

A NetDiscovery™ White Paper**Accurate Time Keeping for Lawful Access and Interception**Anthony M. Rutkowski[†]

VeriSign

Abstract

This White Paper is intended as a tutorial and reference guide. It explains current precision time keeping technology and its increasing critical importance in conjunction with Lawful Access and Interception (LA/LI), including minimizing time uncertainty of Internet event timestamps. The paper includes a survey of timestamp specifications in LI handover law and standards; a description of the global system for precision time synchronization; the use of Network Time Protocol (NTP) to maintain accurate time across the Internet today; and the ongoing NTP Project aimed at extending and enhancing the technology. A basis is provided for a Law Enforcement Agency and regulator requirement for IP lawful access and interceptions data handover with a timestamp within a worst case *time uncertainty* of 200 milliseconds. This is well within the capability of almost every Internet server, considering widespread Internet measurements indicate that 0.1 - 1 millisecond is the "best practice" norm for good commercial servers. A Best Practice requirement template is provided.

1. Introduction

Time keeping is perhaps humankind's earliest scientific discipline. Until the late 20th century, the ultimate time reference was the rotation of the earth about the sun. Then, as need arose for more certain timekeeping, and devices became available for measuring atomic level quantum effects, the ultimate time reference became a global average of continuous running Cesium oscillator based clocks. The uncertainties of these atomic-referenced time systems became so good that a separate time-scale became necessary to account for minor variations in time of the earth rotating the sun.¹ The former is referred to as International Atomic Time (TAI) and the latter as Universal Coordinated Time (UTC).

Today, the uncertainties are measured in picoseconds (10^{-12} sec or a millionth of a millionth of a second) and Internet-based tools exist to allow trivially inexpensive maintenance of Internet-connected devices to uncertainties measured in hundreds of nanoseconds (10^{-9} sec). This is a dramatic change – certainly as measured by the timekeeping costs incurred in the legacy telecommunication industry. Indeed, the latest version of the Microsoft XP operating system bundles the capability as a continuously running service referenced to Microsoft time servers - unbeknownst to most users.

In large measure, this Internet capability was manifested because of the professional work and personal passion of Prof. David L. Mills of the University of Delaware. For more than two decades, Dr. Mills pioneered the Network Time Protocol (NTP) – first developing it, then evangelizing and evolving the protocol.² The basic NTP RFC1129 has been superceded by NTP Version 3 (RFC2030), and a Simple NTP version 4 (RFC2030). Highly recommended for just about anything concerning NTP is the **NTP Project** site

[†] Vice President for Regulatory Affairs trutkowski@verisign.com Acting President, Global LI Industry Forum www.gliif.org.

¹ The current US standard NIST-F1 has an uncertainty of 5×10^{-15} .
<http://www.nist.gov/public_affairs/guide/time_frequency.htm>.

² David L. Mills, *A Brief History of NTP Time: Memoirs of an Internet Timekeeper*, <http://www.eecis.udel.edu/~mills/database/papers/history/history.pdf>. See also, David Mills, "*Internet time synchronization: the Network Time Protocol.*" IEEE Transactions on Communications, October 1991, <<http://www.eecis.udel.edu/~mills/database/papers/trans.pdf>>

at www.ntp.org, including public domain copies of NTP software for almost any operating system and URLs of global NTP reference servers.

What does any of this have to do with Lawful Access and Interception? LA/LI are fundamentally about the observation and recording of events. Some events are used for subsequent forensic or intelligence analysis – especially for the highly distributed, autonomous Internet environment where related events must be independently gathered and correlated to detect and understand unlawful, terrorist, or security threatening activities.

Ultimately, these events may also be presented to a court of competent jurisdiction for use as evidence. In all of these uses, the certainty of the time associated with an event is a critically important attribute. In most LA/LI specifications and law, this data is referred to as a *timestamp*. Precision time may also be relevant to the use of digital signatures in conjunction with authenticating those events.³

Historically, the relatively highly controlled Public Switched Telephone Networks (PSTNs) have maintained timing practices and systems that resulted in most timestamps having very minimal uncertainty values – typically well within a few milliseconds. With significant deregulation, competitive alternative networks, and the highly heterogeneous Internet, the uncertainty of timestamps can no longer be taken for granted – and at a time when the very heterogeneity of the networks makes precision time even more important to understand events taking place.

1.1 Terminology

Timekeeping is both an engineering and scientific discipline. It makes use of carefully crafted terms – some of which have evolved in recent years. For example, the preferred term of timekeeping experts when dealing with the quantitative specification of a time reference is not "precision" nor "accuracy," but rather "uncertainty." Similarly, the use of Greenwich Mean Time (GMT) has long transitioned to the use of Coordinated Universal Time (UTC).

The following terms and discussion are provided courtesy of one of the time standards laboratories in the global system.⁴

Uncertainty

In recent years, the term uncertainty has been given preference over accuracy when a quantitative measure is stated. Accuracy is often used in a qualitative sense. For example, we might say that a time measurement has an uncertainty of 1 microsecond, and that the accuracy of the measurement is very good. The National Institute of Standards and Technology (NIST) defines *uncertainty* for purposes of time and frequency measurements to be a "parameter, associated with the result of a measurement, that characterizes the dispersion of values that could reasonably be attributed to the measurand. By convention, two standard deviations are normally used for uncertainty numbers."

Accuracy

Accuracy is the degree of conformity of a measured or calculated value to its definition. Accuracy is related to the offset from an ideal value. In the world of time and frequency, accuracy is used to refer to the time offset or frequency offset of a device. For example, time offset is the difference between a measured on-time pulse and an ideal on-time pulse that coincides exactly with UTC. Frequency offset is the difference between a measured frequency and an ideal frequency with zero uncertainty. This ideal frequency is called the nominal frequency.

