Network Time Synchronisation
USER MANUAL
Time Server NTS
ELPROMA NTS–3000

ELPROMA Electronics
www.elproma.com

March 31, 2003

Contents

1 Introduction **4**

2 Hardware **5**

3 Mounting GPS antenna **7**

4 Mounting backup DCF antenna (optionally) **8**

5 Powering up NTS-3000 **9**

6 Error messages **10**

7 NTP - Network Time Protocol **11**

8 NTP on Time Failure Tolerance network **14**

9 NTS-3000 software Setup **15**

10 Security and NTP authentication mode **23**

11 NTPq client diagnostic utility **25**

12 Installing NTP client software **27**
12.1 Windows 95/98/Me 28
12.2 Windows NT/2000/XP 29
12.3 UNIX family systems 30
12.4 Novell NetWare 31
12.5 IBM AIX (RS6000) 32

13 Technical specification: **33**
13.1 SYSTEM 33
13.2 HARDWARE 33
13.3 CASE 34
13.4 GPS 34
13.5 POWER 34
13.6 ACCURACY 34
13.7 OTHER 35

List of Figures

1 Front panel of NTS–3000. LAN ports 5
2 Back panel of NTS–3000 5
3 GPS world wide time propagation 7
4 NTS–3000 GPS antenna and converter box 7
5 GPS antenna installation 8
6 NTS–3000 LCD display 9
7 Error missing GPS satellites 10
8 Error NTP failure 10
9 Motorola RAIM error 10
10 Time Adjustments Using Stepping and Slewing 12
11 Strata tree 12
12 Example of NTP stratum configuration in local LAN peer 13
13 NTS–3000 front panel 15
14 Main menu 15
15 Entering IP address 16
16 Entering MASK address 16
17 Entering DEFAULT GATEWAY address 17
18 Enabling/Disabling remote access to NTS–3000 17
19 Enabling SYSLOG 18
20 Enabling SNMP MIB2 service 18
21 Defining list of NTP backup servers (Stratum 1) 19
22 Setting RTC date 19
23 Setting RTC time 20
24 Saving RTC date and time 20
25 Authentication utilities 21
26 Other functions 21
27 Accessing NTS-3000 via web browser 22
28 Broadcast NTP mode 24
29 MD5 keyid for broadcast mode 24
30 NTPq diagnostic for Windows NT/2000/XP 25
31 NTP client for Windows 95/98/Me 28
32 NTP client setup - 1st IP address for local clock 29
33 File ntp.conf 29
34 NTP client config for NetWare stored in file sys:etc\sntpcln3.cfg 31
35 NTP client for NetWare 3.xx, 4.xx, 5.xx 31

List of Tables

1 RS–232 (Terminal/Setup) cable configuration 34

1 Introduction

The NTS–3000 Network Timeserver provides a high precision time directly to TCP/IP networks using NTP (Network Time Protocol). It synchronizes time of any NTP clients running on remote PC's. It supports both NTP and SNTP clients for more of current popular operating systems including: Microsoft Windows 95/98/Me/NT/2K/XP, Linux, FreeBSD, HP-UX, IBM AIX, IBM AS/400, SUN and other UNIX family systems. It can synchronize simultaneously thousands of servers, workstations and routers, including all CISCO products.

The high precision UTC time is powered by cesium atomic clocks coming via GPS (Global Positioning System) satellite system. The independent DCF77 antenna can be connected optionally too. Both antennas works redundant.

The NTS–3000 distributes UTC reference time to 3 isolated and not routed Ethernet 10/100Mbs sub-networks. All time and satellite information is traced on front panel 2x20 character LCD. More detailed statistic is available by remote NTP software: standard NTP utilities "ntpq", "ntpdc", WWW service (both HTTP and HTTPS), TELNET, SSH, SNMP.

The NTS–3000 ideally suits for delivering system-wide for data transmit encryption, NASD brokers, financial institutions, network security, e-commerce and B2B transactions. It supports official timestamps (200pS resolution) and it can operate in NTP authentication mode protected by MD5 algorithms. Unit supports broadcast, manycast, multicast and passive client/server mode of time synchronization.

Special mode of fast NTP startup has been implemented to reduce unsynchronized startup time after powering up CISCO products (which has no battery powered RTC clock). NTS–3000 is ready to work with any SYSLOG or SNMP (MIB2) server. It let friendly warn you on any unexpected situation may happen on you time synchronized network.

The installation of NTS–3000 timeserver is very easy. It simply requires basic TCP/IP address (IP, MASK, GATEWAY) to be set up by ordinary terminal program (e.g. Windows Hyper Terminal). This software can be executed on any remote PC connected to NTS–3000 via RS-232 cable. Once the unit has been configured it is ready to work with more tracing services as e.g. : www, ssh, telnet, snmp, ntpq or ntpdc. Those utilities can be a specially very useful in large organizations or for using multiple NTS–3000 units.

2 Hardware

The NTS–3000 timeserver set includes:

- NTP timeserver unit (rack19 mounted 1U)
- GPS antenna with 200m. cable and frequency converter with built-in over voltage protection
- DCF77 antenna with 20m. cable /optionally/
- RS-232 configuration cable
- Power cable 230V
- CD with software utility and PDF manual

Timeserver unit is a multiprocessor system with 3 not depended (not routed) fast Ethernet 10/100Mbs interfaces. It is design and manufactured without ventilators, fens or any other mechanical parts. Metal housing is an important part of NTS–3000 cooling system but it is designed on a way that NTS–3000 can be located in the neighborhood of any device working inside rack19 mount frame.

Single serial (9pin D-SUB connector) port is dedicated for setup utility, but it can be also used to connect DCF77 antenna (option) later on. The 2x20 char LCD shows GPS communication and timestamp information.

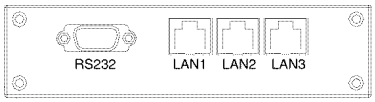

Figure 1: Front panel of NTS–3000. LAN ports

Figure 2: Back panel of NTS–3000

All LAN connectors contains 2 led: yellow indicates cable connection, green one flashes while data transmission.

On the back panel there is a power connection 230V AC (50Hz) and GPS antenna rounded connector.

NTS–3000 has 2 independent build-in power supplies: one for powering server unit and the second one for powering the GPS antenna. The optional backup DCF77 antenna is powered via RS232 signal lines.

Important Note!

The NTS–3000 has been designed for standard as well as military purposes. In case of using NTS–3000 inside time critical environments please use double or triple cable connections for single subnet. This allows to minimize probability of loosing high precision time synchronization in case of any unexpected cable disconnections or poor quality cabling.

3 Mounting GPS antenna

The GPS satellite time receiver has been designed to provide extremely precise time. High precision available 24 hours a day around the whole world is the main feature of the new system which receives its information from the satellites of the Global Positioning System. The Global Positioning System (GPS) is a satellite-based radio-positioning, navigation, and time-transfer system. The source of time is based on real cesium atomic clocks. Time is represented as UTC (GMT).

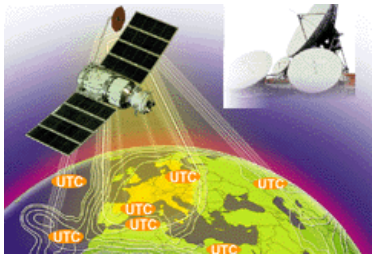

Figure 3: GPS world wide time propagation

The GPS satellites are not stationary but circle round the globe in a period of about 12 hours. They can only be received if there is no building in the line-of-sight from the antenna to the satellite, so the antenna unit must be installed in a location from which as much of the sky as possible can be seen.

Figure 4: NTS–3000 GPS antenna and converter box

The hardware of the GPS antenna contains 2 boxes. The smaller one is a miniature GPS (IP68) antenna with a magnetic footer. This allows antenna be easily to be mounted on any metal part of the roof. This antenna is connected by 5m. coaxial cable (50 ohm) to 1.5GHz frequency converter (IP65). The standard outgoing cable length is 200m and it can not be shortcuted nor expanded. For this reason please use the length of cable you need and leave the remind cable inside the box. Both boxes are water resistance, therefore they should stay over the water level during a rain.

