Australian Government

Department of Industry, Innovation and Science

National Measurement Institute

# How to use NMI Network Time Protocol Servers to Obtain Traceable Time and Frequency

Michael Wouters

1 July 2015

This document gives guidance on how to use NMI's Network Time Protocol servers as a traceable source of time and frequency. These time sources may be useful in applications where only moderate accuracy is required. The verification of stopwatches is considered as a detailed example.

## What is the Network Time Protocol?

The Network Time Protocol (NTP) is a way of automatically setting the time on computers connected to a network. It requires special software on the computer (the client) and a trusted source of time (the server) that responds to NTP requests. The software usually runs continuously, keeping the computer's time adjusted.

In the simplest implementation of NTP, a client records the current time according to its own clock and then sends an NTP request to the server, which replies with the current time according to its clock. The difference between the two times becomes the correction to the client's time. The accuracy of this correction is greatly improved by measuring the delay between sending and receiving the request. The accuracy achieved by NTP depends on many factors but can be expected to be very much better than one second. Under optimal conditions it could be as good as 100 microseconds. This makes it a reasonable way to check devices such as stopwatches.

NMI operates a national network of NTP servers, all traceable to the national standard.

## Traceability of NTP to UTC(AUS)

For a measurement to be traceable, there must be a chain of measurements, each with a properly-established uncertainty, connecting the measurement back to the national standard. The national standard for time and frequency in Australia is Co-ordinated Universal Time or UTC(AUS). In practice this is the output of a caesium atomic clock located at NMI's Lindfield laboratory. In the case of our Sydney NTP server, the one pulse-per-second (pps) output of UTC(AUS) is directly input to the server.

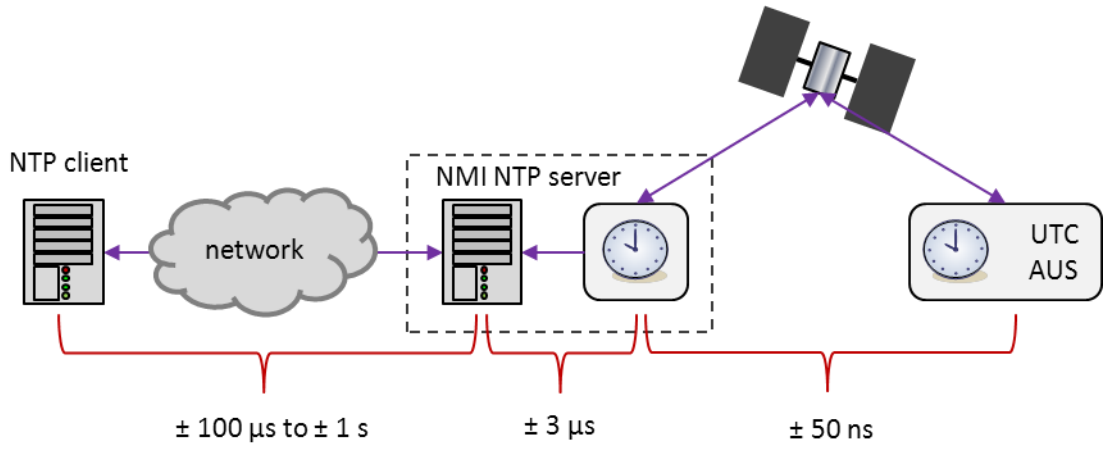


**Figure 1 Traceability of network time to UTC(AUS) and typical uncertainties in the traceability chain.**

Each of NMI's remote NTP servers has a local atomic clock and this clock is linked to UTC(AUS), via a special remote comparison technique. The expanded uncertainty of this link is approximately ± 50 ns

(figure 1). The atomic clock is used to set the time on the server but some extra uncertainty is introduced by the technique used to interface the 1 pps to the server, jitter in reading the server's time and the algorithm used to steer the PC's time. The time on NMI's NTP servers can be taken to have an uncertainty of ±3 µs. There is also a variable offset between UTC(AUS) and the server's time. This is much less than ± 1 ms under normal conditions. More detailed information on the offset can be obtained from data published on our FTP server:

ftp://time.nmi.gov.au/pub/timedata/ntp

The final link in the traceability chain is the NTP-based measurement of the offset between the server and client. The offset must be corrected for the one-way delay between the client and server. However, all that can be measured is the round trip delay. To estimate the one way delay, it is assumed that the two legs of the round trip are symmetric. In practice this is never true and in some circumstances it is possible for nearly all of the delay to be in one leg. We must therefore assume a maximum uncertainty in the offset equal to half the round-trip delay. For many users, the round trip delay will be of the order of 100 ms. This is usually much greater than the other uncertainties and will dominate the final uncertainty.

