSnmpTrapMode

	Trap community	RW	trapmobatime		ntsSnmpTrapCommunity
	IP addr. listener 1	RW			ntsSnmpTrapListenerIPAddress1
	Port listener 1	RW	162		ntsSnmpTrapListenerPort1
	Trap version 1	RW	V2c		ntsSnmpTrapVersion1
	IP addr. listener 2	RW			ntsSnmpTrapListenerIPAddress2
	Port listener 2	RW	162		ntsSnmpTrapListenerPort2
	Trap version 2	RW	V2c		ntsSnmpTrapVersion2
	TRAP alarm mask	RW	All set: FF FF FF FF FF FF FF FF		ntsSnmpTrapAlarmMask
	TO alive message	RW	off	sec	ntsSnmpTrapAliveMsgInterval
	SNMP mode	RW	on		ntsSnmpMode
	SNMP alarm mask	RW	All set: FF FF FF FF FF FF FF FF		ntsSnmpAlarmMask
	Location	RW			ntsSnmpLocation
	Contact	RW			ntsSnmpContact
	rocommunity	RW	romobatime		ntsSnmpROCommunity
	rwcommunity	RW	rwmobatime		ntsSnmpRWCommunity
	2*Access config:				
	Password	RW			ntsSnmpV3UserPassword**x**
	UserSecLevel	RW	1+2: auth		ntsSnmpV3UserLevel**x**
	UserRead	RW	1+2: _all_		ntsSnmpV3UserRead**x**
	UserWrite	RW	1=viewNTS1 2=viewNTS2		ntsSnmpV3UserWrite**x**
	View1	RW	1+2: .1.3.6.1.4.1.8072		ntsSnmpV3View**x**1
	View2	RW	1+2: .1.3.6.1.4.1.2021		ntsSnmpV3View**x**2
	View3	RW	1+2: .1.3.6.1.4.1.13842.5		ntsSnmpV3View**x**3
	View4	RW	1+2: .2		ntsSnmpV3View**x**4
	View5	RW	1+2: .2		ntsSnmpV3View**x**5
	View6	RW	1+2: .2		ntsSnmpV3View**x**6
Alarm output:					**ntsRelayAlarmConfig**
	Alarm mask relay	RW	All set: FF FF FF FF FF FF FF FF		ntsRelayAlarmMask
NTP / time reception					**ntsTimeHandling**
Time source:					**ntsTimeSource**
	Time source mode (DCF)	RW			ntsTSDCFInput
	Time zone	RW			ntsTSTimeZone
	Config. stratum	RW		Stratum	ntsTSFixStratum
	TO time source for alarm Loss synch (TO)	RW	off	min	ntsTSTimeout
	Max. stratum for alarm Loss synch (stratum)	RW	12	Stratum	ntsTSStratumErrorLimit
	TO time source stratum	RW	24	h	ntsTSStratumTimeout
	Source correcture (DCF only)	RW	0	ms	ntsTSDCFAdjusment
	Synch only offset	RW	off	ms	ntsTSOffsetSynchOnly
	Leap second mode	RW	off		ntsTSLeapSecMode
	Leap second date next correcture	RW			ntsTSLeapSecDate
NTP:					**ntsTimeNTPServer**
	4 * NTP source				ntsNTPSourceTable (1..4)
	Addresses	RW			ntsNTPSourceAddr
	Minpoll	RW		2^x sec	ntsNTPSourceMinPoll
	Maxpoll	RW		2^x sec	ntsNTPSourceMaxPoll
	Mode	RW	server		ntsNTPSourceMode
	Prefer(red time source)	RW	normal		ntsNTPSourcePrefer
	Key	RW	off		ntsNTPSourceKey
	2 * Broadcast:				
	Send address	RW			ntsNTPBrodacstAddr**x**
	Interval	RW	2 -> 4s	2^x sec	ntsNTPBrodcastInterval**x**
	Multicast TTL	RW	1		ntsNTPBroadcastTTL**x**
	Key	RW	off		ntsNTPBroadcastKey**x**
	Trusted Keys	RW			ntsNTPKeyTrusted
	Control Key	RW	0		ntsNTPKeyControl
	Request Key	RW	0		ntsNTPKeyRequest
	Autokey Password	RW			ntsNTPAutokeyPassword
					ntsNTPKeyGeneratorCmd
					ntsNTPKeyFileCmd
Manual Time set					**ntsTimeManualSet**

