Network Services 1

2019-2020

Licenciatura em Engenharia Informática

Ramo de Redes e Administração de Sistemas

NTP – Network Time Protocol

School Year 2019-2020

Time

- Time is the interval between two events, or the time indicated by a clock.
- The unit of the International System of Units that measures time is the **second**.
- Historically, the second was measured based on the average solar day (1/86400 of the day), but the rotation of the Earth is rather inaccurate implied error in the measure of unity.
- In 1954, the second was defined based on the rotation of the Earth around the Sun (1 / 31.556.925,9747 of the time that caused the Earth to rotate around the Sun from 12.00 on 04/01/1900). However, the rotation of the Earth around the Sun is also imprecise.
- Thus since 1967, the second is defined based on the measurement of atomic clocks, such as:
  - "***The second is the duration of 9,192,631,770 periods of radiation corresponding to the transition between two hyperfine levels of the ground state of the cesium 133***."

Time

- A basic and at the same time important feature of time is that it always advances.
- Time does not stop and not back.
- As several computer programs use this feature, their operation may be compromised if the machine clock unexpectedly indicates a wrong time.
- It can still be trickier on the Internet, with multiple computers exchanging information. Imagine the confusion that arose if each machine had different hours.

Need

- Why do we need to have machines with the same time?
  - Temporary security marks to associate in documents and their digital signature
  - Proof of delivery of documentation (time stamp)
  - Security protocols
  - Security analysis (logs)
  - Authentication
  - Purchase and sale of shares
  - Air control
  - Intrusion detection
  - Conference call
  - Online games
  - Encryption
  - ...

Time

- Another good definition for the need is given by Thomas Akin, in chapter 10 of his book “Hardening Cisco Routers”:

Time is inherently important to the function of routers and networks. It provides the only frame of reference between all devices on the network. ***This makes synchronized time extremely important****. Without synchronized time, accurately correlating information between devices becomes difficult, if not impossible. When it comes to security, if you cannot successfully compare logs between each of your routers and all your network servers, you will find it very hard to develop a reliable picture of an incident. Finally, even if you are able to put the pieces together, unsynchronized times, especially between log files, may give an attacker with a good attorney enough wiggle room to escape prosecution.*

Network Time Protocol (NTP)

- NTP is a protocol for clock synchronization of a set of computers on UDP protocol-based variable latency data networks for clock synchronization.
- NTP allows you to keep a computer's clock with the time always right and with great accuracy.
- Originally devised by David L. Mills of the University of Delaware, it is still maintained today by him and a team of volunteers.
- It was first used in 1979, and is still very popular today, being one of the oldest protocols used on the internet.

Fonte:
https://en.wikipedia.org/wiki/File:DL_Mills-2.jpg

Network Time Protocol (NTP)

- NTP servers allow their clients to synchronize the clocks of network equipment from a world-standard time-standard known as **UTC (Universal Time Coordinated**).
- The protocol has had several updates and changes over time:
  - 1979 - NTP V0 - RFC-958
  - 1998 - NTP v3 - RFC-1305

Network Time Protocol (NTP)

- The current version, NTPv4, consists of the implementation of the following RFCs:
  - RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification
  - RFC 5906: Network Time Protocol Version 4: Autokey Specification
  - RFC 5907: Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)
  - RFC 5908: Network Time Protocol (NTP) Server Option for DHCPv6
- The task is supported by a hierarchy of servers in the same way as other services on the Internet (remember for example the DNS service).
- Algorithms are used to minimize problems caused by connection failures, server failure, or service attacks.

Network Time Protocol (NTP)

- There are more simplified implementations of NTP but that imply less precision.
  - **Simple Network Time Protocol (SNTP)** - RFC 4330 - is a less complex implementation of NTP that does not require state storage for long periods of time. It is used in some embedded systems and in applications where the full functionality of NTP is not required.
  - **Windows time** - since the Windows 2000 version, Microsoft operating systems include the time service (W32Time), which has the ability to synchronize the computer's clock with an NTP server.
  - **Ntimed** - started being implemented by Poul-Henning Kamp in 2014. It is sponsored by the Linux Foundation to replace the original version of NTP and aims to be simpler and more secure than the original.
  - **Openntpd** - In 2004, Henning Brauer introduced OpenNTPD, an implementation with a greater focus on the generic needs of OpenBSD. It also includes some improvements in the security of the protocol and continue to be compatible with existing NTP servers. The version is available in several Linux package repositories.

Network Time Protocol (NTP)

- The NTP is not based on the principle of synchronizing machines with each other, but rather based on the principles of having all machines get as close as possible to the correct time - UTC.
- It is the responsibility of the operating system and not the NTP time zone management.
- Individual clients run a small program that queries the server periodically to obtain the reference time.
- These procedures are performed at defined time intervals in order to maintain the synchronization accuracy required for the network.
- Server queries are performed:
  - Initially every 64s.
  - In regime, every 15 min.

Modes of operation

- The implementation of NTP based on the following types of actors:
  - **Primary Server**
    - Server directly synchronized with a reference clock source UTC, accurate, based on atomic clocks, GPS, Galileo, ...
  - **Secondary server**
    - Intermediate server that synchronizes your clock from one or more servers.
    - It has one or more clients: servers or end customers.
  - **Client**
    - Synchronize your clock from one or more servers.
    - Does not provide the service to other client equipment.
  - Servers to be used by the client can be explicitly configured or discovered dynamically through broadcast packets.

