Symmetricom

WHITE PAPER

The Importance of Network Time Synchronization For Enterprise Solutions

Introduction

As you read this, your network of workstations and servers, each with their own clock, are time stamping files, email, transactions, etc., all the while your server logs are recording every manner of transaction in the event you need that information. At some point during the day it is quite likely that automatic processes such as archiving, directory synchronization, cron jobs, etc. will execute and alter files based on time stamps. Fundamental to all of this is the belief that the time is correct. Even if the time is not absolutely correct there is often a belief that at least the time is "close enough." This paper describes why "close enough" is no substitute for accurate network time and why network time synchronization is critically important.

Computer clocks are notorious for drifting. They are typically based on inexpensive oscillator circuits or battery backed quartz crystals and can easily drift seconds per day, accumulating significant errors over time. With increasing distributed computing and our interdependence on network infrastructures, having many clocks continuously drift apart puts the network infrastructure and the applications that run on it at risk. In particular, network operations and application related activities are most susceptible to problems related to the lack of time synchronization.

Network Operations

Network operations require time synchronized information to ensure optimal network performance. Often it is not until there is a problem that the lack of time synchronization becomes a key factor in either a failure or the ability to troubleshoot one. In other instances, network processes will not function without time synchronization.

Key areas where time synchronization directly effects network operations are:

- Log file accuracy, auditing & monitoring
- Network fault diagnosis and recovery
- File time stamps
- Directory services
- Access security and authentication
- Distributed computing
- Scheduled operations
- Real-world time values

Log File Accuracy, Auditing & Monitoring

Server log files and subsequent reports allow you to use the data to assess activities within your organization. This includes firewall and VPN security-related activity, bandwidth usage, and various logging, management, authentication, authorization, and accounting functions. Since server logs are a compilation of information from different hosts, it is essential that the time stamps be correct. If not, you will have difficulty ordering events and troubleshooting root-cause problems. Statistics about any factors that relate to time will be difficult to interpret and possibly meaningless. Even in routers, centrally logged configuration events and system error messages, such as router configuration changes, interface up/down status, modem events, security alerts, environmental conditions, trace backs, and CPU process overloads rely on network time synchronization for accurate time stamps for the data to have meaning.[1]

A number of enterprises have suffered from highly publicized Denial of Service attacks. In this case, Remote MONitoring (RMON) logs typically used to detect root-cause network events, are used by network security experts to re-construct the scene of a network crime. Accurately time stamped network packet transits provide the forensic evidence to make this possible.

Network Fault Diagnosis and Recovery

Most IT organizations are measured on their ability to maintain full flow network operations. Strict limits on allowable downtime are one of the most common Quality of Service metrics in place and every IT department is acutely aware of it. In the event of failure, accurate network timing is crucial to fault diagnosis and recovery.

To assist in fault diagnosis, loss of connection, buffer over-flow, missing packets and other key network events are trapped, reported, and logged using the RMON services that reside in servers, routers, switches, and dedicated instruments. Should the network crash, starting with the root-cause, a stream of RMON events will be reported. Each of these events is indexed with the network time stamp affixed by the reporting RMON agent. If these time stamps are synchronized, the proper order can be established and the root-cause quickly identified. Without accurate network synchronization, root-cause isolation is obscured and down-time prolonged.

File Time Stamps

The integrity of any file system is heavily reliant on the name and dates of the files themselves. Individual files typically track the dates for creation, last accessed, last archived, and last modified. In a distributed file sharing system, a master file is maintained by a Network File Sharing (NFS) server for use by remote clients. NFS is network time dependent – when presented with duplicate file names, it saves the latest copy; however, if a client time stamps a remotely accessed file with a time earlier than the file maintained on the server, the client file, along with any changes, will be discarded.

The Importance of Network Time Synchronization For Enterprise Solutions

Directory Services

Network time synchronization is an important part of network design and implementation. For example, many network directory services systems exchange information and synchronize changes in the directory services database according to time stamps. Groupware applications require accurate time for scheduling and collaboration. Without a time-synchronized network, time-sensitive systems and applications will not work correctly. In a Windows active directory network, all PDCs and client workstations need to synchronize with a single, accurate, and standard time source.