	Time	W			ntsManualTimeSetUTC
	Diff	W		ms	ntsManualTimeSetDiff
Product Info					**ntsProdInfo**
	Prod. Number	*R*			*ntsProdInfoProdNo*
	Article number	*R*			*ntsProdInfoArticleNo*
	HW revision	*R*			*ntsProdInfoHWRevision*
	HW code	*R*			*ntsProdInfoHWCode*
	HW name	*R*			*ntsProdInfoHWName*
	Firmware version	R			ntsProdInfoFirmwareVer
System Info					
	NTS state	R			ntsSysStatus
	NTS alarms	R			ntsSysAlarms
	Alarm relay state	*R*			
	SNMP alarms (masked)	R			
Trap Info					
	Trap state	R			
	Trap alarm number	R			
	Trap error state	R			
	Trap time	R			
	Trap message	R			
Time Info					**ntsSystemTimeInfo**
	NTS stratum	R			ntsTinfoStratum, ntsSysStratum
	Last drift	R			ntsTinfoLastDrift, ntsSysLastDrift
	Current offset sec	R		sec	ntsDCFTInfoOffsetSec
	Current offset us	R		us	ntsDCFTInfoOffsetUSec, ntsSysOffset
	Time of last time info	R			ntsTInfoLastTime
	Source Type	R			ntsSysTimeSource
	Last DCF time	R			ntsDCFTInfoLastTime
	DCF pulse counter	R			ntsDCFTInfoSecCount
	DCF Stratum	R			ntsDCFTInfoStratum
	DCF number of sat	R			ntsDCFTInfoSatNbr
	NTP source	R			ntsNTPTInfoCurrentSource
	NTP offset	R			ntsNTPTInfoSystemOffset
	NTP Jitter	R			ntsNTPTInfoSourceJitter
	NTP Stratum	R			ntsNTPTInfoStratum
	NTP Frequency	R			ntsNTPTInfoFrequency
	NTP Reach	R			ntsNTPTInfoReach
Versions					**ntsSystemVersions**
	Version NTS application	R			ntsVerApplication
	Version NTS module	R			ntsVerTimeDriver
	Version NTP	R			ntsVerNTP
	Version kernel	R			ntsVerLinux
	Version busybox (CLI)	R			ntsVerCLIShell
	Version rootfs	R			ntsVerRootFS
	Version language	R			ntsVerLangResource
	Version TZ table	R			ntsVerTimezoneTable
	Version snmp master	R			ntsVerSNMPMasterAgent
	Version snmp common	R			ntsVerSNMPSubAgent
Network Info					**ntsNetworkInfo**
	IP v4	R			ntsNetInfoIPAddr
	GW v4	R			ntsNetInfoIPGateway
	Subnet v4	R			ntsNetInfoIPMask
	DNS v4	R			ntsNetInfoIPNameserver
	Hostname	R			
	Domain	R			ntsNetInfoDomain
	DHCP	R			ntsNetInfoDHCPMode
	Link	R			ntsNetInfoEthernetLinkMode
	IP v6 link local	R			ntsNetInfoIPv6AddrLocal
	IP1 v6	R			ntsNetInfoIPv6Addr1
	IP2 v6	R			ntsNetInfoIPv6Addr2
	GW v6	R			ntsNetInfoIPv6Gateway
Commands					**ntsSystemMaintenance**
	Update cmd.	W			ntsSysUpdateCmd
	Backup cmd.	W			ntsSysBackupCmd
	Restore cmd	W			ntsSysRestoreCmd
	Restore default cmd	W			ntsSysDefaultCmd
	Restart cmd	W			ntsSysRestartCmd
	Set all config changed	W			ntsSysAllChanged

G Technical data

Dimensions	44 x 170 x 85 (H x W x D [mm] without plug) optionally with mounting brackets: 19” rack, 1HU x 28DU = 44 x 483 x 85 (H x W x D [mm] without plug)
Weight	approx. 1.35 kg
Ambient temperature	-5 to 50ºC, 10-90% relative humidity, without condensation
Operation	Telnet or SSH as well as MOBA-NMS (via LAN) In addition, operation is also possible with SNMP.
Accuracy	GPS (DCF input) to NTP server: typical < +/- 0.5 ms DCF 77 radio receiver to NTP server: typical < +/- 5 ms [1)] NTP client to NTP server: typical < +/- 0.5 ms GPS (DCF input) or NTP client to clock lines typical < +/- 0.5 ms + accuracy of the clock line [1)] If necessary, the DCF source must be corrected with an offset (see menu: local time source ➔ 3 DCF/GPS source correcture)

Notice: NTP reception (NTS as client or as server to external clients) can be influenced by the network traffic load and network devices (Hub, Switch, Router, Firewall...). If many clients request simultaneously, the typical accuracy may not be reached. Condition for NTp accuracy: poll interval: minimum 3, maximum 6.