Precision

The term precision is somewhat ambiguous, and has several meanings in time and frequency metrology. Due to its ambiguity, it is not often used in a quantitative sense. Normally, it refers to the

³ See, e.g., Technical Specification, Time stamping profile, ETSI TS 101 861 V1.2.1 (2002-03); Technical Specification, Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities, ETSI TS 102 023 V1.2.1 (2003-01); FIPS Publication 186: "Digital Signature Standard (DSS)"

⁴ Time & Frequency Division, Physics Laboratory, National Institute of Standards and Technology, Boulder Colorado USA <<http://www.boulder.nist.gov/timefreq/general/glossary.htm>>

degree of mutual agreement among a series of individual measurements, values, or results. In this case, precision is analogous to standard deviation. Precision might also be used to refer to the ability of a device to produce, repeatedly and without adjustments, the same value or result, given the same input conditions and operating in the same environment. This use of precision makes it analogous to repeatability, reproducibility, or even stability. In other instances, precision is used as a measure of a computer's ability to distinguish between nearly equal values. For example, a compiler or spreadsheet might have 32-bit precision when doing calculations with floating point numbers. In this case, precision is analogous to resolution.

Coordinated Universal Time (UTC)

The international atomic time scale that serves as the basis for timekeeping for most of the world. UTC is a 24-hour timekeeping system. The hours, minutes, and seconds expressed by UTC represent the time-of-day at the Earth's prime meridian (0° longitude) located near Greenwich, England. UTC is calculated by the Bureau International des Poids et Mesures (BIPM) in Sevres, France. The BIPM averages data collected from more than 200 atomic time and frequency standards located at about 50 laboratories. As a result of this averaging, the BIPM generates two time scales, International Atomic Time (TAI), and Coordinated Universal Time (UTC). These time scales realize the SI second as closely as possible. UTC runs at the same frequency as TAI. However, it differs from TAI by an integral number of seconds. This difference increases when leap seconds occur. When necessary, leap seconds are added to UTC on either June 30 or December 31. The purpose of adding leap seconds is to keep atomic time (UTC) within ± 0.9 s of an older time scale called UT1, which is based on the rotational rate of the Earth. Leap seconds have been added to UTC at a rate averaging about 8 every 10 years, beginning in 1972. The BIPM maintains TAI and UTC as "paper" time scales. The major metrology laboratories use the published data from the BIPM to steer their clocks and oscillators and generate real-time versions of UTC. UTC is regarded as the ultimate standard for time-of-day, time interval, and frequency. Clocks synchronized to UTC display the same hour, minute, and second all over the world (and remain within one second of UT1).

2. Minimizing the Time Uncertainty of Internet Lawful Access and Interception Timestamps

As noted in the introduction, Lawful Access and Interception is fundamentally about the observation and recording of events. Almost every event will have (or should have) a timestamp associated with it. This includes not only intrinsic events like traffic-related data and content, but also authenticating digital signatures and transfers of data, content, authorizing instruments, or other extrinsic information between parties in the LA/LI process.

The Internet environment, however, poses some significant challenges because it is so highly distributed and autonomous. We are not dealing with a monolithic regulated telecommunication infrastructure. As a result, both stored traffic records and real-time intercepts will necessarily emanate from multiple sources at diverse locations that must be correlated to detect target signatures and understand the potentially highly complex patterns of activity capable of observation. See Annex 3.

In many ways, this analytic LA/LI activity and need is not significantly different than many scientific disciplines today where discrete events are being captured and analyzed. This includes, for example, radio astronomy, SETI, meteorology, among many others. All of these activities deal with discovering frequently elusive event-time correlations dependent on timestamps that have minimal uncertainty.

In the case of LA/LI timestamps, the requirements are also linked to legal requirements in many national jurisdictions as well as the international *Convention on Cybercrime*. The *Convention* defines "traffic data" to include "...any computer data relating to a communication by means of a computer system, generated by a

computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, *time*, date, size, duration, or type of underlying service.”[Emphasis added]⁵

Ideally, the time generated as part of the Internet traffic data should possess uncertainties on the order of millisecond, as this is the norm today on most controlled environment Internet servers. A 100 millisecond requirement was specified by the U.S. Department of Justice and its Federal Bureau of Investigation in 1998 for telecommunication networks for the “difference between the time of the event and the time recorded in the time stamp.”⁶ An industry trade association countered with a proposed 200 millisecond value; and the New York Police Department argued for 100 milliseconds. The FCC ultimately found that “...the DoJ/FBI proposal for delivery of the message from the IAP to the LEA's Collection function...with 100 millisecond accuracy to be overly stringent and possibly excessively costly to carriers given the various network designs used by carriers in different services applying this requirement....and...require[d] that delivery of a call-identifying message be transmitted to the LEA's Collection Function...with the call event time-stamped to an accuracy of at least 200 milliseconds.”⁷ ETSI LI timestamp specifications for telecommunication systems exists as an absolute value, but an extremely "loose" 1 second.

As discussed in Sec. 5 below, the implementation today of Internet device timestamp uncertainties under 200 milliseconds is rather easily achievable at essentially zero cost to providers. The “over-stringency” and cost factors simply no longer exist. Measurements made during the course the preparation of this contribution on a "low-end" SOHO server configuration demonstrated uncertainties under 200 milliseconds. Most competent providers under controlled conditions should be able to easily support uncertainties in the range of several milliseconds. The uncertainty specification of 200 milliseconds seems appropriate.

3. Survey of Lawful Access and Interception Timestamp Requirements and Specifications

In the course of preparing this contribution, a brief survey was undertaken of timestamp requirements and specifications in an array of international and national standards fora – largely intended for telecommunication network use. See Annex 1.

All the various ETSI standards appear to use a one second (precision) specification. Somewhat inexplicably, the Swiss E-Mail intercept specification requires reference to a Stratum 1 server which operates at an uncertainty of 1 microsecond or better, but allows ± 5 seconds.

None of the existing specifications appear to use appropriate timekeeping terms of art. Aside from the issue of appropriate timekeeping values, all the standards bodies maintaining these standards should endeavour to use preferred contemporary terms of the metrology community.

In addition to the LI timestamp specifications, almost ever major vendor of Internet operating systems and server platforms publish NTP timekeeping best practices with papers.⁸

⁵ Art 1, *Convention on Cybercrime*, Council of Europe, ETS No. 185 (Budapest, 23 Nov 2001) <<http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=07/04/03>>.

⁶ See para. 92, *Joint Petition for Expedited Rulemaking* in FCC Docket No. 97-213 (27 Mar 1998) at 51 <http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=2030700003>.