## NTP client software

Most computers are shipped with NTP client software. On Linux and MacOS, this is usually ntpd, a fully-featured, open-source program that is the reference implementation of NTP. Windows devices have a simpler NTP client supplied with them but it can be replaced if necessary.

There are many other free and commercial NTP implementations. Some of these have more convenient configuration and monitoring tools than the default NTP clients. There is also commercial software designed for auditing the time on NTP clients.

## Obtaining access to NMI NTP servers

Access to NMI NTP servers is controlled and requires that the public IP address (that is, the Internet-facing address) of the client must be static. Prospective users should contact time@measurement.gov.au and supply their client IP address(es) and contact information.

## Application 1: making PC time traceable

PC time can be made traceable by using NTP client software that logs information about the offset of the client and the delay measured in each NTP query of a server. For example, ntpd can produce two log files, the loopstats and peerstats files. The former records adjustments made to the PC's clock and the latter records the NTP queries of each NTP server, with information about the apparent offset and the delay. Together, these give detailed information about the PC's time and its uncertainty.

A simplified procedure for using this log information could be the following. For a particular day, examine the loopstats file and look at the offsets which are applied – the mean of these could be used as an estimate of the drift of the PC time between synchronizations. Then examine the delays in the peerstats file for those clocks which have been selected as suitable references by ntpd (as indicated by the clock status flags) and take the mean of these as an estimate of the synchronization

accuracy. The total uncertainty might then be estimated as the quadrature sum of the mean drift and delay.

# Application 2: checking stopwatches

NATA recommends that stopwatches be checked every 6 months by comparison with a reference that is traceable to the national standard. NTP is suggested here as a way of satisfying this.

The task is to measure a time-interval $\Delta T$ using NTP. Suppose that we start the stopwatch at time $T_1$ and stop it at time $T_2$ , according to the time displayed on our NTP-synchronized device.

The model for the measurement is:

$$\Delta T = T_2 - T_1$$

We want to compare the time interval $\Delta T$ with that shown by the stopwatch.

We must now estimate the corrections to $T_1$ and $T_2$ and their uncertainties. Corrections are necessary because of imperfect synchronization (or even no synchronization – the procedure described here does not require synchronization of the client). The following procedure is suggested.

The standard NTP distribution (available from http://www.ntp.org) includes ntpdate, a utility that can be used to query the time from an NTP server, without setting the time on the client. It can also return information about the NTP query including the offset and delay (round trip time).

If you run the following command in a terminal on Windows (ntpd version 4.2.8)

```
ntpdate -d -b -p 1 some.ntp.server
```

then at the end of the output you will see something like:

```
originate timestamp: d8b218af.9b60cd68  Tue, Mar 17 2015 14:06:23.606

transmit timestamp:  d8b218b4.4201154f  Tue, Mar 17 2015 14:06:28.257

filter delay:  0.05692  0.00000  0.00000  0.00000
     0.00000  0.00000  0.00000  0.00000

filter offset: -4.66660 0.000000 0.000000 0.000000
     0.000000 0.000000 0.000000 0.000000

delay 0.05692, dispersion 0.00000

offset -4.666603

17 Mar 14:06:30 ntpdate[2772]: step time server some.ntp.server offset -4.666603 sec
```

The information we need is:

1. The transmit timestamp - this is the time according to the client that the NTP request was sent

2. The delay – this is the round trip delay, in seconds
3. The offset - this is the offset that must be added to client time to correct it

The transmit timestamp is corrected by the amount of the offset and the uncertainty is given by half of the delay. So using the data above, the corrected transmit timestamp is 14:06:28.257 - 4.666603 = 14:06:23.591 with a raw uncertainty of 0.05692/2= 0.02846. Assuming a rectangular distribution (reducing factor 1.73), the uncertainty is then 0.0165 s.

**So what we do is simultaneously start the stopwatch and run the ntpdate command above (to get $T_1$) and then some time later, simultaneously stop the stopwatch and run another ntpdate command (to get $T_2$).**

Returning to the measurement model, we see that we just need to add the uncertainties in quadrature. Presuming a similar uncertainty for $T_2$ then the total expanded uncertainty is about 50 ms. This is more than sufficient for checking a stopwatch. Other contributions to the total uncertainty to account for eg reaction time, may of course need to be added.

The procedure just described provides traceability to the remote server. The link between the server and UTC(AUS) must also be considered; in practice though, this will typically make a negligible contribution to $\Delta T$ and its uncertainty.