4 Mounting backup DCF antenna (optionally)

Enterprise edition of NTS–3000 includes also a second DCF77 antenna with 20m long cable. For a standard edition of NTS–3000 this reminds as an open option.

The DCF77 radio signal is send via long waves (77.5kHz) from Frankfurt (Germany) and it can be use in area of 1200km around Frankfurt. For this reason many neighborhood countries can still use this signal with no disturbs. However this is valid only for Middle and Western European locations. Other locations can order NTS–3000 with a special emulation antenna of DCF77 based on GPS receiver.

The DCF antenna can be located inside on any place. The red LED indicates signal level and it should flush 1Hz (1PPS one pulse per second) on a regular way. But before it will flash, DCF77 antenna must be correctly initialized by selecting specific field inside SETUP software described later on in this manual. Therefore we suggest to wait with setting up DCF77 antenna until you learn more how to configure NTS–3000 SETUP. For this moment connecting GPS antenna is more than you need to start work with NTS–3000.

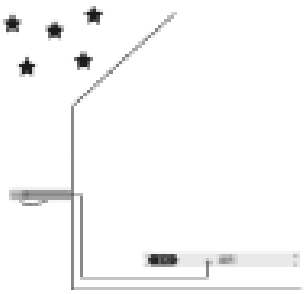

Figure 5: GPS antenna installation

5 Powering up NTS-3000

If both the GPS antenna and the power supply have been connected the system is ready to operate. The DCF77 optional antenna should be connected later on due to the fact that it requires prior software SETUP configuration. Besides that you are ready now to turn on the power.

About 120 seconds after power-up the receiver is warmed up and starts to operate with the required accuracy. If the GPS receiver finds valid almanac and ephemeris data in its battery buffered memory (and the receiver position has not changed significantly since its last operation) the receiver can find out which satellites are in its view at that now. Only a single satellite needs to be found to synchronize and generate output pulses, so synchronization can be achieved maximally two minutes after the powerup.

If the receiver position has changed by some hundred kilometers since the last operation, the satellites real elevation and Doppler might not match the values expected by the receiver thus forcing the receiver to start scanning for satellites. When the receiver has found four satellites in its view it can update its new position and switch to *Normal Operation*. If the almanac has been lost because the battery had been disconnection the receiver has to scan for a satellite and read in the current almanacs. It takes up to 60 minutes until the new almanac is completed and the system starts to operate.

After starting up the system the network function is initiated and the program for communication between GPS and NTP becomes active. The following screen appear on LCD display while starting.

From the left side there are: time, day of week, error status, UTC time, number of satellites reached per total amount of visible satellites.

```
17-02-2000 Wed OK
18:02:21   ST= 5of12
```

Figure 6: NTS–3000 LCD display

Important Note!

The NTP starts max. 5 minutes after powering ON it does not matter what status of GPS or DCF77 signal is available. If for that moment GPS is still not ready, the NTP looks for DCF77. If both signals are not ready, NTS–3000 runs NTP based on RTC and later swaps to GPS or DCF77 when ready.

It is possible to setup much shorter startup time of NTP (about 1 minute) by selecting a special option in SETUP. This can be helpful for environments with a high risk of unexpected power down.

6 Error messages

The NTS–3000 requires min. 3 satellites to be reached continuously. This figure is not constant and it is changing on non-regular way. If satellite communication is lost the following message appears:

```
17-02-2000 Wed Err2
18:02:21   ST= 1of12
```

Figure 7: Error missing GPS satellites

This requires finding better GPS antenna location otherwise NTS–3000 cannot guarantee a high precision of time anymore. The unit will still work properly but the time source will be switched to DCF77 or RTC clocks.

The LCD shows only a status of the GPS antenna. It does not show status of the DCF-77 antenna. However DCF-77 can be monitored and traced by a remote software utility (`cl num` command of `ntpq` utility, where *num* can be guessed from `as` command).

The Err 3 indicates internal NTP problems. If this message reminds for more than 1 hour we advice to reset the unit. There is no risk that NTS–3000 will lose its precision for such a short period. However, if the problem repeats continuously, please contact your local technical support.

```
17-02-2000 Wed Err3
18:02:21   ST= 4of12
```

Figure 8: Error NTP failure

There is one more error message Err 1 possible to display. It indicates RAIM algorithm error called by Motorola GPS hardware. We advice to check your antenna installation if this message appears and restart the unit. If problem reminds unchanged we suggest to contact your local technical support.

```
17-02-2000 Wed Err1
18:02:21   ST= 5of12
```

Figure 9: Motorola RAIM error

7 NTP - Network Time Protocol

Before you learn how to setup NTS–3000, you also should read about what NTP itself.

NTP is a common method for time synchronization over networks. It is a protocol but a very special one. The NTP is much different from any of known other communication protocols. It is because NTP does not base on the principles of synchronizing machines to each other. It is based on the principles of having all machines get as close as possible to the UTC time provided by NTS–3000. How it works?

NTS–3000 forms a statistic of delays and other data necessary to calculate local client RTC offset. Knowing time difference the adjustment of the own RTC clock can be preceded individually by each NTP client.

NTP works on a hierarchical model in which a small number of servers gives time to a large number of clients. The clients on each level, or stratum, are in turn, potential servers to an even larger number of clients on a higher numbered stratum. Stratum numbers increase from the primary (stratum 1) servers to the lowest numbered strata at the bottom of the tree (stratum 15). Clients can use time information from multiple servers to determine automatically the best source of time and prevent wrong time sources from corrupting their own time.

For sure it may take several minutes (or even hours) to adjust a system time to the ultimate degree of accuracy. There are several reasons for this. The most important one is that NTP averages the results of several time exchanges in order to reduce the effects of variable latency. This may take several minutes for NTP to even reach consensus on what the average latency is. Generally it happens in about 5-10 minutes. In addition, it often takes several adjustments for NTP to reach a synchronization. The result is that users should not expect NTP to immediately synchronize two clocks. The ntpdate command can be used if an instant synchronization is needed.

The *peers* command can be used in `ntpq` to determine wheather the synchronization has been achieved. When a client has synchronized, the synchronization server is listed with an asterisk in front of it.

To allow clocks to quickly achieve the high accuracy, yet avoid overshooting the time with large time adjustments, NTP uses a system where large adjustments occur quickly and small adjustments occur over time. For small time differences (less than 128 ms), NTP uses a gradual adjustment. This is called slewing. For larger (but still less than 17 minutes) time differences, the adjustment is immediate. This is called stepping.

If the accuracy of a clock becomes too insufficient (off by more than about 17 minutes), NTP aborts the NTP daemon, with the assumption that something has gone wrong with either the client or server. In order to synchronize well with a server, the client needs to avoid step adjustments.

Due to NTP specification NTS–3000 is visible over network as a peer. Single peer can contain more than single timeservers in order of a hierarchy called stratum. The top of the stratum tree is preserved for radio-controlled timeservers such as NTS–3000. Therefore NTS–3000 will always be your *stratum1* timeserver. Other connected computers can also work in timeserver mode but they will be set down to *stratum2* or even much below.

