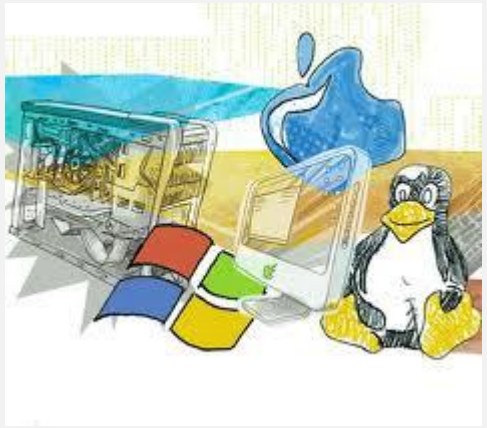
Serviços de Rede 1

2019-2020

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



Serviços de Rede 1

NTP – Network Time Protocol

O Tempo

- O tempo é o intervalo entre dois eventos, ou o momento indicado por um relógio.
- A unidade do Sistema Internacional de Unidades que mede o tempo é o **segundo**.
- Historicamente, o segundo era medido com base no dia solar médio (1/86400 do dia), mas a rotação da Terra é bastante imprecisa implicado erro na medida da unidade.
- Em 1954, definiu-se o segundo com base na rotação da Terra em torno do Sol (1/31.556.925,9747 do tempo que levou a Terra a girar em torno do Sol à partir das 12h de 04/01/1900). Contudo, a rotação da Terra em torno do Sol também é imprecisa.
- Assim desde 1967, o segundo é definido com base na medição de relógios atômicos, como:

  "***O segundo é a duração de 9.192.631.770 períodos da radiação correspondente à transição entre dois níveis hiperfinos do estado fundamental do átomo de césio 133***."

Tempo

- Uma característica básica e ao mesmo tempo importante do tempo é que ele avança sempre.
- O tempo não para e não volta para trás.
- Como vários programas de computador fazem uso dessa característica, o seu funcionamento pode estar comprometido se o relógio da maquina inesperadamente passar a indicar uma hora errada.
- Ainda pode ser mais complicado na Internet, com vários computadores a trocar informação. Imagine a confusão que se gerava se cada uma das maquina tivesse horas diferentes.

Necessidade

- Porque temos necessidade de as máquinas terem o mesmo tempo?
  - Marcas temporais de segurança a associar em documentos e sua assinatura digital.
  - Comprovativo de entrega de documentação (*time stamp*).
  - Protocolos de segurança.
  - Analise de segurança (logs).
  - Autenticação.
  - Sistemas de marcação de eventos.
  - Controlo aéreo.
  - Detecções de intrusão.
  - Teleconferência e Videoconferência.
  - Jogos online.
  - Criptografia.
  - …

Necessidade

- Outra boa definição para a necessidade é dada por Thomas Akin, no capitulo 10 do seu livro *"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)

- O NTP é um protocolo para sincronização do relógio de um conjunto de computadores em redes de dados com latência variável baseado no protocolo UDP para sincronização do relógio.
- O NTP permite manter o relógio de um computador com a hora sempre certa e com grande exatidão.
- Originalmente idealizado por David L. Mills da Universidade do Delaware é ainda hoje mantido por si e por uma equipa de voluntários.
- Foi utilizado pela primeira vez em 1979, sendo ainda hoje muito popular e é um dos mais antigos protocolos usados na internet.

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

Network Time Protocol (NTP)

- Os servidores NTP permitem aos seus clientes a sincronização dos relógios dos equipamentos de rede a partir de uma referência padrão de tempo aceita mundialmente, conhecida como UTC (**Universal Time Coordinated**).
- Foi tendo varias atualizações e alterações ao longo do tempo:
  - 1979 - NTP V0 - RFC-958
  - 1998 - NTP v3 - RFC-1305

Network Time Protocol (NTP)

A versão actual, NTPv4, consiste na implementação dos seguintes 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

- A tarefa é suportada por uma hierarquia de servidores de forma idêntica a outros serviços na Internet (recordar por exemplo o serviço DNS).
- São usados algoritmos para minimizar os problemas gerados com quebras de ligação, falha de servidores ou ataques ao serviço.