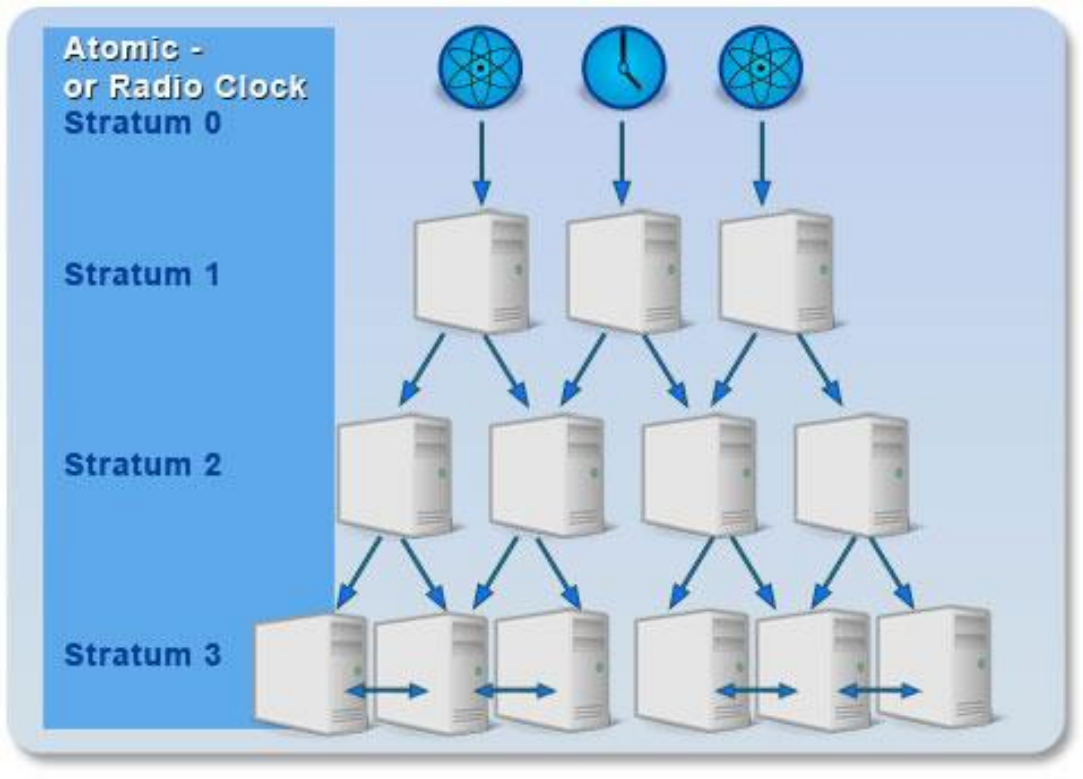
Layered Organization

- NTP servers form a hierarchical topology, divided into layers or layers numbered from 0 (zero) to 16 (sixteen).
- Layer 0 (stratum 0) is not actually part of the NTP server network, but represents the primary time reference, which is usually a Global Positioning System (GPS) receiver or an atomic clock. Stratum 16 indicates that a particular server is down.
- Stratum 0
- Reference Watches (atomic clocks, GPS, Galileo, ...)
  - Stratum 1
  - Primary Servers
  - Stratum 2 .. N
  - Secondary Servers
- The stratum value is calculated based on the number of hops desde a raiz.

Layered Organization

- Any NTP server that has as a time reference a stratum 1 server becomes a stratum 2, any NTP server that has as a time reference a stratum 2 server becomes a stratum 3, and so on.
- The higher the stratum, the greater the probability of the clock error.
- The increase in error between stratum is not very significant.
  - It is better to be connected correctly to stratum 2 than to stratum 1.
- From the point of view of network administration, the use of NTP is very advantageous, since it allows the automatic synchronization of all the equipment connected to the network. That is, the administrator does not have to go from machine to machine to hit the local clock.

Layered Organization



Fonte - https://www.meinberg.co.uk/support/information/ntp-the-network-time-protocol.htm

Structure

List of Stratum servers 1

http://support.ntp.org/bin/view/Servers/StratumOneTimeServers

List of Stratum servers 2

http://support.ntp.org/bin/view/Servers/StratumTwoTimeServers

Protocol

- The relationships between the different NTP devices are usually called associations. These can be:
  - **Permanent**: they are created by a configuration or command and are always maintained.
  - **Prioritized:** They are specific to version 4 of NTP and are created by a configuration or command, and can be undone in case there is a better server, or after a certain time.
  - **Ephemeral or transient:** they are created by request of another NTP device and can be undone in case of error or after a certain time.

Sync Modes

- **Client / server mode**
  - It is a permanent association and the most common form of configuration.
  - A device plays the role of a client, requesting weather information from a server. The client is aware of the associations with the servers and the status of the packet exchange.
  - Another device acts as a server, responding to the customer's request with information about the weather. The server does not store information about the dialogue with the client or about its association with the client.
  - In the process, the client sends a packet to the server and waits for the response. This can also be described as a pull operation, saying that the client fetches the necessary data about the time on the server.
  - A client can create associations with several servers simultaneously (in fact it is recommended that this is the case), and a server can provide time to several clients simultaneously.
  - An NTP (host) device can be both client and server at the same time.

