White Paper

Why Time Synchronization Is Critical for Improving Public Safety Answering Points (PSAPs)

Sadie Nedo
Global Account Manager, Commercial Markets, Orolia

WHO SHOULD READ THIS WHITE PAPER

- Network engineers and architects in PSAPs
- Emergency communications teams
- County and municipal IT security professionals
- 911 directors and administrators
- County and municipal network administrators
- County executives

Executive Summary

It goes without saying that we live in an extremely litigious society. In lawsuits involving serious accidents or deaths, significant time discrepancies are often key factors in the outcome of litigation.

On the emergency response side, when 911 dispatch and other recording systems employ synchronized time solutions, the improved data records deliver measurable life-saving differences in their communities and provide the potential for reduced insurance rates.

Incident verification is key, and for E911/communications centers across the country, liability lawsuits initiated by victims are a major concern. Liability suits represent enormous potential financial outlays by a county or other government entity that oversees a communications center. Over the years, various Public Safety Answering Points (PSAPs) have been sued for millions of dollars in cases where a serious injury or fatality has occurred. PSAPs must be prepared to respond to these requests for information – millions of dollars of taxpayer money may depend on it.

County agencies cannot afford to expend time and energy in courts dealing with technical questions about differences in reported times – for example, the response time noted on a CAD report vs. the time noted on a mobile device vs. the time on the officers' reports – only to have these cases thrown out because they couldn't be proven within a reasonable doubt. That leaves the agencies and their employees with questions of liability and potential threats of civil recourse. To meet the challenges of litigation today, it is critical to have the proper resources to accurately document time.

Time Synchronization for Public Safety: Key Considerations

When it comes to keeping time in a Public Safety Answering Point (PSAP), there are three key considerations.

1. **Consistency** – All systems and devices employing time and/or time stamps must use the same references
2. **Credibility** – The references must be traceable to a government-sanctioned body; i.e., UTC time
3. **Accuracy** –Time synchronization must be suitable and sufficient to provide optimum performance for the connected equipment

Time stamped records, especially those on logging voice recorders, are often subpoenaed in court cases, so the use of legally traceable time is critical. When connected to an Orolia NetClock®, time on all the equipment stays synchronized and traceable to US Government-maintained atomic clocks.

Accurate time of day is important in Public Safety 911 and Communications Centers for coordination between and among systems and agencies, as well as for time stamping event records to provide legal evidence of emergency response times in court. Orolia's NetClock automatically keeps all the clocks in a center running exactly on time. Synchronizing each system to a NetClock eliminates the need for an operator to manually reset equipment clocks due to clock drift.

PC clocks are notorious for their low-cost clock crystals and poor timekeeping, with documented drift rates easily reaching and exceeding 7 to 10 seconds per day. This means the 911 telephony, radio and dispatch systems can easily differ by several minutes after just one or two weeks. Providing time to the center from a NetClock improves operational quality and eliminates two important issues: consistency and credibility of the time stamp attached to each of the 911 event records.

There is a relatively new precision timing requirement in the NG-911 all-IP Emergency Services Network. All calls are VoIP now using the SIP protocol, which routes calls to different regional centers and nationwide to search location databases, jurisdictions and records management systems.

To maintain the two-second response time goal – the time between pressing "send" on your phone and when an operator answers – the complex SIP call routing process must be monitored, and time synchronized to the millisecond. Beyond providing Legally Traceable Time®, the time server in the PSAP is now a crucial network monitoring and diagnostic aid for these complex routing functions.

Orolia offers a complete time synchronization solution to public safety agencies, including a GPS/GNSS-based network appliance timing reference and time management software applications to ensure that accurate legal time is delivered and traceability is documented for each workstation. Our long association with NENA and other major solution providers is evidenced by the more than 4,500 PSAPs who employ NetClock® timing systems to maintain credible, consistent dispatching records, support interoperability between systems and inter-agency coordination efforts, and improve overall response times.