Network Time Protocol (NTP)

- Existem implementações mais simplificadas do NTP mas que implicam uma menor precisão.
  - **Simple Network Time Protocol** (**SNTP**) - RFC 4330 - é uma implementação menos complexa do NTP que não exige o armazenamento do estado durante longos períodos de tempo. É usado em alguns sistemas embutidos e em aplicações onde a total funcionalidade do NTP não é necessária.
  - **Hora do Windows –** desde a versão do Windows 2000 que os sistemas operativos da Microsoft incluem o serviço de tempo (W32Time), que tem a capacidade de sincronizar o relógio do computador com um servidor NTP.
  - **Ntimed** – começou por ser implantado por Poul-Henning Kamp em 2014. É patrocinado pela Fundação Linux para substituir a versão original do NTP e pretende ser mais simples e mais segura que a original.
  - **Openntpd** - Em 2004, Henning Brauer apresentou o OpenNTPD , uma implementação com um maior foco nas necessidades genéricas do OpenBSD. Inclui ainda algumas melhorias na segurança do protocolo e continuam a ser compatível com servidores NTP existentes. A versão está disponível em vários repositórios de pacotes do Linux.

Network Time Protocol (NTP)

- O NTP não se baseia no princípio de sincronização das máquinas entre si, mas sim com base nos princípios de ter todas as máquinas chegar tão perto quanto possível para a hora correta - UTC.
- A gestão dos fusos horários é da responsabilidade do sistema operativo e não do protocolo.
- Os clientes individuais correm um pequeno programa que consulta o servidor periodicamente para obter o tempo de referência (UTC).
- Estes procedimentos são realizados em intervalos de tempo definidos de modo a manter a precisão da sincronização requerida para a rede.
- As consultas aos servidores são realizadas:
  - Inicialmente a cada 64s.
  - Em regime, a cada 15 min.

Modos de operação

- A implementação do NTP baseada nos seguintes tipos de atores:
  - **Servidor primário**
    - Servidor directamente sincronizado com uma fonte de relógio de referência UTC, rigorosa, baseada em relógios atómicos, GPS, *Galileo*, …
  - **Servidor secundário**
    - Servidor intermediário que sincroniza o seu relógio a partir de um ou mais servidores.
    - Possui um ou mais clientes: servidores ou clientes finais.
  - **Cliente**
    - Efectua a sincronização do seu relógio a partir de um ou mais servidores.
    - Não fornece o serviço a outros equipamentos cliente.
    - Os servidores a utilizar pelo cliente podem ser configurados de forma explícita ou descobertos dinamicamente através da pacotes em *broadcast*.

