



Standards and Practices

S&P Article ID: SAP-003

Title: Network Time Synchronization

Description: SNTP network design/implementation for time sync

Revision / Date: 1.0 / 2007-01-22

Status: Final

Author: Glenn Barnas

Client Approval:

Network Time Synchronization

Network time synchronization is a simple task that can be the underlying cause of numerous, difficult to diagnose problems. The Windows time service, while suitable for Active Directory, does not provide adequate accuracy for many applications. It also does not provide the features needed for an enterprise class time synchronization tool, such as control over synchronization cycles, logging, or stratum management.

The implementation of an enterprise time synchronization environment is fairly straightforward, and is based on the industry standard NTP/SNTP protocol. (S)NTP provides a high degree of accuracy, is highly configurable, has excellent status and error reporting, and is available for all major operating system environments.

NTP is implemented in a hierarchal structure. At the top level is a highly accurate time source, such as an “atomic clock”. These represent “Stratum 1” time sources, and are usually maintained by national governments, universities, and standards organizations.

Within an organization, one system is chosen to be a master time source. This system obtains its time from an external Stratum 1 source, and becomes a Stratum 2 time server. All other internal time sources utilize this Stratum 2 server as their time source, insuring that time within the organization remains in sync, even if access to the Stratum 1 server is unavailable. A collection of time servers is used to distribute the load within the organization, and these become Stratum 3 systems, synchronizing only with the internal Stratum 2 server. All other systems utilize the internal Stratum 3 servers as their time source. In a Windows / Active Directory environment, the PDC Emulator uses the Stratum 3 server as a time source, and becomes an “authoritative” time source for the remaining Domain Controllers. All Windows desktop clients then synchronize time from their nearest domain controller.

This design assures accurate time is maintained throughout the enterprise, while balancing the costs of third-party software and implementation man-hours.

Implementation Process

This section outlines the steps needed to implement an enterprise time sync service.

1. Implement a “TimeMaster” server within the network. This single* server connects to an outside source to obtain time. All other Time Servers use this as their time synchronization source. The TimeMaster must be configured to always provide “reliable” time, even when it has failed to communicate with its time source. (In other words, it should never report a “not synced” condition). This assures that all internal servers remain in sync with each other, if not with the outside world. The alternative, when the TimeMaster reports a not-synced condition, is the individual time servers do not sync and rely on their internal hardware clocks. This is *not* a desired condition, as the clocks can be inaccurate, and wide drift between the secondary time servers is possible. The TimeMaster can be a server or a router.
* This can be a cluster, or a pair of SNTP peers for redundancy. The object is to only have the “TimeMaster” system obtain external time, and always report that their time is accurate.
2. Implement the network routers as the secondary TimeServers. These NTP servers sync with the TimeMaster, and provide NTP access to clients on each subnet.

3. Configure all *application* servers to use NTP based time synchronization, using their local gateway or a defined local timeserver as a primary time source, and the TimeMaster (or a secondary time server) as their secondary time source. Both Unix and Windows servers will share a common time source. Unix systems have an NTP client in their default configuration. Windows servers should have a third-party NTP client installed (such as the Dillobits SNTP service or the Windows NTP implementation from <http://www.meinberg.de>) to obtain higher accuracy than that provided by the Windows Time Service. Dillobits SNTP is a commercially supported product available at a reasonable cost, while the Meinberg NTP implementation is open-source and community supported. Other options are available – these are two that are known to work well.
4. Configure the AD PDC-emulator to use Windows Time Service, referencing the TimeMaster for primary NTP time sync, and its gateway as a secondary time source. This server should be configured as an “authoritative” Windows time source.
5. Configure all other AD domain controllers to obtain time sync via Windows Time Service, referencing the PCD-emulator as their time source. This is a default configuration.
6. Configure all Windows desktop clients to use Windows Time Service to sync time with their domain controller. This is a default workstation configuration.

The windows time service (W32Time) should be disabled whenever an alternate time sync service is installed. NTP is natively available on Unix/Linux systems, and can be configured simply by editing the appropriate configuration file to define the time sources.

Steps 4 and 5 can be performed using the w32tm.exe command with appropriate arguments.

Time Sync Schedule

The frequency of time synchronization will change based on the Stratum level of the server.

Internal Stratum-2 server	every 17 minutes
Internal Stratum-3 servers	every 136 minutes
Windows Domain Controllers	Microsoft defined frequency – 8m to 8h depending on prior sync offset. This is not definable.
Application Servers	every 2-4 hours

Network Concept Diagram