Getting Time from the Internet: Don't Do It

There are numerous problems associated with using the internet and public domain time servers:

- **Accuracy** – In an MIT survey, 72% of internet time servers were deemed not useful. Many simply use an arbitrary server time clock. The arrival of the timing packet can continuously change as it transfers across a WAN due to network traffic variations, routing paths, etc., and there is no assurance that internet time is correct.
  - Solution – *NetClock offers a high bandwidth, local, independent, legally traceable timing resource that can respond to thousands of timing requests per second.*
- **Reliability** – Since time from the internet comes from a clock that you don't manage, it cannot be monitored. There are no safeguards against spoofing or time being delivered unintentionally incorrect. Since it is a free service, internet time servers can be unavailable occasionally. Internet sites do not and cannot guarantee 24/7/365 connectivity, and there are numerous instances that have documented the lack of availability.
  - Solution – *NetClock is a solid-state, high MTBF (>100,000 hours) device that tracks multiple satellites simultaneously 24/7/365 for its timing reference.*
- **Security** – Since the time comes from a clock outside the firewall, you must continuously open a firewall port on a scheduled basis. NTP must use port 123, which is a universally known fact to hackers. The files coming in are not under internal control and can't be monitored for security breaches. All public time servers are under constant hacker attack, including DDoS (distributed denial of service) attacks. Even the NIST site has disclaimers to this effect.
  - Solution – *NetClock offers the latest network security protocols that reside behind your firewall.*
- **Traceability** – Internet time has no way to offer an audit trail. NetClocks acquire their time and location data from the NAVSTAR-GPS satellites, which derive their time from the United States Naval Observatory (USNO) and NIST (National Institute of Standards and Technology).
  - Solution – *When NetClock's receiver and circuitry have GPS-lock, all timing outputs are traceable to these time references, including NTP, RS232, 10MHz, etc.*
- **Synchronization** – Wall clocks and other devices are not synchronized to the same source.
  - Solution – *NetClock can provide both network and legacy-based time synchronization to multiple systems and devices throughout a facility.*

Cybersecurity:
The Impact of Timekeeping on Your IT Infrastructure's Security

How your organization keeps track of time has a major impact on the overall security of your IT infrastructure for two reasons.

First, the mechanisms used to keep track of time are among the most vulnerable to exploitation by a hacker. Second, time stamps are critical evidence for retracing a hacker's movements inside a target system – and therefore they can help protect the system against future attacks.

One of the most common time-related vulnerabilities involves the Network Time Protocol (NTP). This protocol, present on virtually all computers, allows the system to synchronize its clocks with a time source over a TCP/IP network such as the internet – or a corporate LAN. If this time source is located beyond the firewall, which is the case when you access free time from the internet, no matter how reliable the source is, potential problems arise. If the time comes from outside the firewall, that means there's a hole left open in the firewall (port 123) to allow packets containing the time information through.

One way to exploit this opening is to crash the NTP program itself. This can be done by sending too much data in an NTP packet. The result is a denial of time services and potentially a crash of the network itself.

NetClock provides the required interface for secure time information. Unlike internet-based alternatives, it provides guaranteed, always-available, highly accurate data without the necessity for continuous external polling outside your firewall (and a five-year industry-leading warranty is standard).

Timing standards that are internal to your organization provide a much higher level of reliability than internet time sources, because the authoritative time server is managed internally and provides secure connections to the GPS system. Providing time on the network as an IP-addressable device behind the firewall ensures that the time source will be as reliable and secure as your own network. Using WWVB of GPS as a time update source supports the use of firewalls and security policies such as MD5. For those who deal in time-sensitive material, issues or operations, the only true safe, secure, reliable, and legally-traceable standard is to use an independent time reference that uses Coordinated Universal Time (UTC) as its source.

If a company chooses to rely on internet time, there is no way to guarantee that the source won't deliver incorrect time. As organizations and processes become even more highly synchronized, the importance of network timekeeping will continue to grow.

Other Reasons to Use a Time Server for Time Synchronization

Using an accurate time reference provides dependable network log files, client/server transactions and email time stamp accuracy.