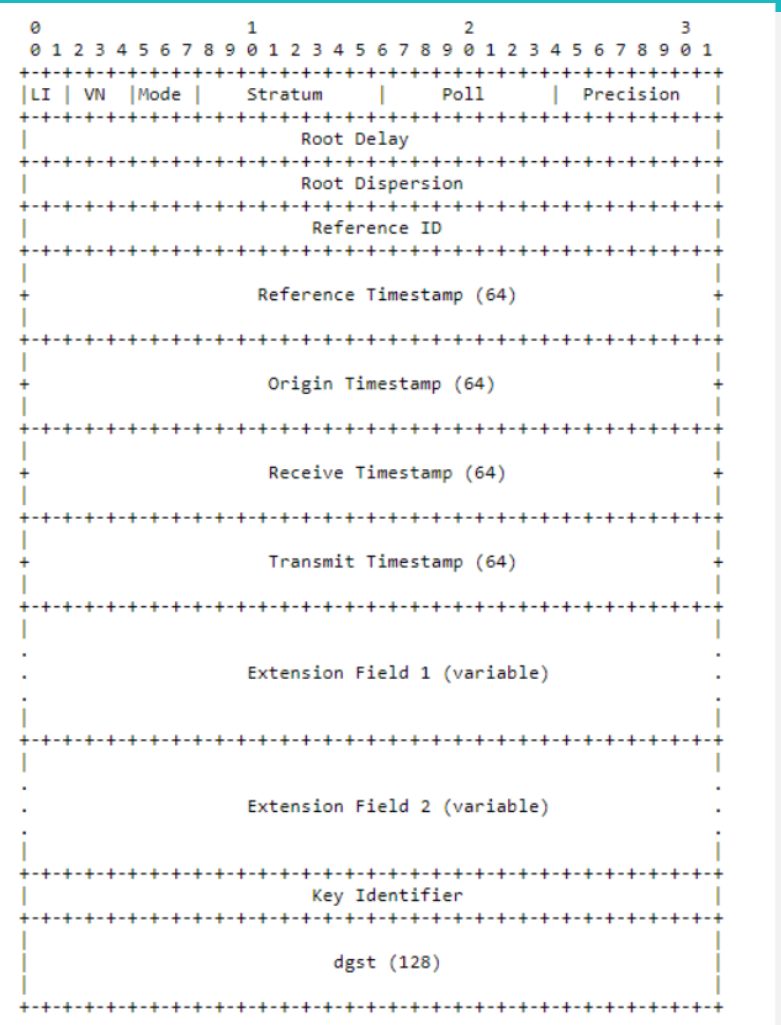
Sync Modes

- **"Symmetric" mode**
  - Two or more NTP devices can be configured as peers, so that they can both search for time and provide it, ensuring mutual redundancy.
  - This configuration makes sense for devices on the same stratum, which are also configured as clients for one or more servers. If one of the pairs loses the reference of their servers, the other pairs can function as a time reference.
  - The symmetrical mode can be:
    - **Active**: Device A configures device B as its peer (thereby creating a permanent association). In turn, device B also configures device A as its peer (it also creates a permanent association).
    - **Passive:** Device A configures device B as its pair (active symmetric mode). But device B does not have device A on its list of servers or peers. Still, when receiving a packet from A, device B creates a transient association, in order to be able to provide or receive the time from A. This mode is particularly susceptible to attacks, where an intruder device can be configured in active symmetric mode and provide false weather information to another. So it should always be used with encryption.

Sync Modes

- **Broadcast mode**
  - NTP can make use of broadcast or multicast packets to send or receive time information.
  - This type of configuration can be advantageous in the case of local networks with few servers, thus feeding a large number of clients.
  - Upon receiving the first packet from a server, the NTP client searches for data for a short period of time, as if it were in client - server mode, in order to know the delay involved. That is, for a few moments there is an exchange of packets between client and server, after that the client only starts to receive broadcast or multicast packets sent to the network by the server.
  - As in the case of passive symmetric mode, there is also a security issue here, because an intruder can easily send fake NTP packets in broadcast mode. So authentication must always be enabled..

Protocol


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
LI | VN | Mode | Stratum | Poll | Precision
Root Delay
Root Dispersion
Reference ID
Reference Timestamp (64)
Origin Timestamp (64)
Receive Timestamp (64)
Transmit Timestamp (64)
Extension Field 1 (variable)
Extension Field 2 (variable)
Key Identifier
dgst (128)

Header

- LI – Jump indicator 2 bits

Value	Meaning
0	no warning
1	last minute of the day has 61 seconds
2	last minute of the day has 59 seconds
3	unknown (clock unsynchronized)

- VN – Version – 3 bits
  - Now are the version 4

- Mode – Mode – 3 bits
  - Modes of association between systems

Value	Meaning
0	reserved
1	symmetric active
2	symmetric passive
3	client
4	server
5	broadcast
6	NTP control message
7	reserved for private use

Header

- Strat - Stratum Number – 8 bits

Value	Meaning
0	unspecified or invalid
1	primary server (e.g., equipped with a GPS receiver)
2-15	secondary server (via NTP)
16	unsynchronized
17-255	reserved

- Poll – 8 bits
  - Maximum interval between messages in Log2 (seconds)
    - Usually values between 4 (16s) and 17 (36h)
  - Prec - 8 bits
  - Clock accuracy in Log2 (seconds)
    - -18 => 1 ms

