Sensor Network

NTP – Network Time Protocol

Laura Etro - 12240371
Denis Tavaris - 12240475

22.06.2023

What is NTP?

The Network Time Protocol can be seen as a set of rules that establish how devices on a network should transmit, receive and understand data. The protocol uses a symmetrical architecture, with a sub-network of distributed time servers operating in a self-organizing hierarchical configuration, synchronizing local clocks within the sub-network with national time standards via cables or calibrated atomic clocks. The servers can also redistribute time information within a network via local routing algorithms.

Importance of the NTP protocol and areas of application

The global computer network depends on the Network Time Protocol (NTP) and this has provided a standardized method for synchronizing the clock of computers to the Internet since its foundation in the 1980s. This time synchronization is essential for many operations we perform every day, such as safely surfing the web and making financial transactions online. In the past, the lack of precise synchronization could cause disorder and confusion in computer systems. Today, with the increasing complexity and interdependence of computer systems, it is even more important to maintain precise time synchronization. In fact, many modern applications, such as cloud computing, the Internet of Things, blockchain and cybersecurity, would be significantly less efficient and might not even function properly without the NTP protocol. Therefore, NTP has not only made an invaluable contribution in the past, but continues to be a vital component of modern network infrastructures.

UTC

Universal Coordinated Time (UTC) is an essential parameter in the time synchronization process, especially in the Network Time Protocol (NTP). This can be seen as the clock to which all devices in a network refer to align. In the global landscape, UTC emerges as fundamental for several reasons.
Firstly, the primary reference sources, i.e. time servers, must provide continuous local time based on UTC. This means that UTC serves as the universal time standard to which all time server clocks are synchronized.
Secondly, the NTP protocol must function in such a way that it also handles leap seconds, which are inserted into UTC. Interleaved seconds are added to compensate for small variations in the earth's rotation and keep UTC aligned with International Atomic Time (TAI). This aspect underlines how UTC, and consequently the NTP protocol, must be flexible and precise to ensure accurate time synchronization.
Third, in situations where connectivity to the network is unstable or lost, the ability to maintain a UTC-based time reference becomes crucial. Even if a device loses connection with the NTP server, it can continue to maintain an internal UTC-based clock until connectivity is restored and the clock can be synchronized again.
In summary, UTC is at the heart of time synchronization in the NTP protocol, acting as a universal time reference that all devices seek to align with, ensuring consistency and time accuracy in complex, geographically distributed networks.

Network architecture

An NTP network consists of one host configured as an NTP server and all other hosts on the network are configured as NTP clients. The Network Time Protocol (NTP) uses a tree-shaped hierarchical network architecture. Each level of this hierarchy is called a **stratum** and is assigned a number, starting from zero and going up to 15. The first number represents the hardware reference clocks. A level one server synchronizes itself with a level zero server, and this relationship continues in such a way that a server synchronized with a stratum **server n** operates at **stratum n+1**. In other words, the stratum number represents the distance to a precise reference clock.

A description of the different stratum levels and a diagram follows:

- Stratum 0: This stratum includes high-precision time measurement devices such as atomic clocks, GPS or other radio clocks. They generate a very precise time signal that is directly connected to a connected computer. Stratum 0 devices are also known as reference clocks. NTP servers cannot advertise themselves as stratum 0.
- Stratum 1: These are computers connected directly to stratum 0 devices. Their system time is synchronized within a few microseconds with their connected devices. Stratum 1 servers can interact with each other for health and backup control. They are called primary time servers.
- Stratum 2: These are computers synchronized on a network with stratum 1 servers. Often a stratum 2 computer queries several stratum 1 servers and selects the most accurate time representation from them. Stratum 2 computers can also interact with other stratum 2 computers to provide a more stable and robust time representation for all devices.
- Stratum 3: These are computers synchronized with stratum 2 servers. They employ the same interconnection and data sampling algorithms as stratum 2, and can in turn act as servers for stratum 4 computers, and so on.