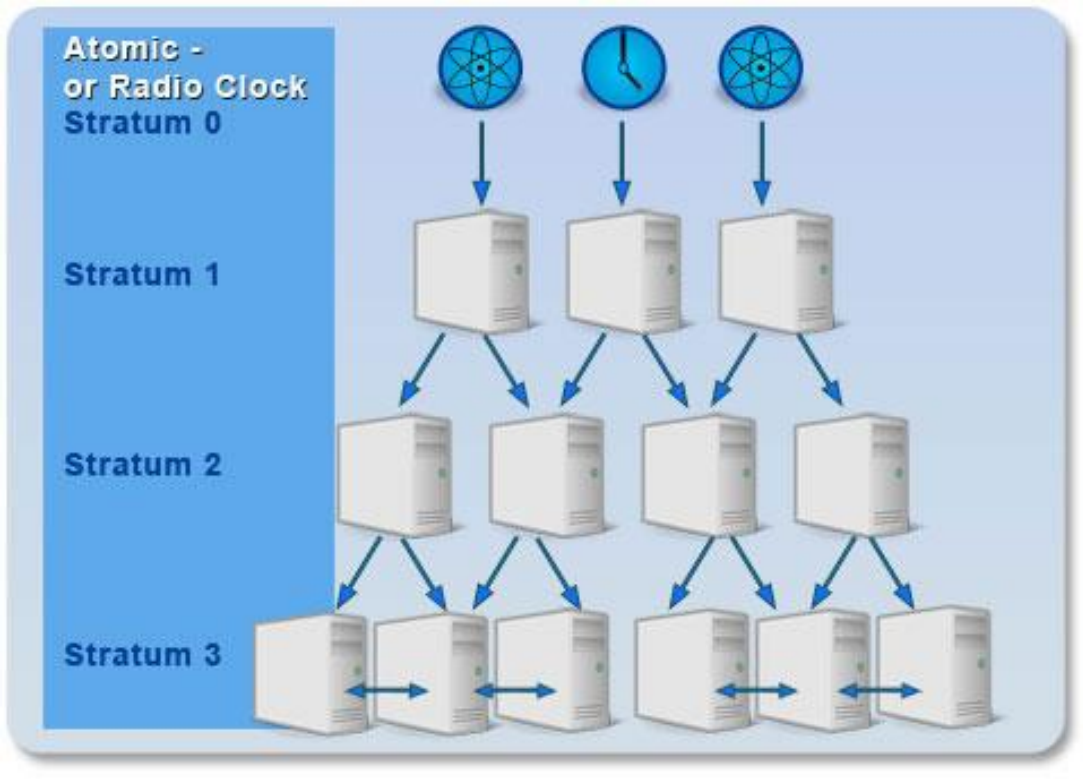
Organização em camadas

- Os servidores NTP formam uma topologia hierárquica, dividida em camadas ou *stratum* numerados de 0 (zero) a 16 (dezasseis).
- A camada 0 (*stratum 0*) na verdade não faz parte da rede de servidores NTP, mas representa a referência primária de tempo, que é geralmente um recetor do Sistema de Posicionamento Global (GPS) ou um relógio atômico. O estrato 16 indica que um determinado servidor está inoperante.
  - Stratum 0
    - Relógios de referência (relógios atómicos, GPS, Galileo, …)
  - Stratum 1
    - Servidores primários
  - Stratum 2 .. N
    - Servidores secundários
- O valor do *stratum* é calculado tendo por base o número de *hops* desde a raiz.

Organização em camadas

- Qualquer servidor NTP que tenha como referência de tempo um servidor *stratum* 1 passa a ser um *stratum* 2, qualquer servidor NTP que tenha como referência de tempo um servidor *stratum* 2 passa a ser um *stratum* 3, e assim por diante.
- Quanto mais elevado for o *stratum* maior será a probabilidade de erro do relógio.
- O aumento do erro entre *stratum* não é muito significativa.
  - É melhor estar ligado de forma correta ao *stratum* 2 do que mal a um *stratum* 1.
- Do ponto de vista da administração de redes, a utilização do NTP é muito vantajosa, pois possibilita a sincronização automática de todos os equipamentos ligados à rede. Ou seja, o administrador não precisa ir de máquina em máquina para acertar o relógio local.