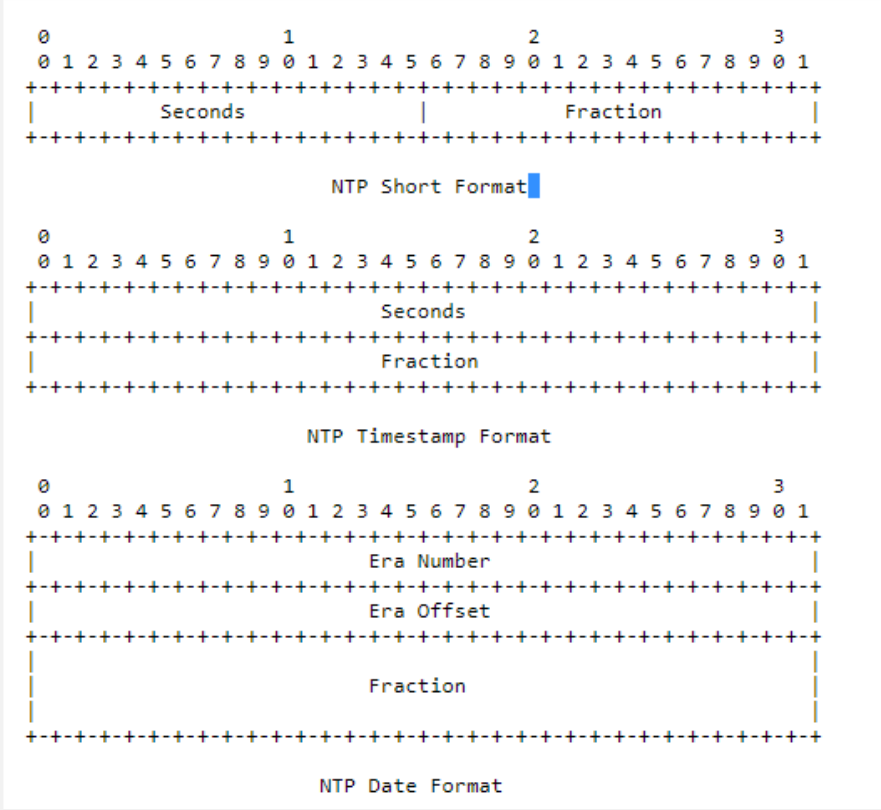
Header

- Root Delay 32 bits
  - Round-trip delay for the reference clock
  - They are updated / accumulated as the stratum increases
- Root Dispersion – 32 bits
  - "Scatter" (error) for the reference clock
  - They are updated / accumulated as the stratum increases
- Reference ID – 32 bits
  - Server identifier or reference clock
  - For stratum 0:

ID	Clock Source
GOES	Geosynchronous Orbit Environment Satellite
GPS	Global Position System
GAL	Galileo Positioning System
PPS	Generic pulse-per-second
IRIG	Inter-Range Instrumentation Group
WWVB	LF Radio WWVB Ft. Collins, CO 60 kHz
DCF	LF Radio DCF77 Mainflingen, DE 77.5 kHz
HBG	LF Radio HBG Prangins, HB 75 kHz
MSF	LF Radio MSF Anthorn, UK 60 kHz
JJY	LF Radio JJY Fukushima, JP 40 kHz, Saga, JP 60 kHz
LORC	MF Radio LORAN C station, 100 kHz
TDF	MF Radio Allouis, FR 162 kHz
CHU	HF Radio CHU Ottawa, Ontario
WWV	HF Radio WWV Ft. Collins, CO
WWVH	HF Radio WWVH Kauai, HI
NIST	NIST telephone modem
ACTS	NIST telephone modem
USNO	USNO telephone modem
PTB	European telephone modem

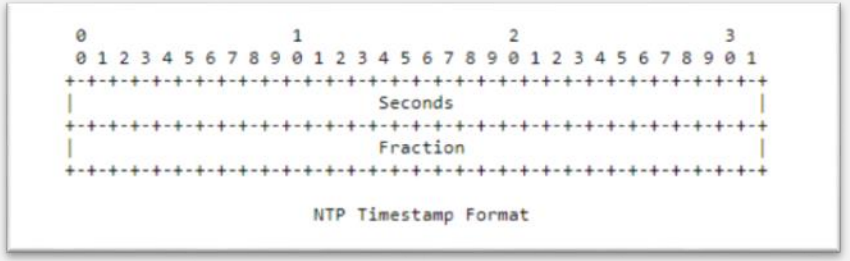
Tipo de Dados

- The 128-bit date format is used where word storage and size are sufficient and available.
- It includes a 64-bit signed second field spanning 584 billion years and a 64-bit fraction field, resolving 0.05 attoseconds (ie, 0.5e-18).



Timestamps

- 64 bits are used to represent a time stamp (date / time)
  - 32 bits represent seconds
    - Supports 136 year intervals
    - To support the representation of more years is used the concept of Era
  - 32 bits represent fractions of a second with a resolution of 232 picoseconds



Timestamps

- To convert the system time into any NTP format, the number of seconds (s) from the zero season (00:00 01-01-1900) to the current system time must be calculated.
- To determine the era and the timestamp given the s, you must do:

era = s / 2^(32) e **timestamp = s - era * 2^(32)**

- To determine the s knowing the era and timestamp you must do:

s = era * 2^(32) + timestamp

Date	MJD	NTP Era	NTP Timestamp Era Offset	Epoch
1 Jan -4712	-2,400,001	-49	1,795,583,104	1st day Julian
1 Jan -1	-679,306	-14	139,775,744	2 BCE
1 Jan 0	-678,491	-14	171,311,744	1 BCE
1 Jan 1	-678,575	-14	202,939,144	1 CE
4 Oct 1582	-100,851	-3	2,873,647,488	Last day Julian
15 Oct 1582	-100,840	-3	2,874,597,888	First day Gregorian
31 Dec 1899	15019	-1	4,294,880,896	Last day NTP Era -1
1 Jan 1900	15020	0	0	First day NTP Era 0
1 Jan 1970	40,587	0	2,208,988,800	First day UNIX
1 Jan 1972	41,317	0	2,272,060,800	First day UTC
31 Dec 1999	51,543	0	3,155,587,200	Last day 20th Century
8 Feb 2036	64,731	1	63,104	First day NTP Era 1