⁷ See para. 96, *Third Report and Order* in CC Docket 97-213, FCC 99-230 (31 Aug 1999) at 37, 44 C.F.R. §§ 22.1102, 24.904, 64.2202

⁸ See, e.g., Cisco Systems, *Network Time Protocol: Best Practice White Paper*, <<http://cisco.com/warp/public/126/ntpm.pdf>>.

4. The Global System for Precision Time Synchronization

The global system for precision time synchronization consists of a mixture of agreements, forums and day-to-day activities among the world's timing centres. The two principal forums for coordinating this activity are the OIML and BIPM.

4.1 L'Organisation Internationale de Métrologie Légale (OIML)

Legal metrology is the entirety of the legislative, administrative and technical procedures established by, or by reference to public authorities, and implemented on their behalf in order to specify and to ensure, in a regulatory or contractual manner, the appropriate quality and credibility of measurements related to official controls, trade, health, safety and the environment.

The International Organization of Legal Metrology (OIML) was established in 1955 (see the Convention) in order to promote the global harmonization of legal metrology procedures. Since that time, the OIML has developed a worldwide technical structure that provides its Members with metrological guidelines for the elaboration of national and regional requirements concerning the manufacture and use of measuring instruments for legal metrology applications.⁹

4.2 Bureau International des Poids et Mesures (BIPM)

The Bureau International des Poids et Mesures (BIPM) was set up by the Convention of the Metre and has its headquarters near Paris, France. It is financed jointly by the Member States of the Convention and operates under the exclusive supervision of the CIPM.

Its mandate is to provide the basis for a single, coherent system of measurements throughout the world, traceable to the International System of Units (SI). This task takes many forms, from direct dissemination of units (as in the case of mass and time) to coordination through international comparisons of national measurement standards (as in length, electricity, radiometry and ionizing radiation).¹⁰

The SI unit of time, the second, is defined in terms of the frequency of a hyperfine transition of the atom of caesium. A practical realization of the second, sufficiently accurate for most applications, may be obtained from commercial caesium-beam frequency standards. More accurate caesium standards exist in a small number of national laboratories; for them, the uncertainties are estimated to be a few parts in 10¹⁵. New developments in clocks using trapped or cooled atoms or ions are leading to improvements in accuracy well beyond this.¹¹

⁹ <http://www.oiml.org/structures/index.html>

¹⁰ <http://www.bipm.org/enus/4_BIPM/bipm.html>

¹¹ http://www.bipm.org/enus/5_Scientific/c_time/time.html

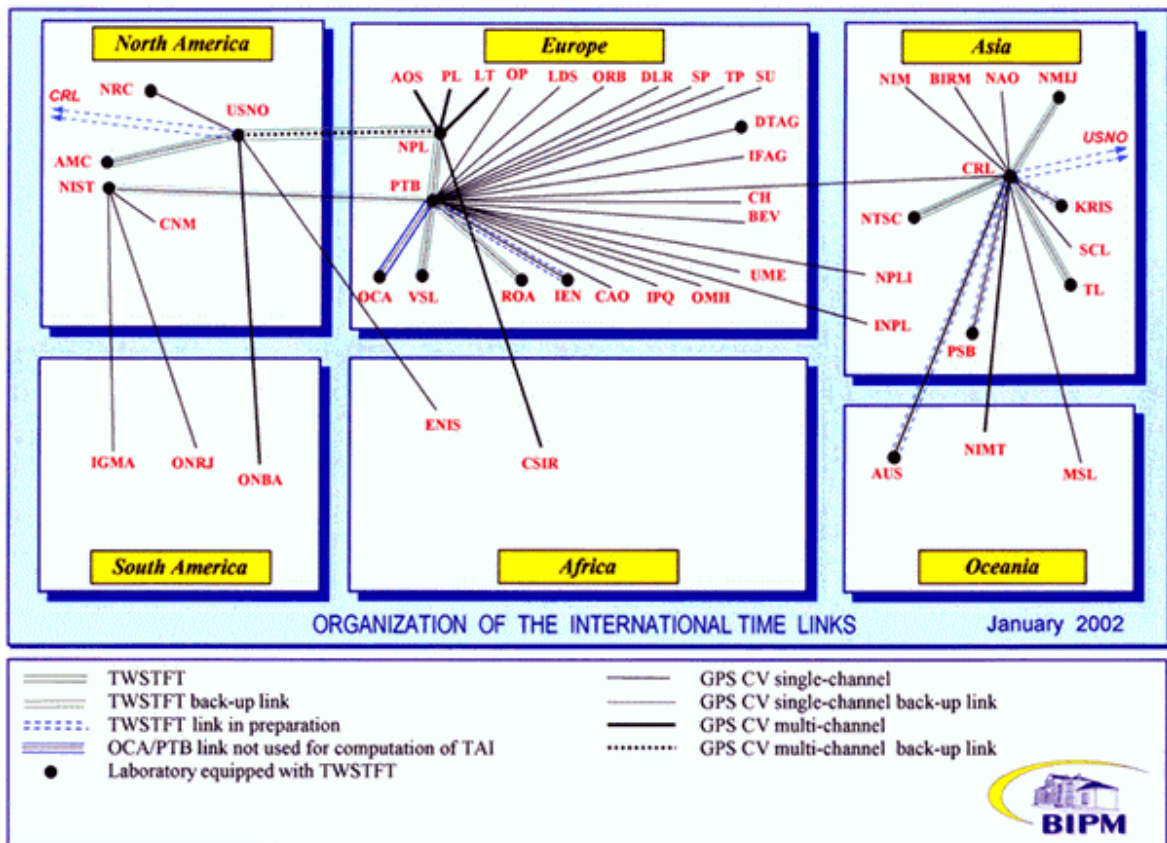


Figure 1. Global Structure for Coordinating Time Standards¹²

UTC is the international atomic time scale that serves as the basis for timekeeping for most of the world. The hours, minutes, and seconds expressed by UTC represent the time-of-day at the Earth's prime meridian (0° longitude) located near Greenwich, England. UTC is calculated by the BIPM by averaging averages data collected from more than 200 atomic time and frequency standards located at about 50 laboratories. See Annex 1 and Figure 1, above.