Organização em camadas



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

Organização em camadas

Lista de servidores de *Stratum* 1

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

Lista de servidores de *Stratum* 2

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

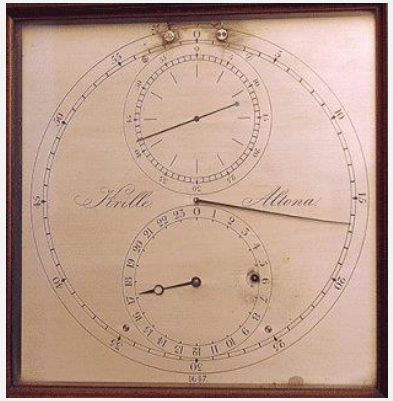
PL	Warsaw	e-utp.net	Europe	OpenAccess	Yes	2019-12-20T20:09:38Z
PL	Wegrzce, near Cracow; Poland		Poland	OpenAccess	No	2019-12-20T19:07:16Z
PT	Lisboa, Portugal	Observatório Astronómico de Lisboa	Portugal/Europe	OpenAccess	No	2006-02-12T16:30:42Z
PY	Asunción	COPACO S.A.	Paraguay	OpenAccess	No	2017-10-27T23:12:55Z
RO	BluePink Datacenter @ Constanta, Romania	BluePink	EU	OpenAccess	Yes	2014-09-28T13:24:15Z

Em Portugal

- O **Observatório Astronómico de Lisboa** (http://www.oal.ul.pt/) foi fundado no dia 11 de Março de 1861.
- Desenvolveu competências em trabalhos de Astrometria no séc. XIX e parte do séc. XX, que lhe granjearam fama internacional.
- O OAL é a instituição que tem a incumbência legal de manter e distribuir a Hora Legal em Portugal.
- OAL está equipado com diversos relógios atómicos que se mantêm sincronizados com a padrão mundial da hora UTC e possui diversos servidores que a disponibilizam segundo o protocolo NTP
- Atualmente, o OAL dirige a Comissão Permanente da Hora, desenvolve e apoia atividades de investigação científica em Astrofísica, de divulgação e formação, no estudo e preservação do excelente acervo patrimonial, além de manter um serviço público nas suas áreas de intervenção.

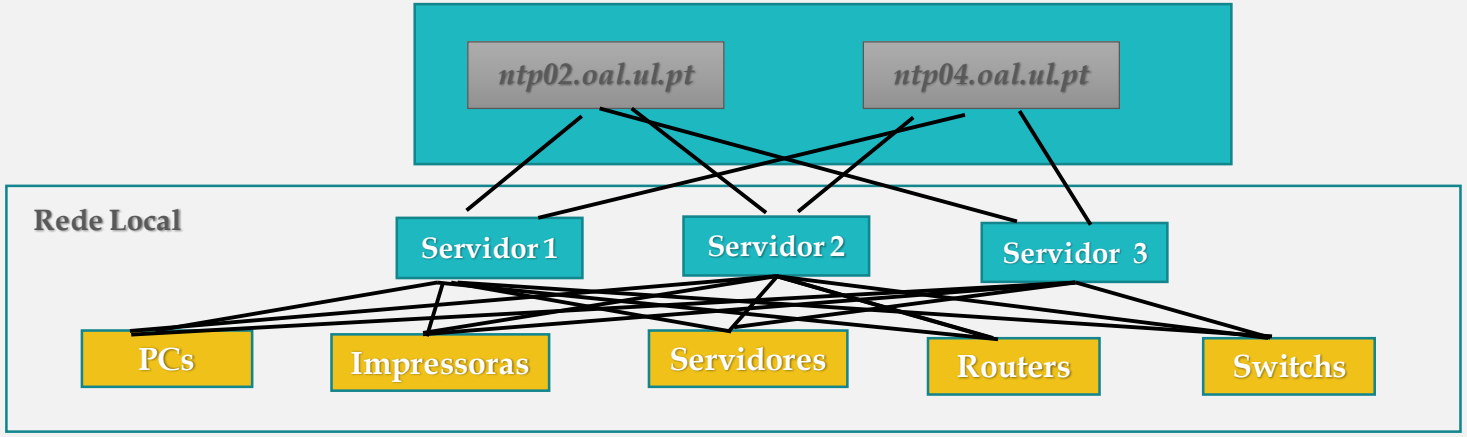
Em Portugal

- Os endereços dos servidores NTP do Observatório Astronómico de Lisboa que mantêm o UTC são:
  - ***ntp02.oal.ul.pt*** e ***ntp04.oal.ul.pt***.
- Pode em http://oal.ul.pt/hora-legal/hora-legal-oal/ver como ativar o surgimento da hora oficial num site e num cliente.



