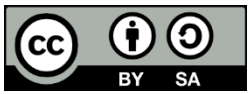
Network Time Protocol

Presentation by Wyatt Zacharias



History

- First network time protocol developed in 1979 and demonstrated at the National Computer Conference. Later described in IEN 173 and made into the Internet Clock Service described in RFC 778.

- Others that came soon after included *Time* and *Daytime* protocols, as well as *timed.*

- In 1985, NTPv0 is implemented on both UNIX and Fuzzball routers, and described in RFC 958.

- NTPv1 released in 1988, which includes the client-server and peer-to-peer functionality seen today.

Basic Operation

- NTP typically runs in a client-server model and will poll multiple servers on diverse networks to achieve synchronization.

- In order to synchronize its clock to the server, the client must know both the local clock offset from the server, and the round-trip time of network traffic between the client and server.

- Once the offset and round-trip times are calculated NTP uses statistical analysis to remove outliers and anomalous values.

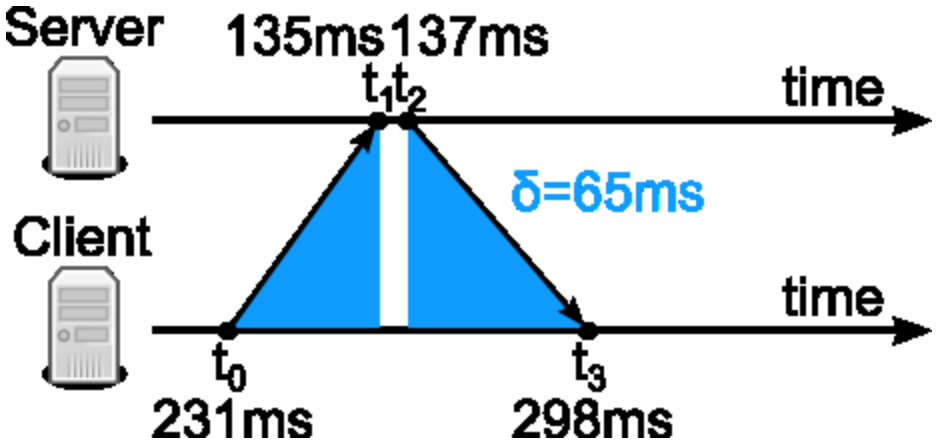
- NTP can however suffer from inaccuracy when packet travel times are asymmetric because the algorithm assumes that the time from server to client is half that of the round trip time.

Offset Calculation

$$\theta = \frac{(t1-t0)+(t2-t3)}{2}$$

Round-Trip Calculation

$$\delta = (t3 - t0) - (t2 - t1)$$



Clock Strata

- NTP uses a hierarchical system of time sources, with each level in the hierarchy assigned a number from 0-15.

- The NTP stratrum number is used to denote a server's logical distance from a reference clock.

Stratrum 0

- High precision atomic clocks that generate pulse signals for connected devices.

Stratum 1

- A server that is directly connected to a Stratum 0 clock, and is accurate to within a couple micro seconds.

Stratum 2

- A server that is connected to one or more Stratum 1 servers. Typically several stratrum 2 servers will be peered to provide robust time to other hosts on the network.

Stratum 3-15

- Servers that are logically farther and farther away from a reference clock.

Popular Implementations

NTPD

- Produced by The NTP Project, and considered the reference implementation of the protocol

Crony

- Claims to be faster and more accurate than NTPD. Adopted by RedHat as the stock NTP daemon as of RHEL 7.

OpenNTPD

- Developed by the OpenBSD foundation. Focused on security at the expense of speed and accuracy.

Vulnerabilities and Attacks

- In the last few years a number of vulnerabilities have been found in the NTP daemon, especially vulnerabilities that allow it to be used in DDoS attacks.

- Versions prior to 4.2.7 released in 2013 were easily exploited for use in DDoS attacks due to bad default configuration.

- In 2015 it was found that versions prior to 4.2.9 did not properly perform message authentication of data received from a server, allowing a man in the middle to insert bogus time data.

Server Pools

- As the number of network devices has been growing, each with the need for synchronized network time, the need for reliable public time servers is far beyond any central organizations capacity to provide.

- The NTP Pool project was launched in 2003, which provides a dynamic list of public NTP servers that have volunteered to provide NTP service to public clients.

- The current pool contains over 4000 servers providing network time, all of which are periodically verified to provide accurate time.

Demo