As a result of this averaging, the BIPM generates two time scales, International Atomic Time (TAI), and Coordinated Universal Time (UTC). These time scales realize the SI second as closely as possible. UTC runs at the same frequency as TAI. However, it differs from TAI by an integral number of seconds. This difference increases when leap seconds occur. When necessary, leap seconds are added to UTC on either June 30 or December 31. The purpose of adding leap seconds is to keep atomic time (UTC) within ± 0.9 s of an older time scale called UT1, which is based on the rotational rate of the Earth. Leap seconds have been added to UTC at a rate averaging about 8 every 10 years, beginning in 1972.

The major metrology laboratories use the published data from the BIPM to steer their clocks and oscillators and generate real-time versions of UTC. UTC is regarded as the ultimate standard for time-of-day, time interval, and frequency. Today, most of these laboratories maintain Internet-based NTP servers synchronized with their UTC standard clocks, described in Sec. 5, below.

Clocks in a telecommunications system or network are assigned a number that indicates its quality and position in the timing hierarchy. The highest quality clocks, called stratum 1 clocks, have a frequency offset of 1×10^{-11} or less, which means that they can keep time to within about one microsecond per day. Only stratum 1 clocks may operate independently; other clocks are synchronized directly or indirectly to a stratum 1 clock. By definition all BIPM Timing Centres which maintain network-based UTC clocks, are stratum 1.

¹² BIPM, <http://www.bipm.org/enus/5_Scientific/c_time/time_1.html>

5. The Network Time Protocol – the NTP Project

5.1 NTP basics

The Network Time Protocol is one of the earliest Internet protocols, with roots traceable back a quarter century to 1979. It has witnessed more than two decades of continuous operation, and the technology has improved from synchronous capability of a few hundreds of milliseconds to tens of nanoseconds. There are now over two dozen software ports for almost every operating system in existence. It runs on everything from embedded controllers to supercomputers. It runs as an operational embedded essential service in Windows XP.

Most of the following material is extracted from Dr. Mills' recent excellent tutorial material on NTP.¹³

- ? Network Time Protocol (NTP) synchronizes clocks of hosts and routers in the Internet.
- ? Well over 100,000 NTP peers deployed in the Internet and its tributaries all over the world.
- ? Provides nominal accuracies of low tens of milliseconds on WANs, submilliseconds on LANs, and submicroseconds using a precision time source such as a cesium oscillator or GPS receiver.
- ? Unix NTP daemon ported to almost every workstation and server platform available today - from PCs to Crays - Unix, Windows, VMS and embedded systems.
- ? The NTP architecture, protocol and algorithms have been evolved over the last twenty years to the latest NTP Version 4 described in this briefing.

Dr. Mills notes that among the many needs for precision time, two important uses include Network monitoring, measurement and control; intruder detection, location and reporting, and secure document timestamps with cryptographic certification.

The essential attributes of NTP include:

- ? Primary (stratum 1) servers synchronize to national time standards via radio, satellite and modem.
- ? Secondary (stratum 2, ...) servers and clients synchronize to primary servers via hierarchical subnet.
- ? Clients and servers operate in master/slave, symmetric or multicast modes with or without cryptographic authentication.
- ? Reliability assured by redundant servers and diverse network paths.
- ? Engineered algorithms reduce jitter, mitigate multiple sources and avoid improperly operating servers.
- ? System clock is disciplined in time and frequency using an adaptive algorithm responsive to network time jitter and clock oscillator frequency wander.

The latest versions of the NTP include:

- ? Current Network Time Protocol Version 3 has been in use since 1992, with nominal accuracy in the low milliseconds.
- ? Modern workstations and networks are much faster today, with attainable accuracy in the low microseconds.
- ? NTP Version 4 architecture, protocol and algorithms have been evolved to achieve this degree of accuracy.
- ? Improved clock models which accurately predict the time and frequency adjustment for each synchronization source and network path.
- ? Engineered algorithms reduce the impact of network jitter and oscillator wander while speeding up initial convergence.
- ? Redesigned clock discipline algorithm operates in frequency-lock, phase-lock and hybrid modes.

¹³ David Mills, Network Time Protocol (NTP) General Overview
<<http://www.eecis.udel.edu/~mills/database/brief/overview/overview.ppt>>.

- ? The improvements, confirmed by simulation, improve accuracy by about a factor of ten, while allowing operation at much longer poll intervals without significant reduction in accuracy.

Current Goals and non-goals include:

- ? Goals

- o Provide the best accuracy under prevailing network and server conditions.
- o Resist many and varied kinds of failures, including two-face, fail-stop, malicious attacks and implementation bugs.
- o Maximize utilization of Internet diversity and redundancy.
- o Automatically organize subnet topology for best accuracy and reliability.
- o Self contained cryptographic authentication based on both symmetric key and public key infrastructures and independent of external services.

- ? Non-goals

- o Local time – this is provided by the kernel.
- o Access control - this is provided by firewalls and address filtering.
- o Privacy - all protocol values, including time values, are public.
- o Non-repudiation - this can be provided by a layered protocol if necessary.
- o Conversion of NTP timestamps to and from other time representations and formats.

5.2 Performance of typical NTP servers in the global Internet

Table 1, below, shows the number of days surveyed, mean absolute offset, RMS and maximum absolute error and number of days on which the maximum error exceeded 1, 5, 10 and 50 ms at least once. These are actual measurements of servers running NTP representing LANs, domestic WANs and the worldwide Internet, done in 1997 over a several month period. Most exhibited mean uncertainties under 1 millisecond. The performance since 1997 is likely to have improved further with greater ubiquity of high bandwidth, low latency Internet connectivity.