The NTS–3000 time server supports multiple source of time. Each source is Stratum 0 (except RTC working on Stratum 1 level). The enterprise of

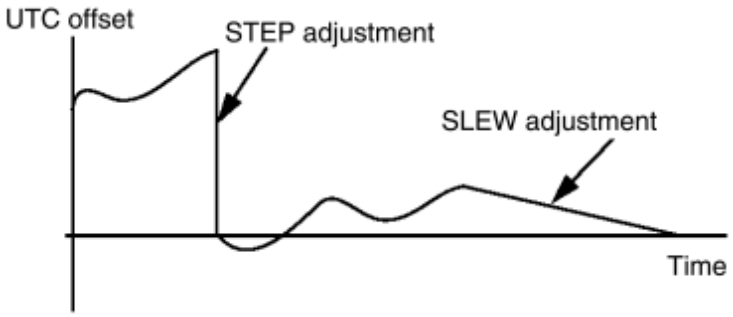

Figure 10: Time Adjustments Using Stepping and Slewing

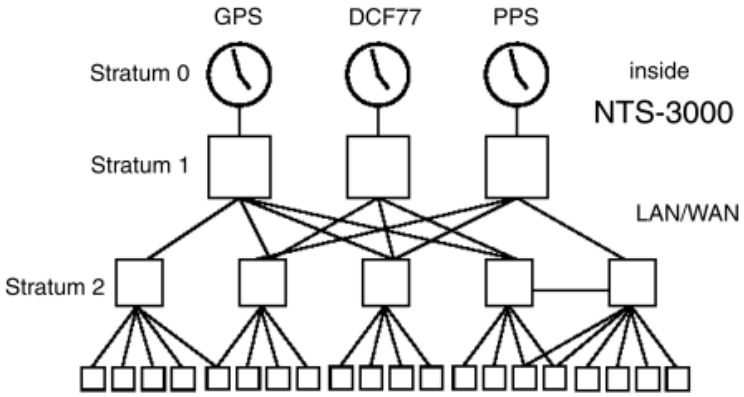

Figure 11: Strata tree

NTS–3000 configuration includes following time sources:

- PPS (pulse per second) signal PLL/FLL locked
- GPS 1.5GHz radio signal (worldwide)
- DCF77 [1] 55.7kHz radio signal (Europe only)
- RTC internal quartz clock systems for backup

A high precision synchronization is chosen by NTP automatically. The NTP always selects best available source of time. Selection is based on several time references like: stratum level, availability of timeserver, network delay, time difference, internal jitter factor etc.

NTP clients of NTS–3000 are referred to be a *Stratum 2 clients*. If they serve time to other clients, they are also referred as *Stratum 2 servers*. The maximum NTP stratum number for a client is 15.

NTP uses the UDP protocol on port 123 to communicate between clients and servers. Attempts are tried at designated intervals until the server responds.

[1] For countries located outside Europe, the 2nd antenna can be easily replaced by special DCF77 emulation antenna set based on the GPS radio signal. All antennas works redundantly and they are NTP visible as Stratum 0.

The interval depends on a number of factors and ranges from about once a minute to once every 17 minutes. Using UDP prevents retries from using up network bandwidth if a time server with a large number of clients goes down. The bandwidth requirements for NTP are also minimal.

Unencrypted NTP Ethernet packets are 90 bytes long (76 bytes long at the IP layer). A broadcast server sends out a packet about every 64 seconds. A non-broadcast client/server requires 2 packets per transaction. When the first starts, transactions occur about once per minute, increasing gradually to once per 17 minutes under normal conditions. Poorly synchronized clients will tend to poll more often than those well synchronized clients. Starting from NTP version 4 implementations, the minimum and maximum intervals can be extended beyond these limits, if necessary.

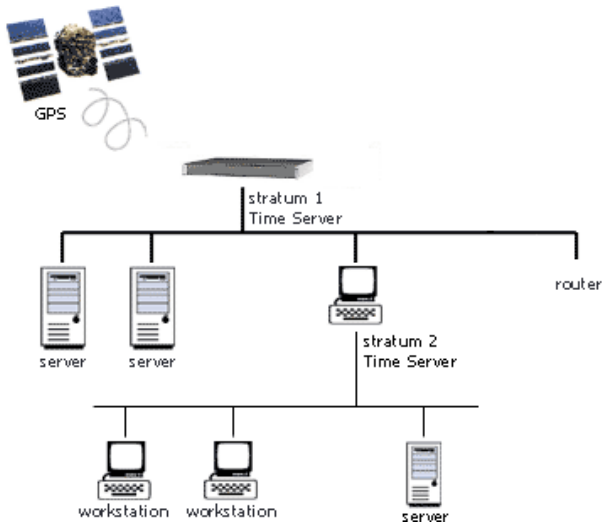

Figure 12: Example of NTP stratum configuration in local LAN peer

8 NTP on Time Failure Tolerance network

Dual antenna (GPS, DCF77) system of NTS–3000 already improves safety because it protects situation when a single antenna could fail. But it is also possible to use several NTS–3000 units simultaneously to improve stability of the time synchronization. In this case all NTS–3000 units would work independently and fully redundant. If one server fails another are still working and NTP swaps to the new existing source automatically.

There is actually one more possibility of NTS–3000. You can define up to 3 NTP backup servers for single NTS–3000 unit. In this mode NTS–3000 reminds Stratum 1 as long as GPS (or DCF77) antenna works fine. But in case of a missing antenna signal NTS–3000 checks backup servers list. If NTP accepts any of them, the NTS–3000 reduces its stratum to N-1 (where N is a Stratum of approved server taken out of the backup list). We advice to specify only Stratum 1 servers on NTS–3000 backup list. This does not let reduce NTS–3000 Stratum below 2.

Every NTS–3000 includes built-in RTC clock. If there is no time source (all antennas are disconnected and the list of NTP backup servers is empty), NTP will choose RTC. In this case NTS–3000 Strata will be reduced to 2.

9 NTS-3000 software Setup

For the very first time of installation the NTS–3000 has to be configured by RS–232 remote terminal software. Please connect your serial cable to NTS–3000 (RS232 front panel port). Other side of cable please connects to any available computer and run any simple terminal (e.g Windows Hyper Terminal) program with serial communication set to: 9600,8,1,n

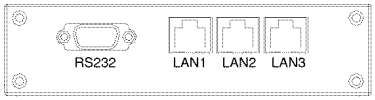

Figure 13: NTS–3000 front panel

Once terminal is connected the setup appears automatically (after pressing ENTER) on screen:

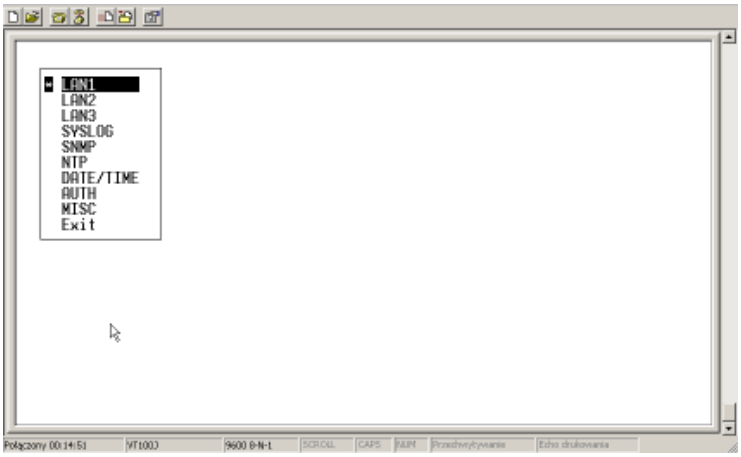

Figure 14: Main menu

To start configuration you shod first configure all LAN interfaces by simply placing IP, MASK, DEFAULT GETEWAY for each Ethernet card (LAN1, LAN2, LAN3).

In addition you can specify what mode you want to work NTS–3000 on specific LAN interface. You can enable extra broadcast and multicast modes running in the background of standard client/server mode, but we suggest to finish basic configuration first before you go to more advanced options. Therefore please leave those options for the moment now by simply filling fields 0.