Header

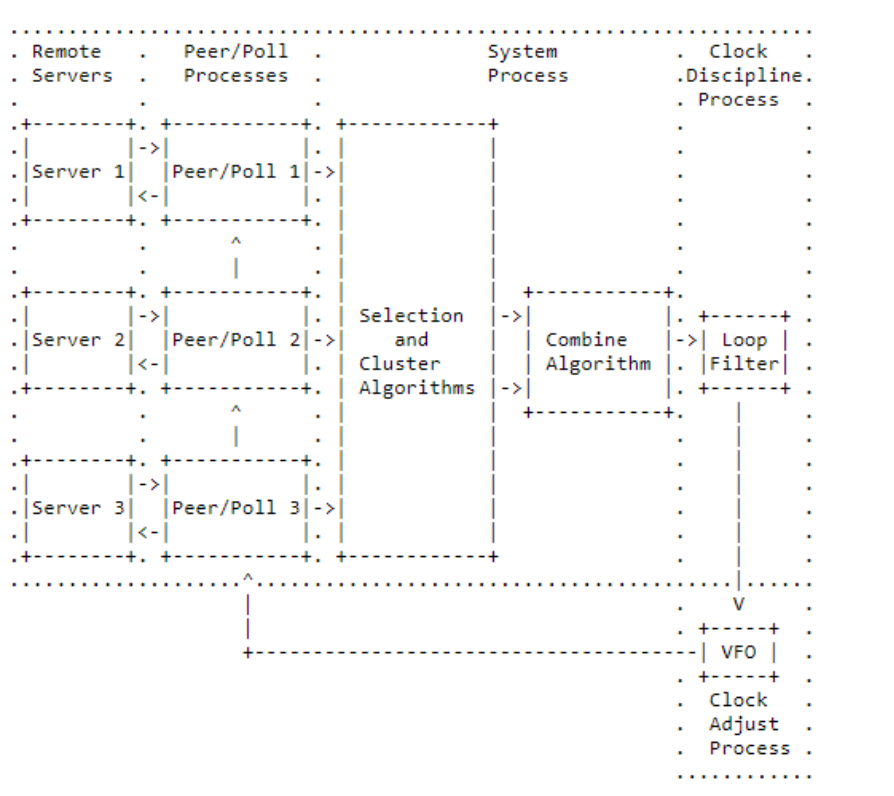
- **Reference Timestamp - 64 bits**
  - Time when the system clock was last set or corrected, in the NTP timestamp format.
- **Origin Timestamp - 64 bits**
  - Time on the client when the request left for the server, in NTP timestamp format.
- **Receive Timestamp - 64 bits**
  - Time on the server when the request arrived from the client, in NTP timestamp format.
- **Transmit Timestamp - 64 bits**
  - Time on the server when the response was sent to the client, in NTP timestamp format.
- **Destination Timestamp - 64 bits**
  - Time on the client when the response arrived from the server, in NTP timestamp format.

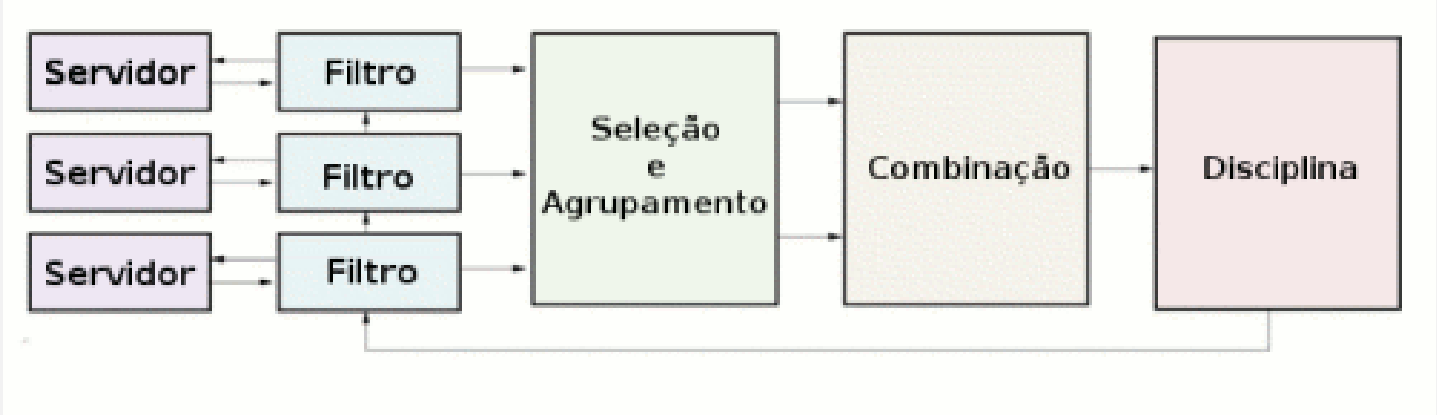
Global Parameters

- RFC 5905 defines the following global parameters for NTP version 4:

Name	Value	Description
PORT	123	NTP port number
VERSION	4	NTP version number
TOLERANCE	15e-6	frequency tolerance PHI (s/s)
MINPOLL	4	minimum poll exponent (16 s)
MAXPOLL	17	maximum poll exponent (36 h)
MAXDISP	16	maximum dispersion (16 s)
MINDISP	.005	minimum dispersion increment (s)
MAXDIST	1	distance threshold (1 s)
MAXSTRAT	16	maximum stratum number

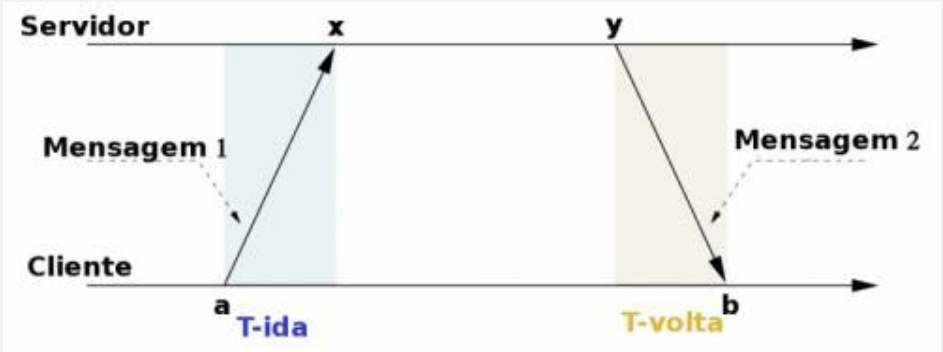
Operation


Remote Servers
Peer/Poll Processes
System Process
Clock Discipline Process
Server 1
Peer/Poll 1
Server 2
Peer/Poll 2
Server 3
Peer/Poll 3
Selection and Cluster Algorithms
Combine Algorithm
Loop Filter
VFO
Clock Adjust Process


Servidor
Servidor
Servidor
Filtro
Filtro
Filtro
Seleção e Agrupamento
Combinação
Disciplina

Remote Server

- Consider server and client with unsynchronized clocks. The exchange of messages is as follows:
  - The Customer reads his watch, which provides the time A.
  - The Client sends Message 1 with the time information to the server.
  - The Server receives Message 1 and in that instant reads its clock, which provides instant X. The server holds a and X in variables.
  - The Server after some time reads again its clock, which provides the instant Y.
  - The server sends Message 2 with a, X, and y to the client.
  - The Client receives Message 2 and in that instant reads his clock, which provides instant B.



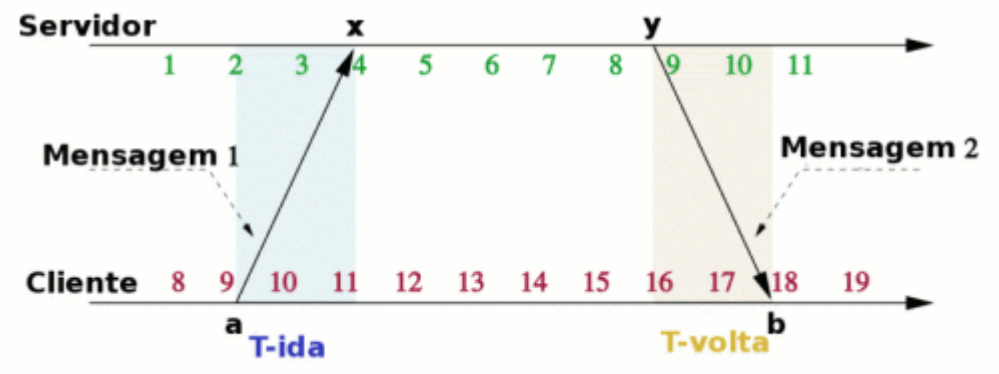
Remote Server

- Upon receiving Message 2, the Customer begins to know the instants a, x, y and b. But a and b are on a time scale, while x and y on another. The increment value of these scales is the same, but the clocks are not synchronized.
- It is not possible, then, to calculate the time that Message 1 took to be transmitted (T-go), nor the time that Message 2 spent in the network (T-turn). However, the total round trip time, or delay (also known as Round Trip Time or RTT) which is the sum T-go + T-turn can be calculated as:
- **delay = (b-a)-(y-x).**
- Considering that the outgoing time is equal to the lap time, it is possible to calculate the displacement between the server and the local clock as:
- **offset = x - (a + delay/2) =**
  offset = (x-a+y-b)/2.

Remote Server

- The Client reads the clock: a = 9.
- The Customer sends Message 1 (a = 9).
- The Server receives Message 1 (a = 9) and reads its clock: x = 4.
- The server some time later reads your clock again: y = 9.
- The Server sends Message 2 (a = 9, x = 4, y = 9).
- Customer receives Message 2 (a = 9, x = 4, y = 9) and reads his / her clock: b = 18.