NTP Server	Location	Days	Mean	RMS	Max	>1	>5	>10	>50
Austron GPS	DCnet	91	0.0	0.012	1.000	0	0	0	0
rackety	DCnet	95	0.066	0.053	2.054	11	0	0	0
mizbeaver	DCnet	17	0.150	0.171	1.141	2	0	0	0
churchy	DCnet	42	0.185	0.227	3.150	15	0	0	0
pogo	DCnet	88	0.091	0.057	1.588	8	0	0	0
beauregard	DCnet	187	0.016	0.108	2.688	30	0	0	0
umdl	U Maryland	78	4.266	2.669	35.89	29	29	28	0
swifty	Australia	84	2.364	56.70	3944	27	27	27	13
ntps1	Germany	70	0.810	10.86	490.9	12	12	12	6
time_a	NIST Boulder	85	1.511	1.686	80.56	28	19	11	2
fuzz	San Diego	77	3.889	2.632	47.59	27	27	23	0
la	Los Angeles	83	0.650	0.771	17.84	28	8	3	0
enss136	NSFnet WashDC	88	0.657	1.203	32.65	38	23	10	0

Table 1. 1997 Survey of NTP Use¹⁴

These measurements appear to have been made against servers in relatively controlled environments. The measurements portrayed in Annex 4 are representative of a rather low-cost, SOHO class server over an initial 7 day period. The dispersions ranged between 100 and 100 milliseconds

5.3 Primary and Secondary Public NTP Time servers

The NTP Project current lists 123 NTP Primary (stratum 1) and 163 Secondary (stratum 2) time servers for anyone to reference.¹⁵ These servers amply cover the entire world.

5.4 NTP Software Downloads and Documentation

The NTP Project provides free-of-charge, current production, release candidate, and development versions of NTP software reference implementations.¹⁶ Extensive documentation is also available. Most operating system vendors provide binary ports of the reference versions bundled with the software. Numerous third party ports are also available.¹⁷

6. Time Service Specifications

Many national and international specifications exist for the provision of time service. During the 1990s, the Object Management Group (OMG) and X/Open sought to develop an object-based specification suitable for use as an open time service specification. The objective was to specify "a service that enables the user to obtain current time together with an error estimate associated with it, [including the ability to] ascertain the order in which 'events' occurred, generate time-based events based on timers and alarms, compute the interval between two events." In May 2002, a revised specification was adopted.¹⁸

¹⁴ *Ibid* at 16.

¹⁵ See Public NTP Time Servers, <<http://www.eecis.udel.edu/~mills/ntp/servers.html>>.

¹⁶ See Source releases and patches, <<http://www.ntp.org/downloads.html>>.

¹⁷ See Where to find NTP software, <<http://www.ntp.org/links.html>>.

¹⁸ OMG, Time Service Specification, version 1.1, May 2002. <<http://www.omg.org/docs/formal/02-05-06.pdf>>

7. Recommended Best Practice for Regulators, LA/LI Standards Developers, Providers and Law Enforcement Agencies

The relatively esoteric subject of precision timekeeping tends to conspire with the tendency of regulators, LA/LI standards developers, and providers, to largely ignore the subject of precision timekeeping and the increasing necessity for timestamps with low uncertainties. The survey of standards specifications contained in this White Paper suggest no apparent collaboration with the precision timekeeping community or cognizance of contemporary capabilities and practice. The subject tends to be unfairly viewed as a cost or liability issue, when the reality is that very minimal due diligence can result in reasonably low timestamp uncertainties.

Just as radio regulatory authorities for many decades have required radio operators periodically measure and certify the precision of their carrier frequencies, so too should network service providers treat timestamp references. This can be mandated by regulatory authorities, voluntarily undertaken as best practice maintenance activities of providers, or mandated by Law Enforcement Authorities in conjunction with a production order for traffic data or content.

The text below is provided as a template for these purposes.

Best Practice Requirement for Lawful Access and Interception Timestamps

Network Service Providers subject to Lawful Access and Interception requirements either as a result of national regulatory requirement or a production order issued by a court or authority of competent jurisdiction shall meet the following requirements.

Definitions

Coordinated Universal Time (UTC): The international atomic time scale that serves as the basis for timekeeping for most of the world. UTC is a 24-hour timekeeping system. The hours, minutes, and seconds expressed by UTC represent the time-of-day at the Earth's prime meridian (0° longitude) located near Greenwich, England. UTC is calculated by the Bureau International des Poids et Mesures (BIPM) in Sevres, France. The national UTC reference designated by law shall be used.

Uncertainty: Parameter, associated with the result of a measurement, that characterizes the dispersion of values that could reasonably be attributed to the time being measured. Two standard deviations will be used for uncertainty numbers. .

Timestamp Uncertainty Requirements

1. Notwithstanding any other specification, all timestamps used for the production, delivery, or authentication of stored or real-time traffic data or content shall have a worst-case UTC synchronization uncertainty of 200 milliseconds.
2. The Network Service Provider or its lawful access and interception agent shall perform regular measurement of timestamp values and keep associated records for review by lawful authorities that demonstrate compliance with the above requirement.

Annex 1. Survey of time accuracy specifications in LI handover standards

ETSI ES 201 671 V2.1.1 (2001-09) at 97

Table F.3.5: Information elements in the CC header

O 134 4 PayloadTimeStamp = Payload timestamp according to intercepting node. (Precision: 1 s, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).

ETSI TS 101 671 V2.5.1 (2003-01) at 97

Table F.3.5: Information elements in the fist [sic] version of the CC header

O 134 4 PayloadTimeStamp = Payload timestamp according to intercepting node. (Precision: 1 s, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).

Table F.3.6: Information elements in the second version of the CC header

O 134 4 PayloadTimeStamp = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).

ETSI TS 101 861 V1.2.1 (2002-03) 7

5.2.1 Parameters to be supported

The following requirements apply:

- ? a genTime parameter limited to represent time with one second is required,
- ? a minimum accuracy of one second is required,

ETSI TS 133 108 V5.1.0 (2002-09) 52 3GPP TS 33.108 version 5.1.0 Release 5

Table C.2: Information elements in the first version of the CC header

O 134 4 PayloadTimeStamp = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).

Table C.3: Information elements in the second version of the CC header

O 134 4 PayloadTimeStamp = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).

ETSI TR 102 053 V1.1.1 (2002-03)

8 Regarding the accuracy of the time stamp value of a record, it may be determined at any point in time during the period between the detection of an event and the sending of the related record.

TIA/EIA/IS -J-STD-025-A, 17 Apr 2000

3 Definitions and Acronyms

timing information: defined in FCC 99-230, CC Docket No. 97-213 to be the capability that permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the carrier's IAP to the LEA's Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event timestamped to an accuracy of at least 200 milliseconds.

4.7 Timing Information

With respect to the matters before the FCC in FCC 99-230, CC Docket No. 97-213, the following has been added to this Interim Standard: This capability permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the TSP's IAP to the LEA Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event time-stamped to an accuracy of at least 200 milliseconds.