A minha topologia

- Se a sua rede for pequena pode configurar os seus equipamentos para se atualizarem diretamente num dos servidores NTP do Observatório Astronómico de Lisboa.
- Se a sua rede tiver alguma dimensão, deve ter 2 ou 3 servidores internos a proceder a sua atualização nos servidores externos e os seus clientes de rede a utiliza-los como os seus servidores NTP.



Protocolo - Relações

- As relações entre os diferentes dispositivos NTP são normalmente chamadas de associações. Estas podem ser:
  - **Permanentes:** são criadas por uma configuração ou comando e mantidas de forma permanente.
  - **Priorizáveis** : são específicas da versão 4 do NTP e são criadas por uma configuração ou comando, podendo ser desfeitas no caso de haver um servidor melhor, ou depois de um certo tempo.
  - **Efêmeras ou transitórias**: são criadas por solicitação de outro dispositivo NTP e podem ser desfeitas em caso de erro ou depois de um certo tempo.

Protocolo - Modos de Sincronismo

- Modo "***client/server***"
  - É uma associação permanente e a forma mais comum de configuração.
  - Um dispositivo faz o papel de cliente, solicitando informações sobre o tempo a um servidor. O cliente tem conhecimento das associações com os servidores e do estado da troca de pacotes.
  - Outro dispositivo faz o papel de servidor, respondendo à solicitação do cliente com informações sobre o tempo. O servidor não armazena informações sobre o diálogo com o cliente ou sobre sua associação com o mesmo.
  - No processo o cliente envia um pacote ao servidor e aguarda a resposta. Isso pode ser descrito também como uma operação do tipo pull, dizendo que o cliente busca os dados necessários sobre o tempo no servidor.
  - Um cliente pode criar associações com vários servidores simultaneamente (na verdade é recomendável que seja assim), e um servidor pode fornecer tempo simultaneamente a diversos clientes.
  - Um dispositivo (host) NTP pode ser cliente e servidor ao mesmo tempo.