Now its time to decide what other remote services you like to keep active for future accessing of NTS–3000. You access each LAN separately:

- Enable/Disable access via Telnet
- Enable/Disable access via SSH
- Enable/Disable access via HTTP
- Enable/Disable access via HTTPS

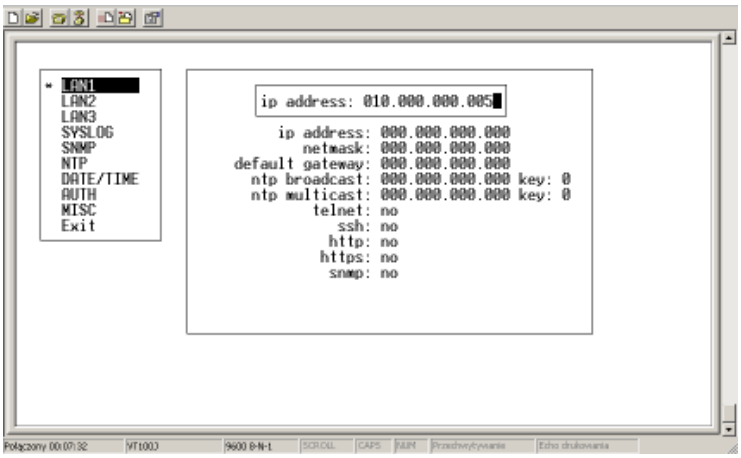

Figure 15: Entering IP address

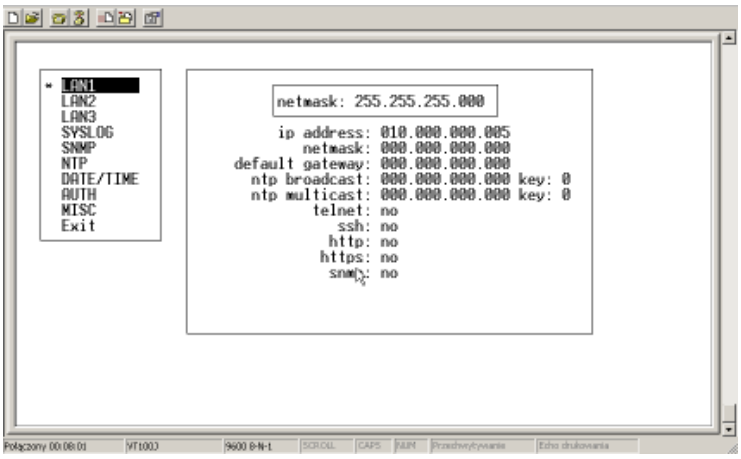

Figure 16: Entering MASK address

- Enable/Disable access via SNMP (MIB2)

Now you should repeat listed above steps for LAN2 and LAN3. You can also specify SYSLOG server for future tracing functionality. You can configure facility and verbosity of NTS–3000 messages, to ease log segregation on your syslog server. Please read your syslog documentation – syslog(8) – for details about logs gathering.

If your network support SNMP, you can configure special MIB2 traps to implement exceptional facts you can be interesting in. It is very easy to set traps on such way that you will be informed by mail or mobile phone (SMS) on any unexpected situation may occur inside NTS–3000 like e.g. losing GPS antenna etc. Also you can trace all TCP/IP statistics using your favorite SNMP client software (ie. *mrtg*).

Another step is you can define up to 3 NTP backup servers for single NTS–3000 unit. In this mode NTS–3000 reminds Stratum 1 as long as GPS (or

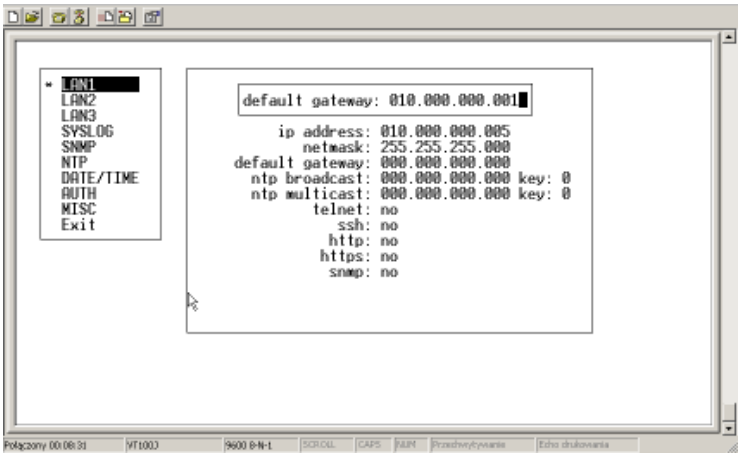

Figure 17: Entering DEFAULT GATEWAY address

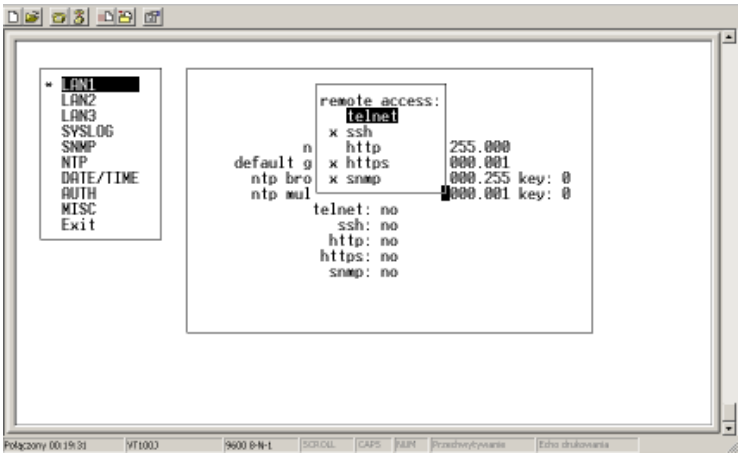

Figure 18: Enabling/Disabling remote access to NTS–3000

DCF77) antenna works fine. But in case of missing antenna signal NTS–3000 checks backup servers list. If NTP accepts any of them the NTS–3000 reduce its stratum to N-1 (where N is a Stratum of approved server taken out of backup list). We advice to specify only Stratum 1 servers on NTS–3000 backup list. This does not let reduce NTS–3000 Stratum below 2.

The backup NTP servers should be configured for authorized NTP transmission. For this reason there is another field key pointing position in encryption list with MD5 keys. But in this step we still advice to continuous Setup without encrypted associations. Safety and protection will be discussed shortly in this manual.

NTS–3000 can work with no GPS nor DCF77 source of time. It can even operate with no backup NTP servers, just based on internal RTC source of time.

For that reason you need to be able to set up manually UTC date and time. However you dont have to do it because once GPS (or DCF77) signal is starting to be receive that automatic RTC synchronization is proceeded. Therefore we

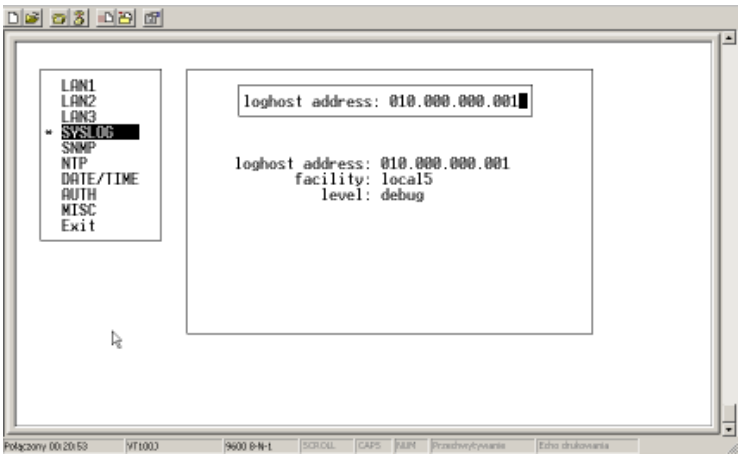

Figure 19: Enabling SYSLOG

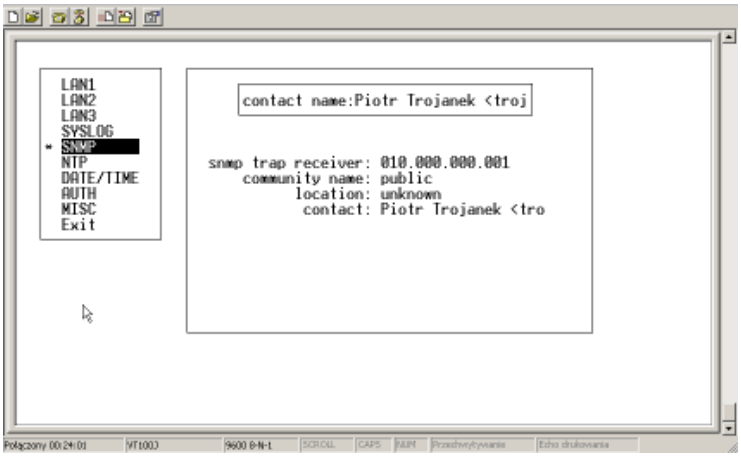

Figure 20: Enabling SNMP MIB2 service

advice to dont use facility if you do not plane to run NTS–3000 with no antennas.