Access Security and Authentication

Windows 2000 and later is the most prominent example of the requirement for network synchronization. Synchronized time is critical in Windows because the default authentication protocol (MIT Kerberos version 5) uses workstation time as part of the authentication ticket generation process. Windows includes the W32Time Time service tool whose purpose is to ensure that all Windows-based computers in an organization use a common time. The Time service uses a hierarchical relationship that controls authority and does not permit loops to ensure appropriate common time usage. All client desktops and member servers nominate their inbound authenticating domain controller as their time partner. This continues up through the hierarchy of domains to the primary domain controller (PDC) at the root of the forest.[2] This PDC is set to synchronize with a reliable time source, such as a dedicated network time server. If a time server is not available and the time difference between domain controllers drifts beyond the skew allowed by Kerberos, authentication/logon between two domain controllers may not succeed and error messages can result.[3]

Scheduled Operations

Cron scripts and crontabs are a list of one or more commands to a computer operating system or application server that are to be executed at a specified time. Each command is executed when its triggering time arrives. In most cases these commands, commonly data back-up oriented, happen at pre-specified times that are intentionally scheduled late at night or after the close of business. Synchronization of a single host with an acceptable time source is mandatory so that commands happen when expected. In the case of multiple hosts responsible for executing independent cron files, time synchronization between the hosts becomes even more critical so that scheduled activities are properly coordinated.

Real-World Time Values

There is no substitute for operating a network using real-world time values. While you can synchronize a network to the incorrect time and have it function, this is a very undesirable policy. Local networks are interconnected with other, larger networks, particularly over the Internet, and correct time is the single common denominator. Real-world time is based on Universal Time Coordinated, or UTC. UTC is the latest in what originated as Greenwich Mean Time (GMT). Networks operating on the underlying UTC share a common time base. UTC time is best obtained from an accurate, secure, reliable source and then converted to local time by all operating systems that reference that source. It is this common time reference that provides network managers the time-accurate information they need about their network to ensure optimal performance and avoid many of the problems discussed in this paper.

Applications

Many applications use time stamps as a key element that adds tremendous meaning to measured and generated data. Shared databases, billing and transaction systems, data acquisition, email, and many more applications rely heavily on accurate time stamps of varying degrees of precision. While the scope of time stamp use is immense, some common applications rely heavily on network synchronization to provide the time for a meaningful time stamp.

Key areas that time synchronization directly effects applications are:

- Transaction processing
- Software development
- Email
- Legal and regulatory requirements
- Password and digital ID

Transaction Processing

Time synchronization in transaction processing is not new. Even since the 1960's, IBM recognized that time synchronization was critical to execute very high value transactions. To quote from IBM's 'Redbook': "There has

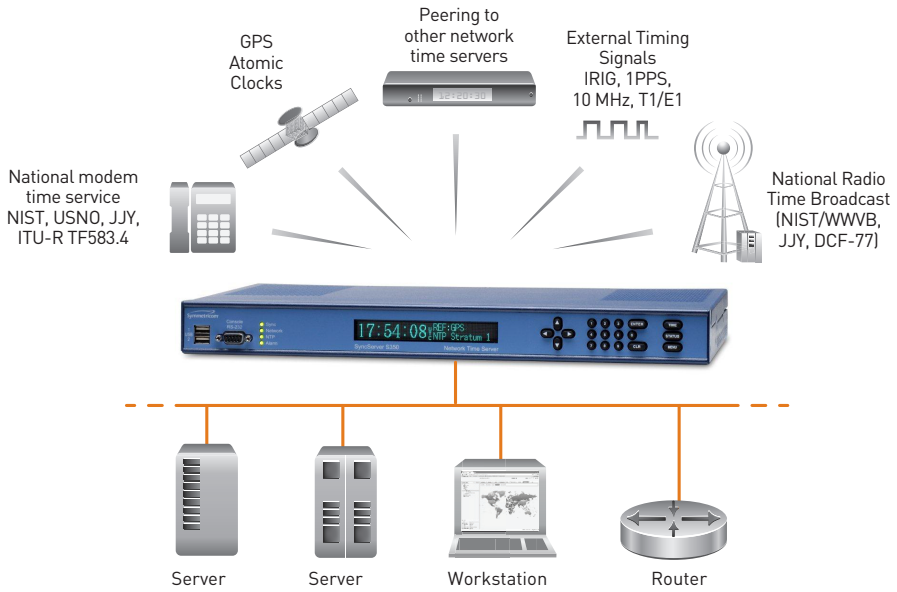

FIG.1 Typical infrastructure devices needing accurate, real-world network time synchronization

The Importance of Network Time Synchronization For Enterprise Solutions

been a long standing requirement for accurate time and date information in data processing. As single systems have been replaced by multiple, coupled systems, this need has evolved into a requirement for both accurate and consistent clocks among these systems." Today we use many servers and workstations of different types and function, all networked together, performing a variety of transactions. Application time stamps tend to have a 1 second lower limit (absolute). These time stamps basically answer the question, when did the transaction occur – I.E. when was a purchase order issued, the phone call connected and completed, etc.