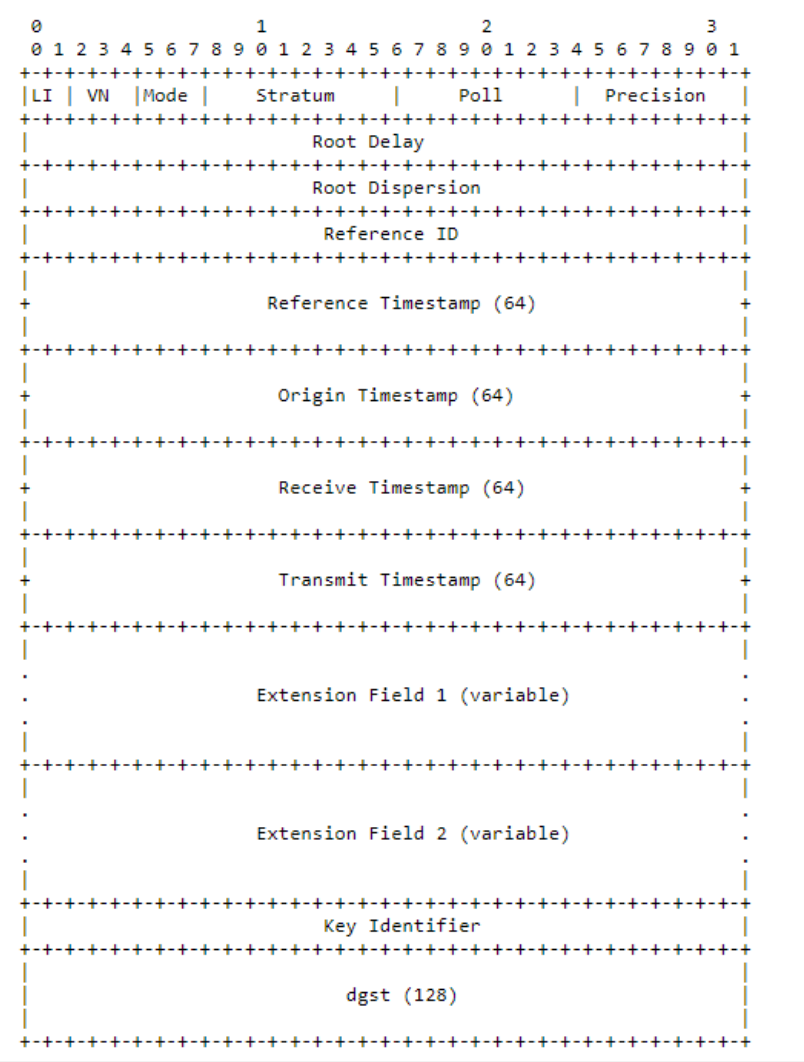
Protocolo - Modos de Sincronismo

- Modo "***symmetric***"
  - Dois ou mais dispositivos NTP podem ser configurados como pares (peers), de forma que possam tanto procurar o tempo, quanto fornecê-lo, garantindo redundância mútua.
  - Essa configuração faz sentido para dispositivos no mesmo *stratum*, configurados também como clientes de um ou mais servidores. Caso um dos pares perca a referência de seus servidores, os demais pares podem funcionar como referência de tempo.
  - O modo simétrico pode ser:
    - **Ativo**: O dispositivo A configura o dispositivo B como seu par (criando dessa forma uma associação permanente). Por sua vez, o dispositivo B também configura o dispositivo A como seu par (também cria uma associação permanente).
    - **Passivo**: O dispositivo A configura o dispositivo B como seu par (modo simétrico ativo). Mas o dispositivo B não tem o dispositivo A na sua lista de servidores ou pares. Ainda assim, ao receber um pacote de A, o dispositivo B cria uma associação transitória, de forma a poder fornecer ou receber o tempo de A. Esse modo é particularmente suscetível a ataques, onde um dispositivo intruso pode estar configurado no modo simétrico ativo e fornecer informações de tempo falsas para outro. Por isso deve sempre ser usado com criptografia.

Protocolo - Modos de Sincronismo

- Modo "***broadcast***"
  - NTP pode fazer uso de pacotes do tipo *broadcast* ou *multicast* para enviar ou receber informações de tempo.
  - Esse tipo de configuração pode ser vantajosa no caso de redes locais com poucos servidores alimentando assim uma grande quantidade de clientes.
  - O cliente NTP ao receber o primeiro pacote de um servidor, procura os dados por um curto período de tempo, como se estivesse no modo cliente - servidor, a fim de conhecer o atraso envolvido. Ou seja, durante alguns instantes há troca de pacotes entre cliente e servidor, depois disso o cliente passa apenas a receber os pacotes *broadcast* ou *multicast* enviados para a rede pelo servidor.
  - Tal como no caso do modo simétrico passivo, também se coloca aqui uma questão de segurança, porque um intruso pode facilmente enviar pacotes NTP falsos em modo broadcast. Assim a autenticação deve sempre estar habilitada.

