

Technical information

Technical Information

- Introduction to NTP
- NTP on Unix systems
- Fetching and building the NTP software
- NTP on non-Unix systems
- Your own clock
- Advice from CSIRT

Introduction to Network Time Protocol (NTP)

Accurate time is needed across the network for a number of reasons, as well as being desirable on convenience grounds. Some security mechanisms rely on the time being the same in distributed systems; log scanning for security incidents is easier; information in mail headers and the like is more useful. Where file systems are updated by a number of computers (distributed systems), the computers' clocks need to be kept in step.

The Janet Network Time Service delivers a stable time reference to organisations using the Network Time Protocol (NTP) specified in [RFC 5905](#) [1]. The RFC defines messages to be sent between systems, which contain the current time as known to the sender and other information sufficient for the NTP process running on each system to compensate for network delays and assess the quality of each source. By exchanging messages with a number of time sources the NTP server software can calculate a precise time with which it can synchronize the system's own local clock. The system can, in turn, be used to provide the time to others. This mesh of communicating systems gets "true time" from external references which may be atomic frequency standards, radio clocks that receive broadcast time signals from special dedicated transmitters, or the GPS (Global Positioning System) satellite navigation system. The result is that clock settings across the whole mesh are very closely synchronised and a single rogue system with the wrong time will have very little effect.

The number of steps a particular system is from an independent time source is called its "stratum". An external reference such as an atomic clock is stratum-0. A computer directly

linked to an external clock and taking its time from it will be stratum-1. A computer obtaining time information from NTP sources including at least one stratum-1 will normally operate as stratum-2, and so on. Although having a low-stratum machine is broadly a good idea, it is not necessary in normal use and the majority of end-user systems will typically run at stratum-2, 3 or 4. An excessive number of clients on one server may adversely affect the system and thus the time quality. The Sun servers used as Janet servers readily cope with 1000 clients, but 10,000 is too many. It is, therefore, a bad idea to try and run all machines at stratum-3.

NTP is designed to be resilient to failures and aberrant behaviour of clocks, servers and network links. Although at any one time a system will be using the time from only one server, it will typically be exchanging NTP messages with several other servers to provide redundancy and a quality check. For this to be effective, a site server should be configured to communicate with a number of servers that have independent paths to external sources of time, i.e. to different radio clocks. We recommend that a Janet site has up to four local servers (stratum-2) distributed around it, each server peering with a different Janet stratum-1 server. The local servers can in turn provide a feed for the rest of the site. This limits the NTP traffic across the wide-area network and the load on the stratum-1 servers.

NTP on Unix systems

The main NTP implementation is public-domain Unix software developed by the NTP author, David Mills of University of Delaware et al. The distribution is steadily being improved, and comes with a README file.

For Unix systems, the current production version is ntp-4.2.6p5 which implements the latest NTP 4 specification. Version 4 includes a number of enhancements over NTP 3. [RFC 5905](#) ^[1] contains the full specification of the protocol as well as considerable background material on time.

Fetching and building the NTP software

Recent Unix systems may come with a version of ntpd already installed, or pre-built packages may be available from the usual software repositories or the suppliers.

For end-user Unix systems, ntpd itself is straightforward to build, install and configure on most platforms.

The ntpd source distribution can be found at: <http://www.ntp.org/downloads.html> ^[2]

The Makefiles for ntpd are sophisticated internally but simple to use, and can cope with the differences between most systems. In most cases, it should be sufficient to read the upper-level README and INSTALL files and just type "configure" and "make" to build the software for the Unix platform. Then typing "make install", as *root*, will install it.

Having built and installed the ntpd daemon and various utilities, a configuration file will need to be created for the daemon to work properly. Notes on configuration of ntpd in general are in the "html" subdirectory of the ntpd build. Further information, is available at the NTP Public Services Project <http://support.ntp.org> ^[3] The configuration files of the top-level servers for each site will need to be set to reference the Janet stratum-1 servers.

If you require any further help in fetching and building the software, then contact the Janet Service Desk [4].

NTP on non-Unix systems

For non-Unix systems, the production version can be built on some recent versions of Windows, and a pre-built version with installer is available from Meinberg at <http://www.meinbergglobal.com/english/sw/ntp.htm> [5].

Windows systems now come with their own implementation, Windows Time Service, also known as w32time or w32tm, for which admins should see Microsoft's documentation.

Your own clock

Janet organisations may wish to acquire their own stratum-0 radio or GPS clock and attach it to one of their servers, making it a stratum-1. This will improve the resilience of time distribution within the organisation, as the network distance to the Janet servers means reduced accuracy in comparison to an onsite clock. Radio clocks are available from various manufacturers and ntpd has support for most of those on the market.

Advice from Janet CSIRT

The Janet CSIRT department has provided useful advice on securing ntp servers from DDoS attacks <https://community.ja.net/library/janet-services-documentation/seven-steps-secure-ntp-servers-ddos-attacks> [6].

Source URL: <https://community-stg.jisc.ac.uk/library/janet-services-documentation/technical-information>

Links

[1] <http://www.faqs.org/rfcs/rfc5905.html>

[2] <http://www.ntp.org/downloads.html>

[3] <http://support.ntp.org>

[4] <mailto:service@ja.net>

[5] <http://www.meinbergglobal.com/english/sw/ntp.htm>

[6] <https://community.ja.net/library/janet-services-documentation/seven-steps-secure-ntp-servers-ddos-attacks>