Important Note!

Setting date and time manually you always need to be careful. It is extremely important to input reliable UTC time manually. If GPS (DCF77) starts with a RTC time/date difference larger than 17 minutes the adjustment will be not proceeded and NTS–3000 reminds running based on RTC source of time. You need to refer to NTP specification for better understanding this way of beehive.

NTS–3000 is ready to work in NTP authentication modes. This is valid for all modes of synchronization including:

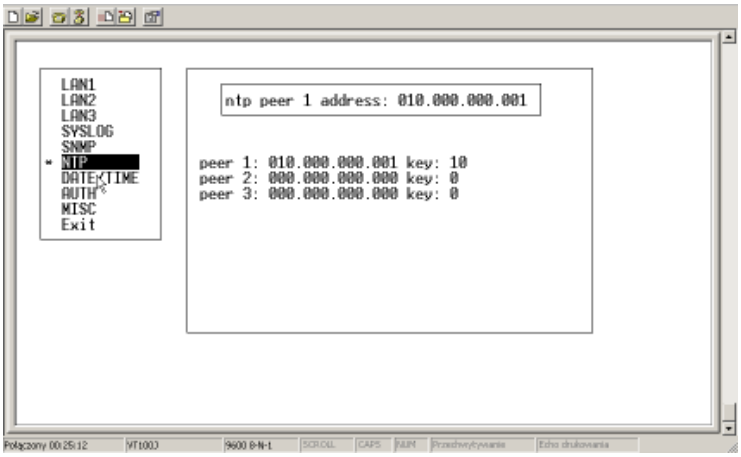

Figure 21: Defining list of NTP backup servers (Stratum 1)

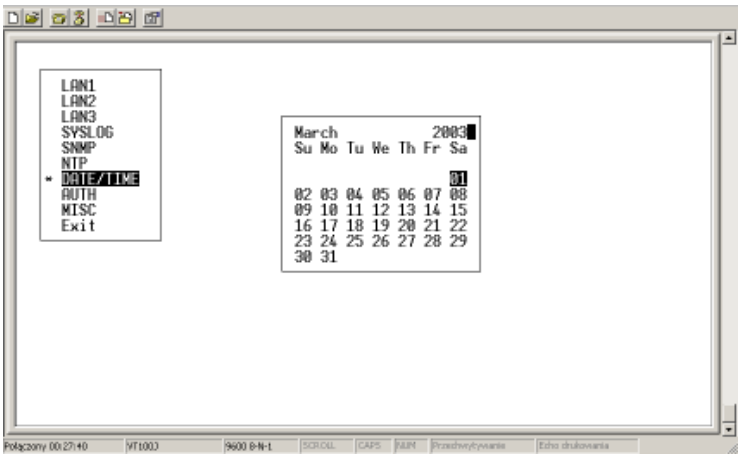

Figure 22: Setting RTC date

- broadcast,
- multicast,
- client/server

and NTP backup communication.

This screen helps you generate SSL and SSH keys. You can also edit MD5 keys, but generation is not supported by NTS–3000.

Changing password allows you to protect against unauthorized remote access to NTS–3000. We advice to use min. 8 character passwords.

Enbling/Disabling DCF77 antenna requires good understanding DCF77 connection works. Please read it before you go forward!

Both setup and DCF77 antenna are going to be connected to same RS–232 I/O port. It is designed on this way because we believe once you setup NTS–3000 there will be no necessary to change settings too often. Also DCF77 antenna

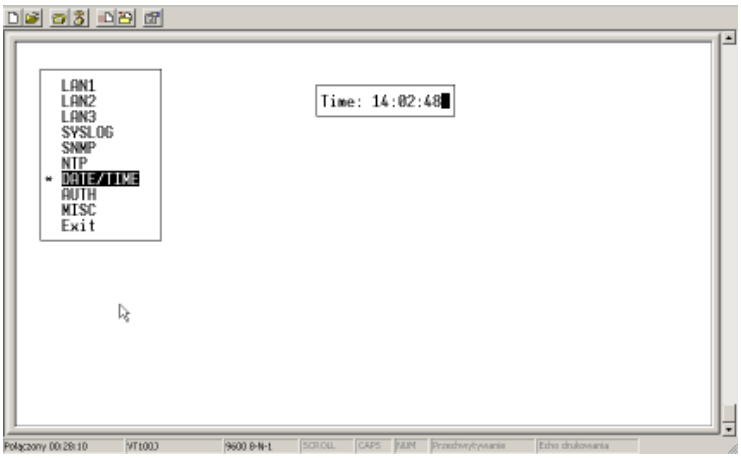

Figure 23: Setting RTC time

Figure 24: Saving RTC date and time

is something extra to main GPS antenna. Therefore once you turn on DCF77 antenna option and you save setting next time you will be able to access setup for 5 minutes only. After 5 minutes timeout will switch RS–232 to handle DCF77 antenna. So, if your next setup access will take too long all changes will be lost. Therefore if you like to change your settings slowly, please first disable DCF77 antenna option first and save settings again. This let you turn back to unlimited time of setup modification. Later on when changes are done you simply turn on DCF antenna option again and save setting. The DCF77 antenna cable can be simply connected and disconnected on fly. This also mean than DCF77 antenna can be ready to work as soon as 5 minutes passes since last setup save or power down/up routine. Than red led indication shows if your DCF77 signal is already receiving.

Fast NTP startup is an unique Elproma solution for situation where your network environment requires urgently ready NTP out of any NTS–3000 LAN output. Normal power up requires up to 5-10 minutes before NTP is ready

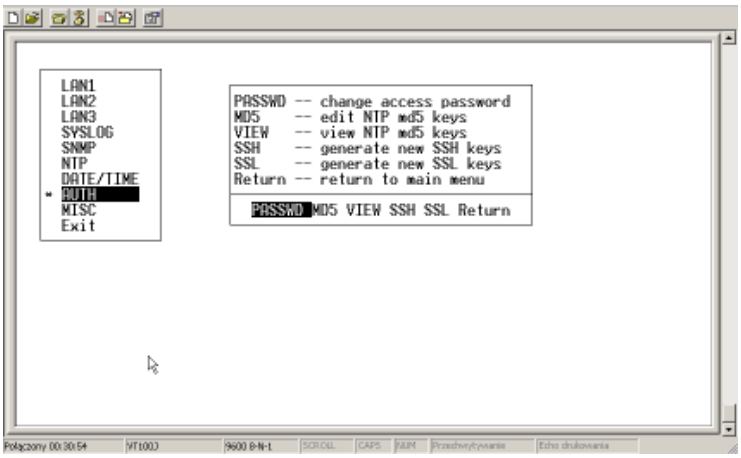

Figure 25: Authentication utilities

Figure 26: Other functions

to work. For some applications this time is too long even this is absolutely standard beehive of NTP stand up routine. Setting ON this option you simply make NTP startup time much shorter (max. 1 minute), however the price you pay for quick service is much poor time accuracy for first 10-15 of NTS–3000. We do not advice to use this option for users not experience so much on NTP synchronization.