TIA/EIA PN-4465-RV1 (Subject to Change) 7 Oct 2002

3 Definitions and Acronyms

timing information: defined in FCC 99-230, CC Docket No. 97-213 to be the capability that permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the carrier's IAP to the LEA's Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event timestamped to an accuracy of at least 200 milliseconds.

4.7 Timing Information

With respect to the matters before the FCC in FCC 99-230, CC Docket No. 97-213, the following has been added to this Standard: This capability permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the TSP's IAP to the LEA Collection Function within eight

seconds of receipt of that message by the IAP at least 95% of the time, and with the call event time-stamped to an accuracy of at least 200 milliseconds.

This capability places timing requirements on call-identifying message generation after triggering events that shall be met for these messages. It also requires time stamp accuracy for call events.

Switzerland, *Lawful Interception of Telecommunications Traffic Packet Switched Services Technical Requirements for the Delivery of Intercepted Electronic Mail*, Version 1.0 vom 2. April 2002 Gültig ab: xx. März 2002 Seite 9 / 18

6.2.2 Synchronization

The precision of the timestamps generated by the ISP's systems with respect to the reference time base must be within +/- 5 seconds. The following server is defined as the reference time base: NTP primary (stratum 1) time server: swisstime.ethz.ch It is proposed to use the Network Time Protocol (NTP) [8] for synchronization, but any other system (e.g. DCF77, GPS, etc.) may also be used as long as the offset from the reference time base remains within the range of +/- 5 seconds.

UK Home Office *NATIONAL HANDOVER INTERFACE SPECIFICATION*, Version 1.0 May 2002 at 13

49. The timestamp field is not mandatory. If present, the timestamp must be written according to ISO 8601. An example is shown in appendix B. CSPs should take all reasonable measures to ensure the accuracy of the timestamp.

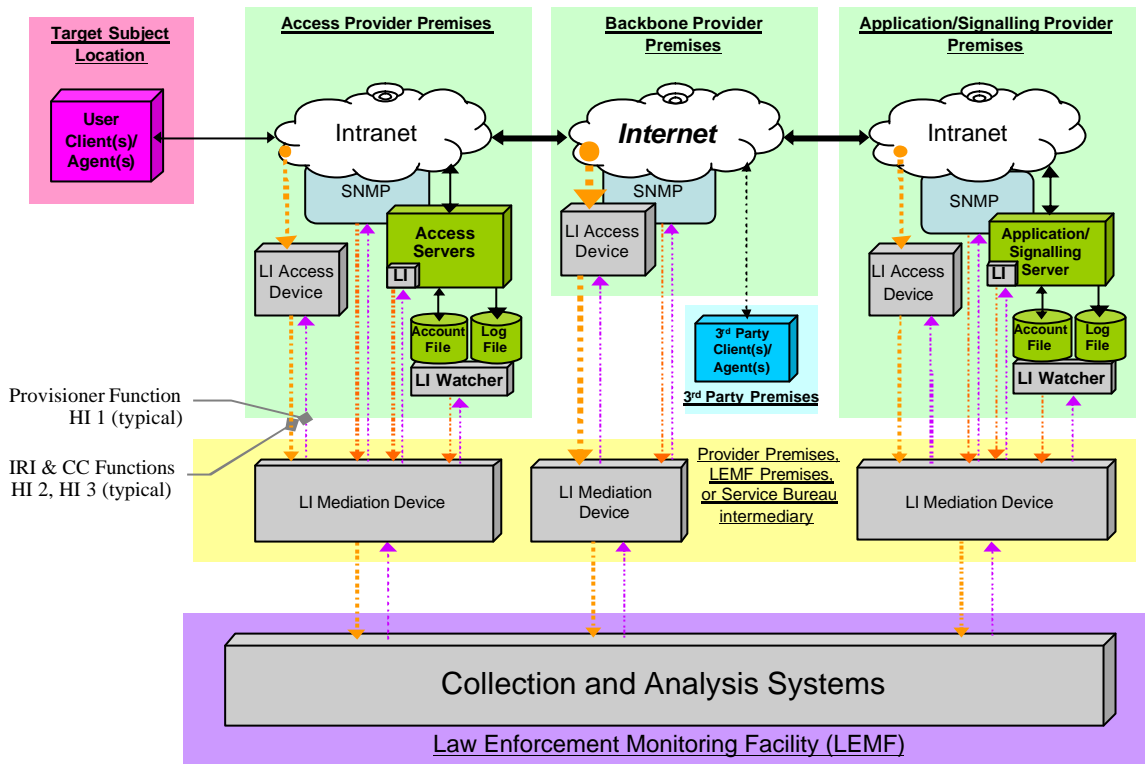
The Netherlands, Ministry of Economic Affairs (EZ) Directorate-General for Telecommunications and Post, TIT V1.0.0 (2002-09) *Transport of Intercepted IP Traffic* at 11

6) S1 MUST maintain a correct system time, by using the NTP protocol [4]. S2 MAY operate as a stratum 2 NTP server.

Annex 2. Acronyms and Locations of the Timing Centres which Maintain a Local Approximation of UTC (BIPM Reference)