The need for transaction time stamp accuracy at the millisecond level is caused by a need to place transactions into a correct sequence of execution, particularly if there are a great deal of near simultaneous trans actions (see Legal discussion below). Since computer operations happen automatically and quickly, system clock resolution must be less than the minimum transaction composition and transmission time – leading to a need for 1-2 millisecond resolution.

Software Development

Software development can be a very distributed task as teams of programmers develop code stored on different servers and sometimes at different geographic locations. Eventually this code is compiled into a single program. A 'make file' function or version control system of some sort is used to manage the compilation of the software from the distributed servers. File time stamps are used to decide which files need to be rebuilt when the underlying source file has been changed. If some of the directories are NFS mounted, and the server and client have different notions of the current time, then the 'make' function can fail to rebuild some derived objects and produce an executable that is not based on the most up-to-date sources.

There have been many reported instances of engineers entering a 'fix' into a source code file, only to have the 'fix' dropped during the final 'make' operation – with embarrassing and costly results to the company. These types of errors are very difficult to detect. The first response is often to blame a software bug in the application. Countless hours have been wasted by application coding teams generating test scenarios to detect a bug that is, in fact, an infrastructure issue related to lost file changes due to lack of server time synchronization.

Email

Email is the de facto standard of written business communication. Every email message passing across the network bears the originator's time stamp. If that time stamp is obviously in error, it can create confusion on the part of the recipient, not to mention it challenges the credibility of the originating organization.

Legal and Regulatory Requirements

Sometimes you have to provide accurate, traceable network time because the laws or rules governing your industry require it. For instance, the National Association of Security Dealers, NASD, requires its members to time stamp stock trades with an accuracy of 3 seconds or better traceable to UTC at the National Institute of Standards and Technology, NIST. This represents a very large synchronization challenge since the NASD has 5,500 members with more than 82,000 branch offices across the U.S. The reason for synchronized, traceable time is to validate when a transaction occurred for the purposes of order auditing. Other applications such as legal, medical and telecommunications are also expected to adopt traceable time standards as part of their network operating policies.

Password and Digital ID

In 2000, the United States passed the Electronic Signature Act. This act provides properly secured and identified computers the power of attorney to commit their host organization to a contractual obligation. When a computer or person possesses the correct password or digital identification, it/they have the power to conduct business. In turn, it is crucial to be able to deny access the instant the password or digital certification is withdrawn.

A typical example is when an employee having access to company accounts via a digital certificate leaves the company, the certificate must be revoked to prevent continued access. Since the digital ID certificate exists in 'cyberspace,' the time of certificate revocation must also be lodged into cyberspace, and any process that uses this certification must have a synchronized network clock to correctly determine whether or not the certificate has passed its revocation time.

Summary

At Symmetricom we have learned the value of network time synchronization from the experiences of our customers. Everyday we help customers whose job it is to keep the essential network functions of their companies running smoothly. These customers recognize that many network operations and applications rely on accurate network time synchronization to function properly and be more manageable in the event of a failure.

We strongly believe that taking a proactive position with regard to establishing a high quality network time synchronization system pays dividends both now and in the future. GPS synchronized network time servers like Symmetricom's SyncServer S200/S250 and S300/S350 have the ideal features to form the basis of such a system.

References

[1] Cisco Systems; Using Syslog, NTP, and Modem Call Records to Isolate and Troubleshoot Faults; http://www.cisco.com/univercd/cc/td/doc/cis intwk/intsolns/dialnms/syslog.htm

[2] Basic Operation of the Windows Time Service; http://support.microsoft.com; Q224799

[3] RPC Error Messages Returned for Active Directory Replication when Time is Out of Synchronization; http://support.microsoft.com

Symmetricom

2300 Orchard Parkway
San Jose, California 95131-1017
tel: 408.433.0910 fax: 408.428.6960
www.symmetricom.com