Time keeping (internal)	After at least 24 hours of synchronization from the time source: < +/- 0.1 sec. / day (< 1 ppm), measured during 24 h, at 20°C +/- 5°C. In case of a loss of feed (based on internal RTC): < 5 ppm, but with jitter of +/- 15 ms, measured over 24 h, at 20°C +/- 5°C. (After 24 h, the deviation may increase further due to quartz aging) The RTC time is available for at least 5 days after the loss of feed (RTC supported by SuperCap).
Time server	NTP V4 (fully V3 compatible), RFC 1305 (Port 123) NTP authentication with MD5 key / autokey SNTP (UDP), RFC 2030 (Port 123) TIME (TCP/UDP), RFC 868 (Port 37) DAYTIME (TCP/UDP), RFC 867 (Port 13) Max. number of NTP and SNTP client requests: > 250 requests / sec. (e.g. client requests every 60 seconds ➔ 15000 clients)
NTP Mode	Server, Peer, Broadcast, Multicast
NTP slave clock lines:	1 line with up to 15 different time zone entries. Communication through multicast: -RFC 3376: Internet Group Management Protocol, Version 3 -RFC 1112: Host extensions for IP multicasting -RFC 4601: Protocol Independent Multicast - Sparse Mode (PIM-SM) -RFC 3973: Protocol Independent Multicast - Dense Mode (PIM-DM)
Time zones (see App. B)	Up to 80 predefined, 20 programmable entries (MOBA-NMS)
Network interface	10BaseT / 100BaseTX (IEEE 802.3) Data transmission rate: Auto-negotiation / manual Connection: RJ-45 Only shielded cables permitted.
IP Configuration	DHCP, Static IP, IPv4, IPv6

Network services	NTP	UDP, Port 123	see timeserver
	SNTP	UDP, Port 123	see timeserver
	TIME	TCP/UDP, Port 37	see timeserver
	DAYTIME	TCP/UDP, Port 13	see timeserver
	Telnet	TCP, Port 23	operation
	SSH	TCP, Port 22	operation
	SCP	über SSH	update
	SFTP	über SSH	update
	FTP	TCP, Port 21	update
	SNMP	UDP, Port 161	operation
		UDP, Port selectable (162)	alarm notification, see SNMP
	SMTP	TCP, Port selectable (25)	alarm mail see E-Mail
	DHCP	UDP, Port 68	dyn. address allocation (client)
	DNS	TCP/UDP, Port 53	address resolution (client)
	DHCPv6	only IPV6	
	ECHO	ICMP	“Ping“

SNMP	V1, V2c, V3 with MD5 for authentication and DES for encryption (privacy).
E-mail	Alarm reporting via SMTP. Authentication at the mail server: - with sender address - with username/password SMTP-Auth with LOGIN, PLAIN (RFC 4954) or CRAM-MD5 (RFC 2195) no “POP before SMTP“ possible
DCF Input	DCF77 or DCF from GPS, current loop active (nominal 24VDC) max. 32mA, response threshold 8mA, time zone selectable
DCF / pulse output	DCF time code or Synch-Pulse output selectable. Passive power interface Umax = 30 VDC, I_{on} = 10..15 mA, I_{off} < 1 mA @20VDC Cable length max. 30 m (not in the 3-m area of a contact line (rail)). DCF output: Time zone selectable Pulse modi: Second, minute, hour, user-defined interval: 1-3600 sec. Pulse length: 20 – 500 ms, jitter pulse length: +/- 2 ms Max. deviation from internal time: +/- 1 ms, jitter pulse start < 0.5 ms
Alarm reporting / Error reporting	E-Mail see E-Mail SNMP-Notification see SNMP-Trap Alarm LED -
DC power supply	24 – 28 VDC / 200 mA typical: < 75 mA @ 28 VDC with GPS4500 < 60 mA @ 28 VDC without external load
Mains power supply	external power pack (Lieferumfang) 100 – 240 VAC / 50 - 60 Hz / max. 12 W typical: < 7.5 VA @ 230 VAC with GPS4500 < 6.5 VA @ 230 VAC without external load
Power supply output	nominal 24 VDC, max. 200 mA (for GPS receivers)

H Index

I Connection table (to fill in)

Line	Type	Description

Example:

Line	Type	Description
DCF	DCF out	*DCF for master clock ETC1*

HEADQUARTERS / PRODUCTION

MOSER-BAER AG
Spitalstrasse 7, CH-3454 Sumiswald
Tel. +41 34 432 46 46 / Fax +41 34 432 46 99
moserbaer@mobatime.com / www.mobatime.com

SALES WORLDWIDE

MOSER-BAER SA EXPORT DIVISION
19 ch. du Champ-des-Filles, CH-1228 Plan-les-Ouates
Tel. +41 22 884 96 11 / Fax + 41 22 884 96 90
export@mobatime.com / www.mobatime.com

SALES SWITZERLAND

MOBATIME AG
Stettbachstrasse 5, CH-8600 Dübendorf
Tel. +41 44 802 75 75 / Fax +41 44 802 75 65
info-d@mobatime.ch / www.mobatime.ch

MOBATIME SA
En Budron H 20, CH-1052 Le Mont-sur-Lausanne
Tél. +41 21 654 33 50 / Fax +41 21 654 33 69
info-f@mobatime.ch / www.mobatime.ch

SALES GERMANY, AUSTRIA

BÜRK MOBATIME GmbH
Postfach 3760, D-78026 VS-Schwenningen
Steinkirchring 46, D-78056 VS-Schwenningen
Tel. +49 7720 8535 0 / Fax +49 7720 8535 11
buerk@buerk-mobatime.de / www.buerk-mobatime.de