IGMA	Instituto Geográfico Militar	Buenos Aires	Argentina
ONBA	Observatorio Naval	Buenos Aires	Argentina
NML	National Measurement Laboratory	Sydney	Australia
AUS	Consortium of laboratories in Australia		Australia
BEV	Bundesamt für Eich- und Vermessungswesen	Vienna	Austria
ORB	Observatoire Royal de Belgique (Royal Observatory of Belgium)	Brussels	Belgium
ONRJ	Observatório Nacional	Rio de Janeiro	Brazil
NMC	National Centre of Metrology	Sofiya	Bulgary
NRC	National Research Council of Canada	Ottawa	Canada
TCC	TIGO	Concepcion	Chile
BIRM	Beijing Institute of Radio Metrology and Measurement	Beijing	China
NIM	National Institute of Metrology	Beijing	China
SCL	Standards and Calibration Laboratory	Hong Kong	China
JATC	Joint Atomic Time Commission	Lintong	China
NTSC	National Time Service Center of China	Lintong	China
TP	Institute of Radio Engineering and Electronics - Academy of Sciences of the Czech Republic	Prague	Czech Republic
F	Commission Nationale de l'Heure	Paris	France
OP	Observatoire de Paris (Paris Observatory)	Paris	France
PTB	Physikalisch-Technische Bundesanstalt	Braunschweig	Germany
DTAG	Deutsche Telekom AG	Darmstadt	Germany
DLR	Deutsche Zentrum für Luft- und Raumfahrt (German Aerospace Centre)	Oberpfaffenhofen	Germany
IFAG	Bundesamt für Kartographie und Geodäsie (Federal Agency for Cartography and Geodesy) Fundamental station	Wetzell Kötzting	Germany
OMH	Országos Mérésügyi Hivatal (National Office of Measures)	Budapest	Hungary
NPLI	National Physical Laboratory	New Delhi	India
INPL	National Physical Laboratory	Jerusalem	Israel
CAO	Stazione Astronomica di Cagliari (Cagliari Astronomical Observatory)	Cagliari	Italy
IEN	Istituto Elettrotecnico Nazionale Galileo Ferraris	Turin	Italy
NAO	National Astronomical Observatory	Misuzawa	Japan
CRL	Communications Research Laboratory	Tokyo	Japan
NMIJ	National Metrology Institute of Japan	Tsukuba	Japan
KRIS	Korea Research Institute of Standards and Science	Daejeon	Korea (Rep of)
LT	Lithuanian National Metrology Institute	Vilnius	Lithuania
NMLS	National Metrology Laboratory of SIRIM Berhad	Shah Alam	Malaysia
CNM	Centro Nacional de Metrología	Querétaro	Mexico
MSL	Measurement Standards Laboratory	Lower Hutt	New Zealand
NMAS	Norwegian Metrology and Accreditation Service	Kjeller	Norway
AOS	Astronomiczne Obserwatorium Szerokosciowe (Borowiec Astrogeodynamic Observatory)	Borowiec	Poland
GUM	Główny Urząd Miar (Central Office of Measures)	Warsaw	Poland
PL	Consortium of laboratories in Poland		Poland
IPQ	Instituto Português da Qualidade	Monte de Caparica	Portugal.
NIMB	National Institute of Metrology	Bucharest	Romania
SU	Institute of Metrology for Time and Space (IMVP) NPO "VNIIFTRI" Mendeleev	Moscow	Russia
SG	Standards - Productivity and Innovation Board		Singapore
SMU	Slovensky metrologi c ky ústav (Slovak Institute of Metrology)	Bratislava	Slovakia
CSIR	Council for Scientific and Industrial Research	Pretoria	South Africa
ROA	Real Instituto y Observatorio de la Armada	San Fernando	Spain
SP	Sveriges Provnings- och Forskningsinstitut (Swedish National Testing and Research Institute)	Borås	Sweden
CH	Swiss Federal Office of Metrology and Accreditation (METAS)		Switzerland
TL	Telecommunication Laboratories	Chung-Li	Taiwan
NIMT	National Institute of Metrology	Bangkok	Thailand
VSL	Van Swinden Laboratorium	Delft	the Netherlands
UME	Ulusai Metroloji Enstitüsü - Marmara Research Center	Gebze Kocaeli	Turkey
LDS	University of Leeds	Leeds	United Kingdom
NPL	National Physical Laboratory	Teddington	United Kingdom
NIST	National Institute of Standards and Technology	Boulder CO	USA
AMC	Alternate Master Clock station	Colorado Springs CO	USA
APL	Applied Physics Laboratory	Laurel MD	USA
USNO	U.S. Naval Observatory	Washington DC	USA

Annex 3. The Distributed Internet and Associated LI Architecture



Annex 4 Measurements Undertaken

In an attempt to evaluate in a relatively modest server setting, the actual performance of currently available NTP client software, a one-week trial was conducted and data collected over a one week period. This is portrayed in this annex as graphical summaries of 57,000 measurements of offset, delay, dispersion and RMS jitter make over the seven day period. The server consisted of a standard Pentium III processor in a Soyo motherboard running Windows NT4 and the most recent NTP v4.0.74 Release for Microsoft Windows NT in an ordinary SOHO environment employing iDSL connectivity. The reference clocks were the primary "tick" and "tock" U.S. master time clock servers at the U.S. Naval Observatory. See Fig. 1

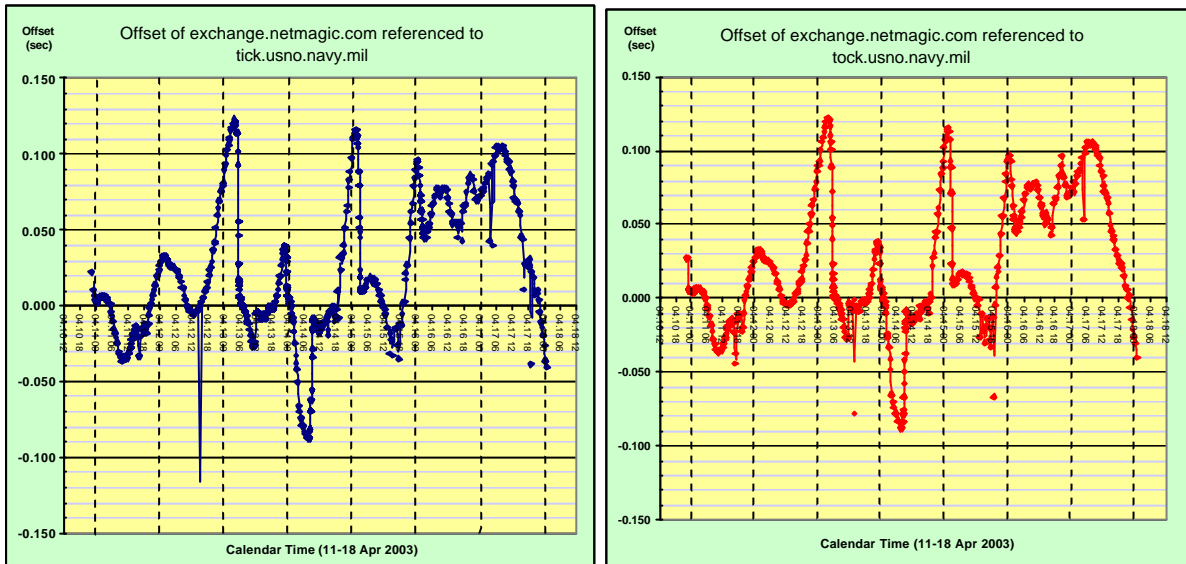


Fig. 1 Offset against U.S. Master Time Clock Servers

The path between the trial server and the reference clocks typically encompassed 13 intermediate routers; displaying the delay characteristics shown in Fig. 2.