Cabeçalho


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)

Cabeçalho

- **LI** (*Leap Indicator*)– 2 bits - Indicador de salto

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 Number*) – 3 bits - Número da versão
  - Actualmente versão 4

- **Mode** - 3 bits - Modo
  - Modos de associação entre os sistemas

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

Cabeçalho

- **Stratum** – 8 bits - Nº do Stratum

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- Máximo intervalo entre mensagens em Log2 (segundos)
- **Precision** – 8 bits - Precisão do relógio em Log2 (segundos)

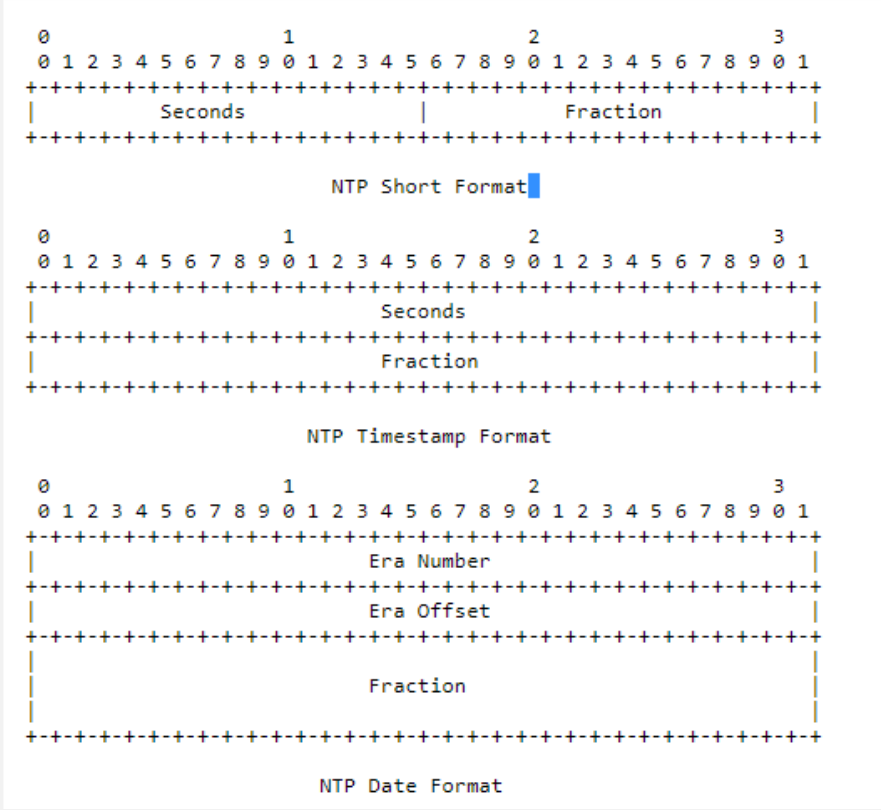
Cabeçalho

- **Root Delay** – 32 bits
  - Atraso do *round-trip* para o relógio de referência.
  - São actualizados/acumulados à medida que aumenta o *stratum*
- **Root Dispersion** – 32 bits
  - "dispersão" (erro) para o relógio de referência
  - São actualizados/acumulados à medida que aumenta o *stratum*
- **Reference ID** – 32 bits
  - Identificador do servidor ou relógio de referência para o *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

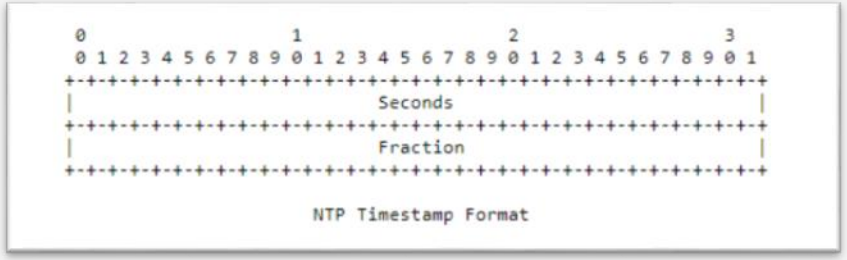
Tipo de Dados

- O formato da data de 128 bits é usado onde o armazenamento e tamanho de palavra são suficientes e estão disponíveis.
- Inclui um campo de segundos assinados de 64 bits, abrangendo 584 bilhões de anos e um campo de fração de 64 bits, resolvendo 0,05 attosegundos (isto é, 0,5e-18).