Remote Server



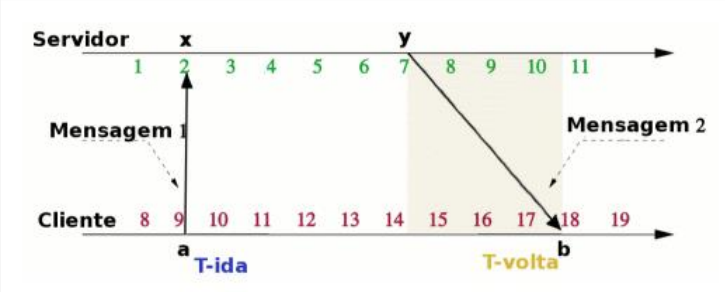
- It is easy to see that $T_{go} = 2$ and $T_{turn} = 2$. However, neither the Client nor the Server has this view. The server at the end of the message exchange discards all information about it. The customer knows the variables a = 9, x = 4, y = 9 and b = 18, but from them it is impossible to calculate T_{go} or T_{turn} . However, it is possible to calculate the delay and displacement:
- **delay = (b-a)-(y-x) = (18-9)-(9-4) = 9 - 5 = 4.**

  offset = (x-a+y-b)/2 = (4-9+9-18)/2 = -14/2 = -7.
- A shift of -7 means that the client's local clock must be delayed by 7 units of time to match that of the Server.

Remote Server

- In the previous example, we consider that T_{go} is equal to T_{turn}
- But this is not always true! There are random delays in the networks due to the queues of routers and switches. In a WAN or on the Internet, connections at different speeds and asymmetric routes, traffic and other factors, also cause differences between these two times.
- However, NTP works exactly that way, always considering that T_{go} is equal to T_{turn}
- And that implies an error ...

Remote Server



delay = (b-a) - (y-x) = (18-9) - (7-2) = 9 - 5 = 4.

displacement = (x-a + y-b) / 2 = (2-9 + 7-18) / 2 = -18/2 = -9.

The offset is wrong! The correct value is known to be -7., However the calculated value is -9. This is due to the error introduced by the network and which implies that T_{go} and T_{turn} are not the same.

However, from the calculation of displacement and delay, and taking into account the limitation of the method, which considers $T_{go} = T_{turn}$, it is known that the true displacement is between:

displacement - delay / 2 <= true displacement <= displacement + delay / 2

-9 -2 <= true offset <= -9 + 2

-11 <= true offset <= -7

That is, given a displacement of -9 and a delay of 4, it is known that the true value of the displacement is somewhere between -11 and -7, but there is no way to be sure what the value is.

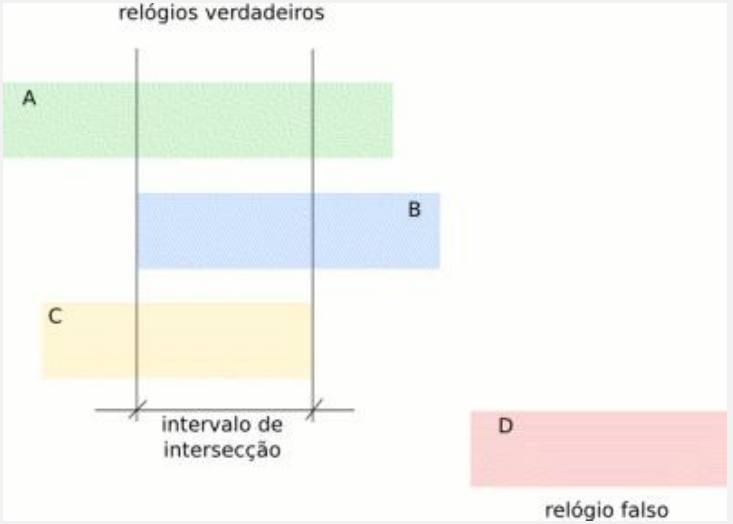
Peer/Poll

- Through the exchange of messages, NTP obtains the delay and displacement information from a server. This exchange of messages is not carried out only once, but is repeated periodically, in a time interval controlled by the protocol.
- At the start of synchronization, the NTP client queries each server every 64s. This period varies over time, usually increasing, until it reaches 1024s.
- In reality, each sample is composed of 4 values: delay, displacement, dispersion and timestamp. The timestamp indicates when the sample arrived and the dispersion is the estimated error of the remote server clock, reported by the server in the NTP message.
- The list of values is ordered according to the delay. Considering that the samples with less delay are better because they probably were not subject to queues in the telecommunications equipment and thus are closer to ensuring that Tida is equal to Tvolta
- The oldest values are discarded, because the displacement value may no longer correspond to reality, as the accuracy of the local clock varies over time and network conditions.
- After discarding the old samples, a list with the most recent samples and ordered according to the delay remains. From the first entry in this list, the delay and displacement for the client-server pair are removed (note that for each client-server pair there is a variable of each type).

Selection and Cluster

- After calculating the main parameters for each server in the previous phase, it is now important to find out which ones are reliable and which are not.
- Servers that have an error in the given time are called **fake clocks**.
- Servers that provide the time correctly are called **real clocks**.
- For the selection of clocks, the NTP considers as true the displacement that is within a certain confidence interval, calculated as:

confidence interval = (displacement / 2) + dispersion.