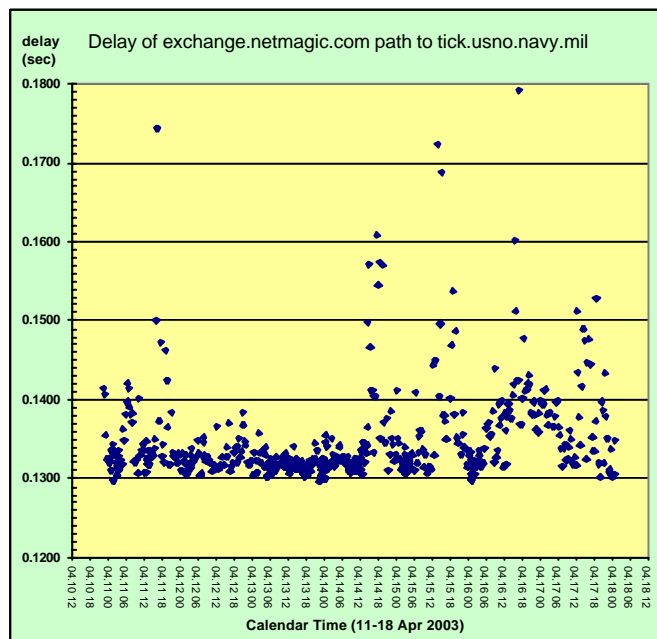


Fig. 2 Delay in path to U.S. Master Time Clock Server "Tick"

The dispersion measurements typically ranged between 100 and 200 milliseconds, with several short periods to as low as 10 milliseconds. See Fig. 3. The value of dispersion in this context represents the uncertainty of the measured server clock values.

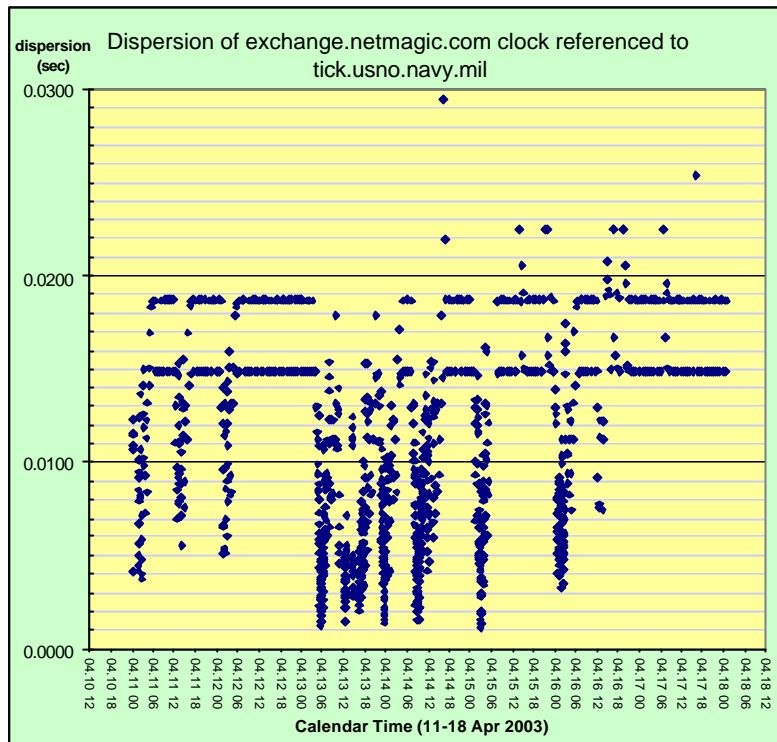


Fig. 3 Dispersion of the measured times reference to U.S. Master Time Clock Server "Tick"

The RMS jitter of the server clock typically measured in the range of 0-50 milliseconds. See Fig. 4.

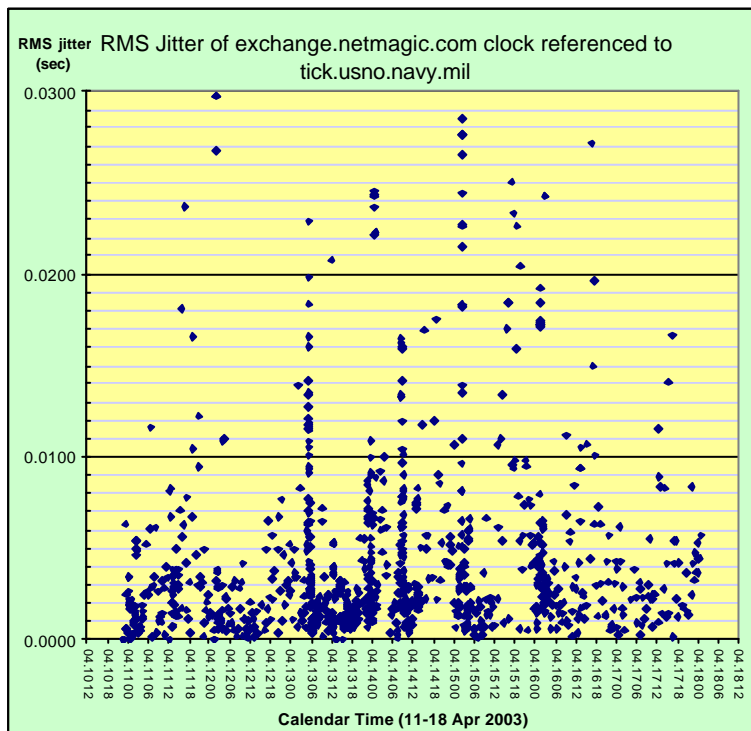


Fig. 4 RMS jitter of server clock relative to U.S. Master Time Clock Server "Tick"