Automatic Upgrade by Internet. Switching on this function you simply let NTS–3000 search internet for newer firmware version of NTS–3000. This is function was implemented for public Stratum 1 NTP servers constructed based on NTS–3000 hardware.

Once setup is done you have to exit with save option. Than NTS–3000 internally restarts NTP service. If you have switched on DCF77 antenna option now your 5 minute count down start for another new access with short setup modifications. If you do not plan to make any setup changes now it is time to connect you DCF77 antenna.

You can use simply any web browser (including Microsoft Explorer or Netscape) to access NTS-3000:

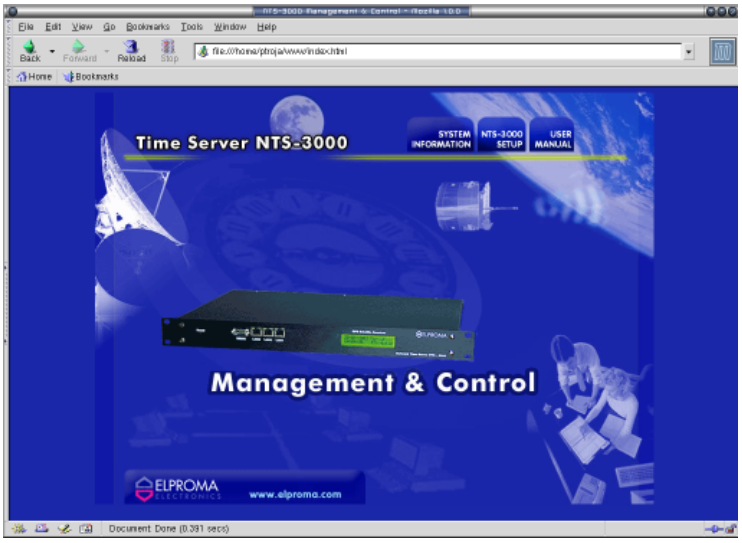

Figure 27: Accessing NTS-3000 via web browser

Following menu system in the top of page you will be able to get:

- System information
- Run Setup
- Read User Manual

To access first two of them you will be asked for PASSWORD first.

The NTS–3000 supports SETUP available via SSH and TELNET service. This WWW utility is intended as read-only fast way to look at working NTS–3000 unit.

You can also use SNMP service to indicate system failures and GPS problems.

10 Security and NTP authentication mode

The notion of accurate time is essential to determining the order in which events occur. This is a fundamental aspect of transactional integrity, system and networkwide logging and auditing, and troubleshooting and forensics. Having an accurate time source plays a critical role in tracing and debugging problems that occur on different platforms across a network. Events must be correlated with each other regardless of where they were generated. Furthermore, the notion of time (or time ranges) is used in many forms of access control, authentication, and encryption. In some cases, these controls can be bypassed or rendered inoperative if the time source could be manipulated. For example, a payroll function could be tricked into providing access over a weekend when normally it would be restricted to normal business hours. Many organizations have become reliant on NTP just as they are with other services such as the domain name service (DNS). This reliance can be a weakness if the service is not properly safeguarded. Therefore, it is important that these time sources are adequately protected against a wide array of threats, both internal and external, local and remote.

Time is not just an extraneous service. It is fundamental to the successful operation of todays environments. The most significant risks to NTP services are tampering and jamming. Tampering occurs when the NTP server is affected by either accidental or malicious data modification. Jamming occurs when a time server is either destroyed or prevented from providing NTP service. As with any other application, administrators must remember that NTP is not guaranteed to be secure; poor coding and other flaws in the program could allow unintended access to NTP internals or the underlying operating system. The NTP service is capable of protecting itself against some of these threats using architectural choices such as redundancy, and configuration options such as access control and authentication. Redundancy and its impact on an NTP implementation was discussed previously. Access control is achieved by restricting what NTP functions can be accessed from specific hosts or networks. Authentication is currently provided using symmetric keys that are installed on the NTP servers and clients.

NTP MD5 keying. NTP packets can be encrypted using standard MD5 algorithm. In this mode each packet is hashed using specified key number. In NTS–3000 you can use keys in range from 1 to 65000. Both sender and receiver of encrypted packet must have identical key (string) entered at the same numer (key id) to work.

You can enter and view NTS–3000 MD5 keys in AUTH menu. All entered keys are considered to be trusted for time service needs, but there is `default nopeer nomodify` restriction in NTS–3000 access control list.

You have to put the same keys at the same positions to file (`/etc/ntp.keys`) on client side. Please make sure that key file is not world readable – it should be owned by root (on UNIX platforms), and be chmoded to `0600`. Then you need to add `keys /etc/ntp.keys` line to your `/etc/ntp.conf` file.

You can have many NTP clients accessing NTS–3000 in bradcast and multicast modes. Please note, that in default client NTP setup these modes requre authenticated packets to work (unless you add `disable auth` line to your `ntp.conf` file).

Make sure, that you choose approiate broadcast and multicast address.

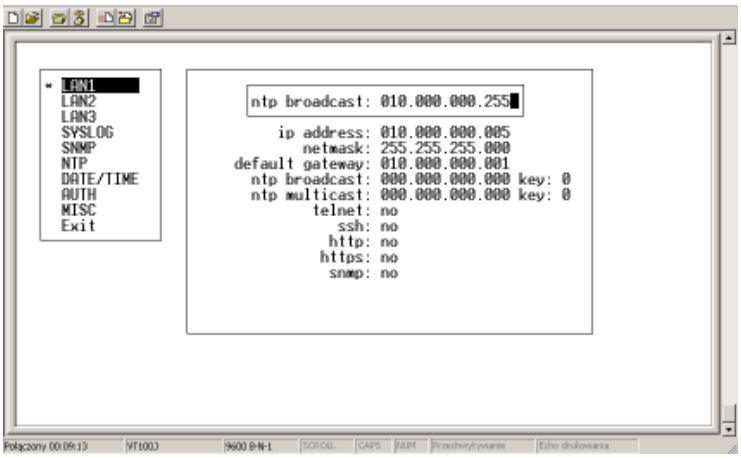

Figure 28: Broadcast NTP mode

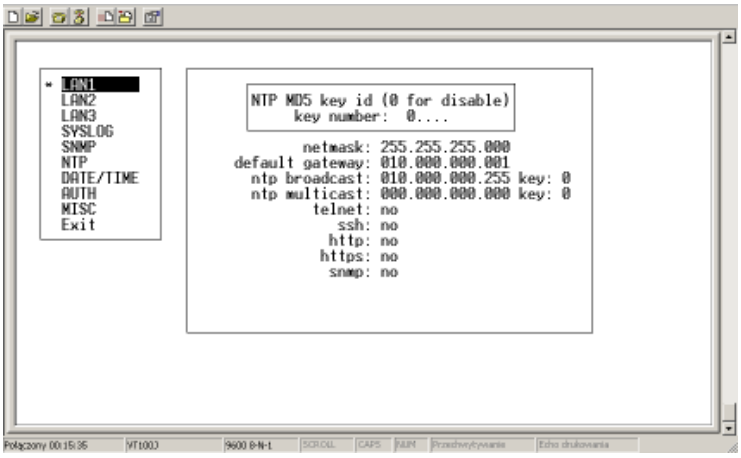

Figure 29: MD5 keyid for broadcast mode

Please refer to original ntp documentation for further details about authenticated modes, and planing subnet synchronization using broadcast and multicast.

11 NTPq client diagnostic utility

Any NTP implementation supports special diagnostic client ntpq. The command ntpq requests the actual status of NTS–3000. An command interpreter appears. Type "?" for a list of all available commands.