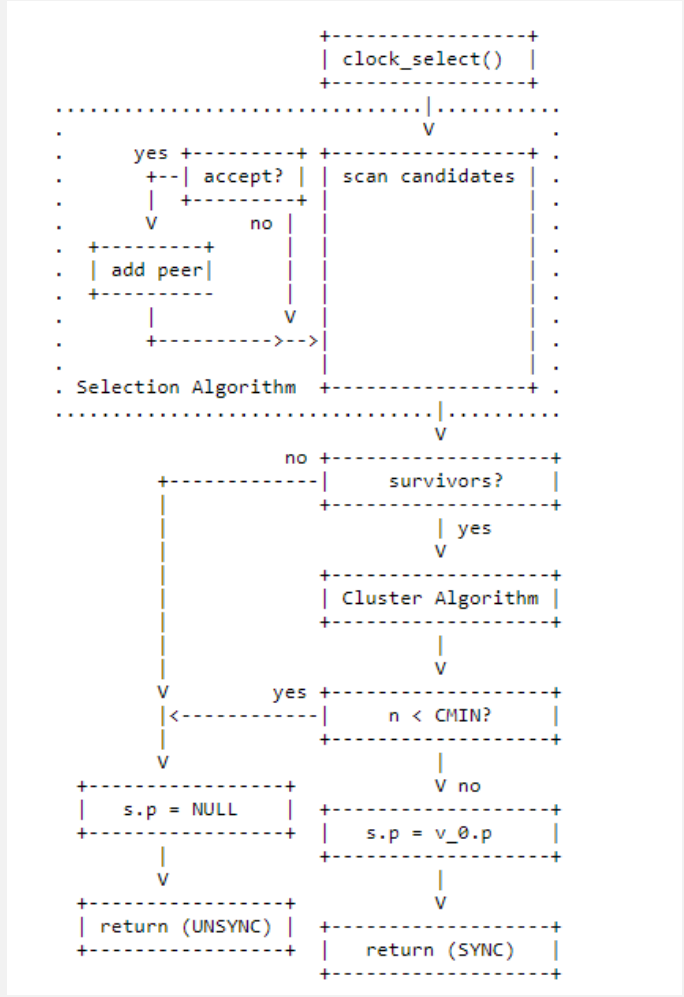


Selection and Cluster

- After real watches have been chosen, statistical techniques are used in order to select the best ones.
- The selection criteria used are:
  - Stratum.
  - distance to the root.
  - variation (jitter).
- In the process, some servers are discarded and are called remote clocks.
- Those that remain are called surviving clocks.
- The best of the surviving clocks is considered to be a system peer.

Combine

- If the system peer is determined by the algorithm of the previous phase, it does not enter this step anymore.
- For the other cases in which there is more than one survivor and none of them have been configured as a system peer, a weighted average of the displacements of the clocks is calculated in order to increase the accuracy.



Discipline

- The process controls the phase and frequency of the system clock.
- Phase-based control is best for occasions where there is a wide range (jitter). This approach seeks to minimize the error in time, indirectly controlling the frequency.
- Frequency-based control is best for when there are frequency instabilities. The approach directly controls the frequency, and indirectly the error in time.
- NTP continuously monitors the local clock, even in periods when it is not possible to consult time servers.
- Like this:
  - Time jumps are avoided whenever possible. The time is adjusted gradually with the variation of the clock's local frequency.
  - If the difference is greater than 128ms, the NTP will only set the clock if it persists for a period longer than 900s (15min).
  - If the difference is greater than 1000s (~ 16.7min) the algorithm aborts its execution, considering that something very wrong has happened. Differences of that order or greater must be corrected manually before running the NTP query again.

Security

- In any telecommunications service we must guarantee the following aspects with regard to information:
  - integrity,
  - availability,
  - authenticity;
  - confidentiality.
- The previously seen algorithms, combined with the correct system configuration, with a sufficient number of time sources with independent primary references, satisfactorily guarantee the integrity and availability of the service.
- The encryption algorithms aim to guarantee the authenticity of the information. That is, they aim to assure the client that the server is who he claims to be.
- Confidentiality is not considered a problem in the context of NTP. That is, the weather information will "walk" on the network in an open way.
- The main reasons for NTP to work this way are:
  - time is public information, there is no reason to hide it;
  - encrypting the information would introduce complexity and processing time on both the server and the client which would degrade system performance, making it less accurate.

Security

- There are basically two methods in NTP to perform authentication:
  - symmetric key
  - public key (autokey).
- Symmetric key authentication is the schema originally used in version 3 of NTP, but maintained from version 4.
- A set of keys must be generated and shared by the server and the client. NTP does not provide means for secure transmission or storage of keys; this should be done with other resources.
- Symmetric keys can be used to:
  - authenticate servers or peers in active symmetric mode;
  - authenticate pairs in passive symmetric mode or broadcast or multicast servers;
  - authenticate requests from monitoring and control programs

Security

- **Public Key Authentication (Autokey)**
  - In version 4 of the NTP is supported a new form of authentication, based on public keys and a protocol that was called autokey.
  - The integrity of the packets is verified through MD5 keys and the authenticity of the time sources is ascertained through digital signatures and various authentication schemes.
  - Identity schemes based on challenge / response type exchanges are used to avoid various types of attacks to which the symmetric key method is potentially vulnerable.
  - Authentication is based on security groups. A security group can be understood as a set of NTP servers and clients that share the same authentication methods, having at its root one or more servers that are trusted and administered by the same entity. A group does not necessarily need to have tier 1 servers at its root, but can be a client of other security groups.

Questions

References

- http://www.ntp.org/ - acedido em maio de 2020
- http://pt.wikipedia.org/wiki/Network_Time_Protocol - acedido em maio de 2020
- http://oal.ul.pt/hora-legal/- acedido em maio de 2020
- https://ntp.br/ntp.php - acedido em maio de 2020
- https://tools.ietf.org/html/rfc5905 - acedido em maio de 2020
- http://www.eecis.udel.edu/~mills/ntp/html/index.html - - acedido em maio de 2020
- http://www.endruntechnologies.com/pdf/NTP-Intro.pdf - acedido em maio de 2020