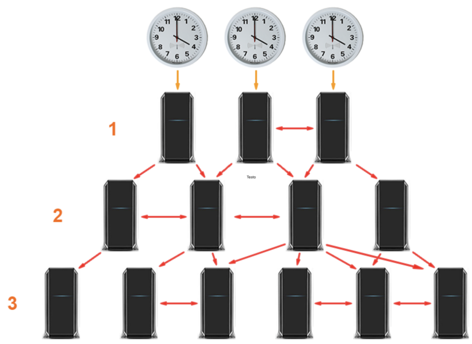

Image source:
https://www.galsys.co.uk/news/what-is-ntp-a-beginners-guide-to-network-time-protocol/

This hierarchy continues up to stratum 15. The reference clocks at the top of the hierarchy are accurate time-measuring devices, and stratum 1 includes the computers connected to these clocks where the increase in stratum numbers indicates from where each computer synchronizes time data.

The clock synchronization algorithm

Network Time Protocol (NTP) is based on a clock synchronization algorithm, which ensures that all devices in a network are synchronized with an accurate reference clock. During a typical operation, an NTP client regularly queries one or more NTP servers for updated time data. When it receives new data, the client calculates the time offset and round trip delay from the server.
The time offset (θ) is the absolute time difference between the two clocks, including the duration of the packet transmission between the client and the server. This is defined mathematically as:

$$\theta = \left| \frac{(t_2 - t_1) + (t_3 - t_4)}{2} \right|$$

Using the time data, we can also calculate the network delay (δ):

$$\delta = (t_4 - t_1) - (t_3 - t_2)$$

Where:

- t1 is the client's time at the time of transmission of the request packet,
- t2 is the server's time at the time of receipt of the request packet,
- t3 is the server's time at the time of transmission of the reply packet,
- t4 is the client's time at the time of reception of the reply packet.

Synchronization algorithm

In the NTP protocol the time synchronization algorithm is one of the main and most important parts. Marzullo's algorithm is the synchronization algorithm used in NTP and is used to compute the best estimate of the true time while accounting for clock offset, clock skew, and network delay. The main idea behind this approach is to collect timestamp information from several time sources, which are commonly referred to as time servers. These time servers send their timestamps to the client device that requests time synchronization.

The algorithm uses statistical methods to examine the collected timestamps and identify the most accurate estimate of the true time in order to synchronize the time. It takes into account elements such as clock offset and clock skew. Marzullo's algorithm seeks to reduce the influence of outliers or inaccurate time sources by analyzing timestamps from several time servers and using statistical techniques. It computes the most likely time estimate by accounting for clock offset and skew fluctuations, adjusting for network delays, and producing a more precise and synchronized time.

NTP processes

NTP is mainly divided in three steps in order to ensure accurate time synchronization: filtering, selection and clustering:

- Filtering in NTP is examining time information received from various time sources and applying methods to eliminate outliers and incorrect data. NTP uses statistical methods to assess the consistency and accuracy of time readings collected from various sources. NTP enhances total time synchronization accuracy by filtering out inconsistent or erroneous data.
- After filtering, NTP chooses the most accurate and dependable time sources for synchronization. NTP assigns a **stratum** level to each time source based on its proximity to a reference clock. The closer the time source is to the reference clock, the lower the stratum level. NTP prefers time sources with lower stratum levels because they are more accurate and trustworthy. To choose the best time sources, the selection procedure considers parameters such as network delay, round-trip time, and synchronization distance.
- Clustering is used to improve reliability and fault tolerance in larger NTP systems with numerous servers. Clustering is the process of arranging NTP servers into clusters, each with

its own primary server. The primary server is in charge of determining the best time sources within the cluster and synchronizing time for the other servers in the cluster. This hierarchical structure distributes the strain and ensures that even if one server dies or becomes unreliable, the remaining servers in the cluster can still maintain correct time synchronization.

Overall, the filtering, selection, and clustering procedures of NTP work together to increase time synchronization accuracy, reliability, and fault tolerance. NTP assures that devices in a network can maintain precise and continuous time synchronization by filtering out untrustworthy data, selecting the most accurate time sources, and using clustering for fault tolerance.

Security aspects in NTP

NTP integrates several critical security components to protect against common security threats. There are both problems and solutions in the field of security applied to NTP.