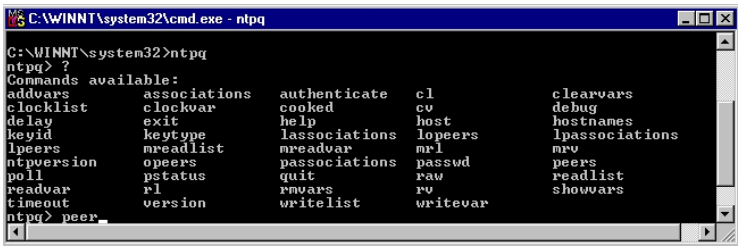

Figure 30: NTPq diagnostic for Windows NT/2000/XP

The command `peer` is used to list all active reference clocks:

```
  remote   refid  st t when poll reach  delay  offset  jitter
==============================================================
*LOCAL(0)  .RTC.   3 l   36   16    3   0.000   0.000  7885.0
 NTS-3000  .PPS.   0 l   36   16    1   0.000  60.100  1587.5
```

with the following meaning:

remote list of all valid time servers,

refid reference number,

st actual stratum value (0 - for STRATUM 1),

when time of last successful answered request in seconds,

poll period of requesting the time server in seconds,

reach octal notation of the successful requests, shifted left,

delay delay of the network transmission in milliseconds,

offset difference between system time and reference time in milliseconds,

jitter variance of the offsets in milliseconds,

where:

"*" indicates stabilised source of time,

"+" points best candidate to become a new stable source of time.

After while stratum hierarchy can change (it does not mean it has to) selecting new source for NTP. Than peer looks like:

```
  remote   refid  st t when poll reach  delay  offset  jitter
==============================================================
 LOCAL(0)  .RTC.   3 l   72   16    6   0.000   0.000  7885.0
*NTS-3000  .PPS.   0 l   72   16    3  45.000  50.220  2487.5
```

Repeatedly a "peer" command lets the user observe the accuracy of the NTP daemon. Every 16 seconds (value of -poll) a new time string is red in from the radio clock. The NTP daemon needs approx. 3...5 minutes for initialisation and to get stabilised. This is indicated by a wildcard (*) on the left side of the remote name.

Sometimes wildcard (+) appears infract of single peer line. This indicated a possible change of timeservers to that one indicated by wildcard (+). Wildcard (-) papers to indicate timeserver with low priority. Those servers can not be chosen by NTP as fare as wildcard (-) appear, however situation can change with next pool interval.

The NTP daemon terminates itself if the system time differs from the UTC time by more than 1024 seconds. This often happens when the time zone is not correctly set or you play on system date and time changes during testing.

There is a set of NTPq commands available by typing "?".

12 Installing NTP client software

NTP became to be a world wide standard in network time synchronization. Almost every existing operating system has its own implementation of NTP including Microsoft Windows and Cisco products. Many systems includes NTP clients to standard distribution. This is true for more of Unix familiar operating systems like: Linux or Free BSD.

The source code of the latest NTP distribution is available online at:

http://www.ntp.org

On this site you will be able to find as many as you are interesting links to NTP clients for various of operating systems.

On attached CD you will find NTP clients for most of popular todays operating systems.

12.1 Windows 95/98/Me

Simply copy all `cd:\Win9598Me` directory to your hard disk. Add your local NTS-3000 IP address to list of available timeservers by selecting Add button. You should select SMTP protocol to be active. We also advice to keep adjustment once per minute with maximum time corrections as possible. You can use hidden tag option to run software in background. This settings is more than enough for any Windows workstation. For some server purposes you may need a bit more frequent checking. You can use this utility for all Win32 including Windows NT/2000/XP, however we advice to use another software for NT based kernels.

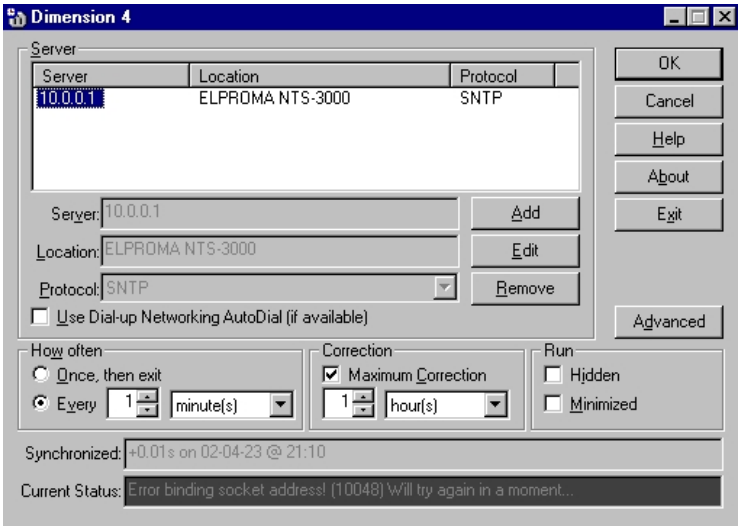

Figure 31: NTP client for Windows 95/98/Me

12.2 Windows NT/2000/XP

Before you start be sure you are operating as system administrator.

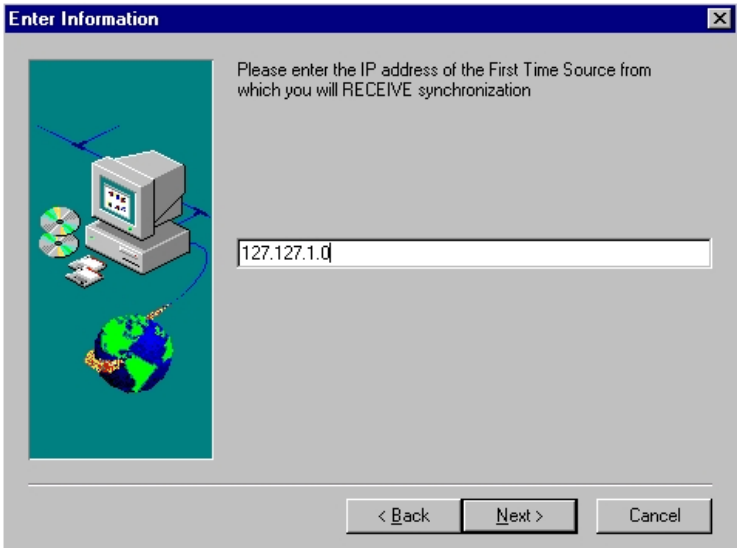

Figure 32: NTP client setup - 1st IP address for local clock

Run `cd:\WinNT2KXP\setup.exe` and follow instructions on screen. During installation you will be asked for 2 IP addresses. The first address you should type is always 127.127.1.0. The second address is IP of your NTS–3000.

As soon as installation is finished the NTP service become to be active and ready to work. To uninstall software please run setup.exe again. Standard NTP configuration file is stored in `c:\winnt\ntp.conf` or `c:\windows\ntp.conf` and it is listed below. This utility is operating in NT/2000/XP service mode. It is synchronizing time on same way as NTP demon for Unix. We advice to use this utility for NT/2000/XP servers and workstations.

```
#
# NT/2000/XP ntp.conf file
#
driftfile %windir%\ntp.drift        # path for drift file
#
#
server 127.127.1.0                  # local clock
server 10.0.0.5                     # NTS-3000 tcp/ip
#
```

Figure 33: File ntp.conf

12.3 UNIX family systems

Most of modern Unix systems have NTP included in distribution. Please note, that `xntpd` is NTP version 3 daemon. Therefore the NTP daemon can be compiled on the target system at any time. There is NTP distribution included on `cd:\drivers\ntp\unix`. First unpack gzipped tar archive:

```
# gzip -dc ntp-4.1.1a.tar.gz | tar xvf - -C /usr/local/src
```

Then run configuration script from main NTP distribution directory:

```
# cd /usr/local/src/ntp-4.1.1.a
# ./configure --disable-all-clocks --enable-LOCAL-CLOCK
```

All necessary information from the system will be collected and the corresponding make files will be generated in the subdirectories. After that the NTP daemon and all needed utilities will be generated. Please type:

```
# make
```

While compiling the several warnings may appear. This warnings are mostly unimportant. In case of problems during the compilation read the system dependent notes in the `'./html'` subdirectory. Afterwards the generated programs and tools have to be moved in the corresponding directories in `/usr/local` tree. Please type:

```
# make install
```

The time adjustment can occur in different ways. Either the system time can be set once by using the tool `ntpdate` or the NTP daemon is started. In the first case it is recommended to set the time automatically from crontab or once when booting the system. The second case is described below.

