

**Addressing the Need for Synchronized
Time Sources for LANs in Industrial Security Settings
and Other Time-Critical Environments**



GarrettCom™

Industrial Networking at Its Best™

GarrettCom, Inc

47823 Westinghouse Drive

Fremont, CA 94539

Tel: (510) 438-9071

Fax: (510) 438-9072

www.GarrettCom.com

Addressing the Need for Synchronized Time Sources for LANs in Industrial Security Settings and Other Time-Critical Environments

September 2008

When you ask someone what time it is, you can typically absorb variances from the absolute real time as designated by Coordinated Universal Time (UTC). However, there are exceptions, such as when you need to synchronize with train departure times, rocket launches, or the opening bell at a stock exchange. There are similar issues when comparing the recorded time an event took place somewhere on an industrial network.

Often some variation on the time as logged in various parts of a network will be unnoticed and irrelevant; however, there are three areas where absolute time synchronization is critical:

- Video surveillance and physical security
- Operations
- Time slice billing

This paper describes a methodology for ensuring time synchronization on industrial networks utilizing GarrettCom's MNS-6K-SECURE network management system with SNTP server capability.

THE NEED FOR TIME SYNCHRONIZATION

When networks and devices on a network need to synchronize time for various services, they reference an authoritative source for time information. In the USA, this role is provided by National Institute of Standards and Technology (NIST). While an accurate time source can be a NIST web site or a satellite download from an atomic clock, an efficient and effective system for industrial application is a server called an NTP (Network Time Protocol) server – that responds to time synchronization queries within the local area network. In industrial networks, time needs to be synchronized for a variety of reasons.

For example, video surveillance cameras, access control devices, and other security systems must have accurate time stamps. Events logged using *syslog*, for security monitoring must have

an accurate time stamp to allow for database searches and synchronization with other monitoring devices. This is critical not only for localized security monitoring, but also for monitoring on a global basis, as when multiple cyber or physical attacks occur in what might be a coordinated assault on a company, government, or other entity. Without synchronization, it is impossible to coordinate information gathered from a variety of systems to reconstruct the sequence of events or to gather meaningful data using a search based on time stamp.

Operations also needs synchronization for software installations, updates and backups to avoid confusion and to allow reconstruction if there is a system failure. Without accurate time stamps, running system-wide diagnostics or scheduling pings can often be a futile exercise.

Time slice billing for entities such as telecommunications companies and electrical utilities requires accurate timing. When phone records are accessed for billing disputes or criminal investigations, accurate timing is critical. Electrical utilities bill on prime versus non-prime time, and a swing of several minutes could dramatically affect revenues for the utilities and impact the bottom line of some of their large customers.

Time Synchronization Strategies

The standard timescale used by most nations of the world is Coordinated Universal Time (UTC), which is based on the Earth's rotation about its axis. Time Zone offsets are typically set to the UTC, including GMT.

To provide accurate time synchronization to UTC, there must be a reference clock. Today, the cesium clock developed by the National Institute of Science and Technology and the University of Colorado at Boulder is the most accurate – it loses a second only once every 200 million years. Systems around the world access it through satellites that pull the information up and make it available through the world via GPS receivers. Much like the “atomic clocks” that one can install in one’s office or kitchen, a desktop or laptop computer can access the reference clock directly from a GPS receiver (which may be difficult to access from within a modern industrial building). Accessing over the network provides an alternative, hence the need for a time server as well as a time synchronization client.

The problem, of course, comes when multiple attempts are made to access the same information over the same network at the same time, causing not only bandwidth overload but also potential overload on the time server. It is instructive to note that Microsoft Windows OS has a default setting that accesses a site managed by Microsoft as well as NIST. The site may have a few million hits per second, and it doesn't have the bandwidth to respond. Sometimes requests are dropped or ignored due to the load. This is normally not a problem -- a home PC can afford to lose a few seconds -- but for a power plant or a video surveillance site, when accuracy is more critical, the solution is often a local, reliable time source. These local services have a high probability of immediate response, and reduce the demand on WAN bandwidth.

Simple Network Time Protocol (SNTP)

One of the best solutions for setting up a local time synchronization server is SNTP, a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. Having a local SNTP source reduces upstream network traffic and improves efficiency by providing a quick response to synchronization queries. SNTP is compatible with NTP as implemented for the IPv4, IPv6 and OSI protocol stacks. NTP is more than 20 years old and one of the oldest Internet protocols still in use. It was designed by Dave Mills of the University of Delaware, who still maintains it with a team of volunteers.

GarrettCom offers a time synchronization service, along with other high-end security features in its MNS-6K-SECURE network management software package, offered as an option with GarrettCom Magnum 6K switches. MNS-6K- SECURE allows a network administrator to set up a reliable time source for one or multiple LAN segments. Video capture devices, time clock card readers, and door access devices that may be connected to an Ethernet network can be synchronized using the Magnum 6K time synchronization capabilities. PCs running Windows XP, Vista or other operating systems such as Linux can also synchronize from the time source on MNS-6K-SECURE.

For more information on Simple Network Time Protocol (SNTP) and Network Time Protocol (NTP), see the descriptions in IETF (Internet Engineering Task Force) RFC-1769 as well as in RFC-2030. A complete description of how to set up a time service using the GarrettCom

Magnum 6K family of switches with MNS-6K-SECURE, version 14.1 and higher, is available, along with more information on time synchronization and its history, in GarrettCom's Technical Brief, "Synchronizing Time Sources and Setting up Reliable Time Services in a LAN" August 2008. (http://www.garrettcom.com/techsupport/papers/setting_up_reliable_time.pdf)

####

GarrettCom, Inc.

47823 Westinghouse Dr. • Fremont, CA 94539

PH: (510) 438-9071 • FAX: (510) 438-9072

Email: mktg@garrettcom.com • Web: www.GarrettCom.com



©2008 GarrettCom, Inc. Printed in United States of America

GarrettCom, Inc. reserves the right to change specifications, performance characteristics and/or model offerings without notice. GarrettCom is a registered trademark of GarrettCom Inc. Magnum, S-Ring, Link-Loss-Learn, Converter Switch, Convenient Switch and Personal Switch are trademarks of GarrettCom, Inc. NEBS is a registered trademark of Telcordia Technologies. UL is a registered trademark of Underwriters Labs.