OTHER REASONS FOR TIME SYNCHRONIZATION

- Achieve accurate file time stamping, fault diagnosis and restoration
- Protect networks against fraud, hacking and commercial disputes
- Ensure compliance with many regulatory standards, including FDA, HIPAA, Sarbanes-Oxley
- Eliminate manual setting errors with full automation

In addition, you'll benefit from network security, confidentiality and authentication of electronic records for:

- 21 CFR Part 11, the FDA guidelines for trustworthy electronic records
  Sarbanes-Oxley
  HIPAA
  HL7
  JCAHO
  ISO/IEC 17799:2005
- Log File Accuracy
- Correct client/server transactions
- Correct email message time stamps

Time Synchronization and IP-Telephony

IP telephony solutions are being deployed in more organizations every year. Yet many users overlook an important part of the system architecture: the need to synchronize the infrastructure design with an independent network time server. Accurate clock synchronization improves performance, effective diagnostics and troubleshooting, and provides reliable call detail records for billing.

Network time synchronization plays a key role in keeping IP telephony networks operational and performing well. Although many people reluctantly accept that a data network may occasionally fail, no one is prepared to lose a voice network for even a minute. Problems with IP telephony must be avoided or, in the worst case, minimized to keep business-critical voice systems operating.

Accurate server and router log files are essential to IP telephony reliability. Every log file entry is time stamped to establish the time of events and facilitate the sequencing of events. Log file data and subsequent reports allow administrators to identify the root causes of problems in the network. Since server logs are a compilation of information from different hosts, it is essential that time stamps be accurate within milliseconds. If they are not, sequencing events can be problematic, troubleshooting root-cause issues becomes much more difficult, and keeping the IP telephony network operations online becomes nearly impossible.

In addition, comprehensive traffic reporting provides information about the grade of service, peak hours and call volumes, and assists in determining whether the network is over- or underused. These same metrics can be used to estimate agent staffing requirements, find dimension s for trunk groups and calculate IP telephony (IPT) bandwidth. Effective actions based on this information, however, cannot be taken if traffic analysis relies on faulty timing or if call rerouting algorithms use time as the trigger – and that time is inaccurate.

Conclusion

If your date/time stamps are simply arbitrary, have no established standard, and other systems and devices in the communications center are not synchronized, there can be no certainty of the data or start/stop times in operations. There is no legal, traceable value and the lack of synchronization can cause inefficient coordination and issues with interoperability between departments and agencies. Using arbitrary, non-standards-based timing can create serious logistical problems when time is in question.

Employing a time server such as Orolia's NetClock offers:

- A NENA-compliant time server/master clock that exceeds NENA Master Clock specifications for timing accuracy and interconnections to all networks and systems in a PSAP.
- Highly secure network design that exceeds NENA TID network security requirements, with software updates provided several times a year at no charge.
- Reliable, accepted product design to synchronize mission-critical systems: over 4,500 E911, RCMP/ Police, Fire & Emergency Communications Centers.
- Established relationships with all the major public safety vendors and integrators. Orolia is the _20-year partner to AT&T, CenturyLink, Motorola, Airbus, Harris, and all the major two-way wireless dealer/integrators in North America.
- Industry-leading tech support and service with live personnel to assist in installation, configuration and troubleshooting, lifetime product support, and lowest total cost of ownership.
- The industry's best warranty: a full five years with average product lifetime exceeding ten years.
- Short lead times – typically two weeks.

For more information, visit www.orolia.com or Request a Quote today.

About the Author

Sadie Nedo is a global account manager at Orolia, where she supports the public safety market. For nearly a decade, she has specialized in helping PSAPs develop and deploy solutions that simplify the integration of precision timing and frequency into their critical infrastructure. She holds a bachelor's degree in advertising and public relations from Rochester Institute of Technology.

About Orolia

Orolia is a world leader in Resilient Positioning, Navigation and Timing (PNT) solutions that improve the reliability, performance and safety of critical, remote or high-risk operations. With expertise in government, maritime, aviation and enterprise applications, Orolia provides virtually fail-safe GPS/GNSS and PNT products and solutions for their customers' most mission critical needs. Orolia's US headquarters is in Rochester, NY, with a commercial presence in more than 100 countries worldwide.

Orolia US Headquarters
1565 Jefferson Road Suite 460
Rochester, NY 14623 USA

Orolia European Headquarters
Parc Technopolis, Bât. Sigma
3 Avenue du Canada
91974 Les Ulis, Cedex, France
Phone: +33 (0)1.64.53.39.80

www.orolia.com
sales@orolia.com

21 May, 2019 - Why Time Synchronization Is Critical for
Improving Public Safety Answering Points (PSAPs) (A)
Specifications subject to change or improvement without notice.