First a file named `/etc/ntp.conf` has to be generated with an editor. Adapting the file to NTS–3000 it should contain the following config:

```
# Example for /etc/ntp.conf for NTS-3000
server 127.127.1.0  # local clock
server xxx.xxx.xxx.xxx  # IP address of \mbox{NTS--3000}
# optional: driftfile
# driftfile /etc/ntp.drift
# optional: activate all messages in logfile
# logconfig = all
```

The NTP daemon is started with `ntpd`" or, using `rc.local`, while booting the system. If you want to star NTP without downtime, consider using "`-g -x`" options, to force slewing time and ignore sanity 1000s offset check.

Status messages during operation are saved in `/var/adm/` directory (corresponding to the syslog configuration):
e.g.: `# tail -f /var/adm/messages`

It shows the last lines from the file `messages`. The status messages can also be redirected in a log file by using the following option:

```
# xntpd -llogfile
```

12.4 Novell NetWare

Actually NetWare 5 and 6 support NTP clients. Please refer to NetWare documentation to understand how to configure NTP clients for specific version of NetWare.

Customers who want to synchronize time of NetWare 3, 4 (some versions 5 too) should contact Elproma info@elproma.com.pl for special software license. Listed below instructions will help you install this software to try how it works.

Before you start be sure you are SUPERVISOR and you are operating in NetWare BINDERY mode.

Please copy all files `\NetWare` to `SYS:\ETC` directory. The standard NTP configuration file is stored in `sys:etc\ntp.cnf`. Simply edit this file and add NTS-3000 IP address.

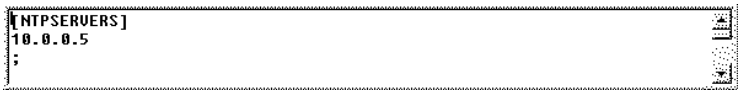

Figure 34: NTP client config for NetWare stored in file sys:etc\sntpcln3.cfg

To run SNTP client on NetWare you need to activate TCPIP (load `TCPIP.NLM`). That run simply comment:

```
>LOAD SNTPCLN3.NLM
```

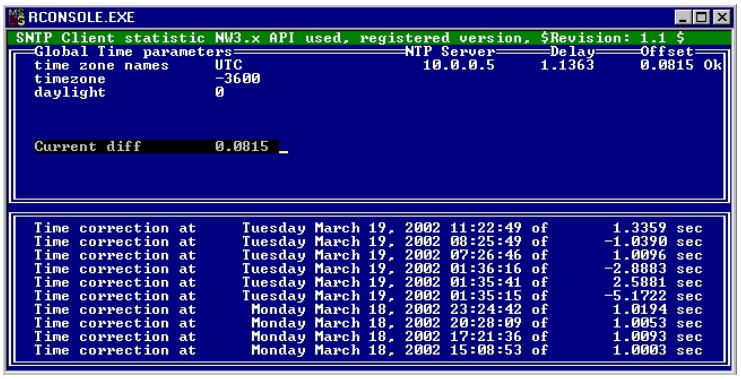

Figure 35: NTP client for NetWare 3.xx, 4.xx, 5.xx

12.5 IBM AIX (RS6000)

The IBM AIX is ready to work with NTS–3000. All NTP components including NTPD demon and NTPQ client are located at /usr/sbin. There are also available ntpdate and ntptrace. Please refer to filesys: `bos.net.tcp.client` in case of missing any of NTP components. You can get total list of installed filesyses by typing command:

```
lslpp -l
```

To check whatever `bos.net.tcp.client` filesys is installed please use following system command:

```
lslpp -l bos.net.tcp.client
```

Simply start NTP demon with ntp.conf specified in Unix (please refer to section 12.3 "Installing NTP client on UNIX" on page 30).

13 Technical specification:

The NTS–3000 is high quality professional time server for computing, telecom, military and other science purposes. It has been manufactured with no mechanical parts as coolers or hard disk. All cooling system has been resolved on natural air circulation outgoing via metal case of unit.

13.1 SYSTEM

NTP supports all versions of NTP, SNTP including latest release 4.1.1 supporting modes: CLIENT, SERVER, BROADCAST, MULTICAST. Authentication: MD5 with manual/automatic key generation.

SNTP - supports all versions of Simple Network Time Protocol

SETUP - initial setup via RS232 (any terminal program)

- System control & management: SSH, TELNET, SNMP, WWW.
- Security features: SSH, TELNET, SNMP, WWW enable/disable - each LAN port separately
- TCP/IP setup features: IP/MASK/GATEWAY - each LAN port separately Extra one default GATEWAY for all LANs

NTPbackup - up to 3 backup units per single primary NTS–3000 Time Fail Tolerance Ready

SNMP implemented for remote alarm management

FIRMWARE download and upgrade in 3 modes:

- Manual via RS232 and workstation (requiring terminal program for any OS environment)
- Automatic LAN (require direct internet access)
- Internal via WWW service

OS supports Windows 95/98/Me/2K/XP/CE, OS/2, VAX-11/785 v4.3, HPUX, SunOS, Solaris, MIPS Ultrix, ALPHA OSF/1, SGI IRIX, A/UX, AIX, Sinix, BSD, Linux, Dell SVR4, SCO Unixware, CISCO products.

13.2 HARDWARE

CPU - 2 processor system

- GPS: Winbond 7E58
- NTP/SNTP: 486DX/66MHz

RAM - 32MB EDO RAM

HD - Compact Flash 16MB set to read-only mode

LAN - 3x RTL-8139 10/100 Based T: RJ-45 connector
IEEE 802.3 - shielded data line

COM - DB-9 RS–232 (U16550 with FIFO)

send →receive	send →receive	send →receive
(9pin)→(9pin)	(25pin)→(25pin)	(9pin)→(25pin)
3 → 2	2 → 3	1 → 8
2 → 3	3 → 2	2 → 3
4 → 6	20 → 6	3 → 2
6 → 4	6 → 20	4 → 20
5 → 5	7 → 7	5 → 7
1 → 7	8 → 4	6 → 6
7 → 8	4 → 5	7 → 4
8 → 1	5 → 8	8 → 5
NC → NC	NC → NC	9 → 22

Table 1: RS–232 (Terminal/Setup) cable configuration

13.3 CASE

HAUSING - Metal desktop case, 1U
Front panel: 43mm high / 483mm wide

PROTECTION - rating IP20

DIMENSIONS - PHYSICAL DIMENSIONS: 483/43/286mm

LC DISPLAY - 2 x 20 character

13.4 GPS

CHIPSET - Motorola receiver (8) channel with RAIM

ANTENNA - BNC 1.5GHz / 8m + active converter (IP65 to UTP Cat 5. cable 200m. (max. 500m),

RECEIVER - input frequency 1575.42MHz (L1).

13.5 POWER

INPUT - 250V / 50Hz max

FUSE - 1 electronic + 1 thermal

OUTPUTS - +5V / 5A, +12V / 0.6A, -12V / 0.5A

TOTAL LOAD - 60 Watt

13.6 ACCURACY

GPS - better than ±500 nsec after synchronization of first 1 hour
better than ±2 μsec during the first hour of operation

NTP - better than 10 msec (with nanosecond kernel)

DRIFT - free running ± 5.10 – 8.00

13.7 OTHER

TEMPERATURE - 0 . . . 50C

STORAGE - -20 . . . 70C

HUMIDITY - 85% max.