MITM (Man-in-the-Middle) attacks, in which an attacker intercepts and manipulates communication between the time server and client, are one of the most prevalent risks. To alleviate this danger, NTP includes authentication techniques that enable time servers and clients to confirm each other's identities and secure the integrity of time synchronization data. NTP can build a trusted communication channel by integrating authentication which is critical to NTP security. NTP supports a number of authentication methods, including symmetric key encryption and public-key cryptography. These procedures entail digitally authenticating NTP packets with cryptographic algorithms, ensuring that the time information received comes from reliable sources. Clients can have confidence in the accuracy and integrity of the time data they receive by checking the validity of time server responses.

DoS (Denial-of-Service) attacks are another serious danger to NTP. These attacks try to interrupt or overload the time server, leaving it inaccessible or unresponsive. This risk is addressed by NTP by providing rate restriction methods and access control lists. The number of requests that may be processed from a single IP address or network is limited by rate limiting, and access control lists establish the rules and permissions for contacting the NTP server. NTPsec is an alternative NTP implementation that focuses on security and bug fixes. It is intended to fix flaws in the original NTP implementation while also improving overall security. Organizations can benefit from a solution that prioritizes security and integrates additional capabilities to improve the resilience and integrity of time synchronization by adopting NTPsec.

Another key part of NTP security is cryptography. It aids in the security of communication channels and the integrity of data during transmission. NTP hashes or signs NTP packets using encryption algorithms such as the Message Digest Algorithm (MD5) or the Secure Hash Algorithm (SHA). NTP uses encryption to protect against tampering or illegal change of time synchronization data, improving the protocol's overall security.

SNTP (Simple Network Time Protocol)

SNTP (Simple Network Time Protocol) is a lightweight and simpler variant of NTP (Network Time Protocol) used to synchronize the time of computers and networked devices. SNTP concentrates on providing a straightforward and uncomplicated approach to time synchronization, making it easier to implement and configure. SNTP lacks some of the additional capabilities present in NTP, such as authentication, precision timekeeping, and intricate algorithms for dealing with clock drift and network latency but still accomplishes the basic goal of aligning clocks across a network.

One of SNTP's main aspects is its simplicity. When compared to NTP, it takes less implementation and administrative effort, giving it a more accessible solution for environments with fewer resources or simpler network configurations. SNTP is frequently used in cases where the primary requirement is for devices to be reasonably synced without the need for additional functionality or lengthy configuration. This protocol may not be appropriate for applications or systems that require high accuracy and precise time synchronization, such as financial transactions, scientific investigations, or distributed systems with rigorous timing requirements.

Conclusions

The Network Time Protocol (NTP) is critical in modern life since it provides exact and accurate time synchronization for numerous applications and systems. NTP's significance stems from its ability to offer a standardized way for aligning device clocks to the Internet, assuring consistency and reliability across networks. The reliance on precise time synchronization extends to a wide range of applications, including cloud computing, the Internet of Things, blockchain, and cybersecurity.

NTP not only helps these technologies run smoothly, but it also increases their efficiency and efficacy. The importance of NTP is highlighted in the context of global interconnectedness and interdependence. With rising computer system complexity and reliance on networked infrastructure, exact time synchronization is more important than ever. NTP provides a foundation for keeping consistent time over geographically dispersed networks, allowing for seamless communication, data integrity, and device coordination. Furthermore, the use of the Universal Coordinated Time (UTC) standard by NTP ensures a universal reference point for time synchronization. NTP allows accurate comparisons and reliable coordination of time-sensitive processes by aligning devices with UTC. Moreover, NTP's hierarchical network design, clock synchronization mechanism, and security features like authentication and cryptography contribute to the protocol's general stability and resilience.

Bibliography

[1] https://ieeexplore.ieee.org/document/103043
[2] https://sookocheff.com/post/time/how-does-ntp-work/
[3] https://www.galsys.co.uk/news/what-is-ntp-a-beginners-guide-to-network-time-protocol/
[4] https://study-ccna.com/ntp-network-time-protocol/