Timestamps

- São usados 64 bits para representar uma marca temporal (data/hora)
  - 32 bits representam os segundos
    - Suporta intervalos de 136 anos
    - Para suportar a representação de mais anos recorre-se ao conceito de Era
  - 32 bits representam frações de segundo com uma resolução de 232 picosegundos



Timestamps

- Para converter a hora do sistema em qualquer formato NTP tem de ser calculado o número de segundos (s) desde a época zero (00:00 01-01-1900) até à hora atual do sistema.
- Para determinar a era e o *timestamp* dado o s, deve fazer:

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

- Para determinar o s sabendo a era e o **timestamp** deve fazer:

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

Cabeçalho

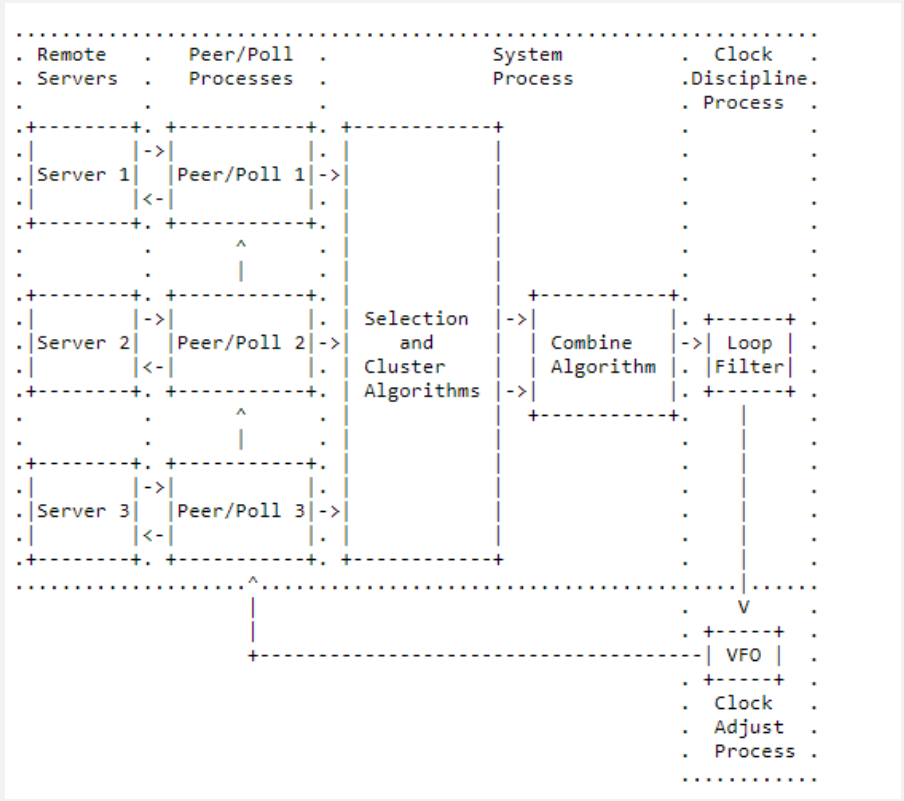
- **Reference Timestamp** – 64 bits
  - Hora em que o relógio do sistema foi ajustado pela última vez ou corrigido, no formato de carimbo de data / hora NTP.
- **Origin Timestamp** – 64 bits
  - Hora no cliente em que a solicitação partiu para o servidor, no formato de carimbo de data / hora NTP.
- **Receive Timestamp** – 64 bits
  - Hora no servidor em que a solicitação chegou do cliente, no formato de carimbo de data / hora NTP.
- **Transmit Timestamp** – 64 bits
  - Hora no servidor em que a resposta foi enviada para o cliente, no formato de carimbo de data / hora NTP.
- **Destination Timestamp** – 64 bits
  - Hora no cliente em que a resposta chegou do servidor, no formato de carimbo de data / hora NTP.

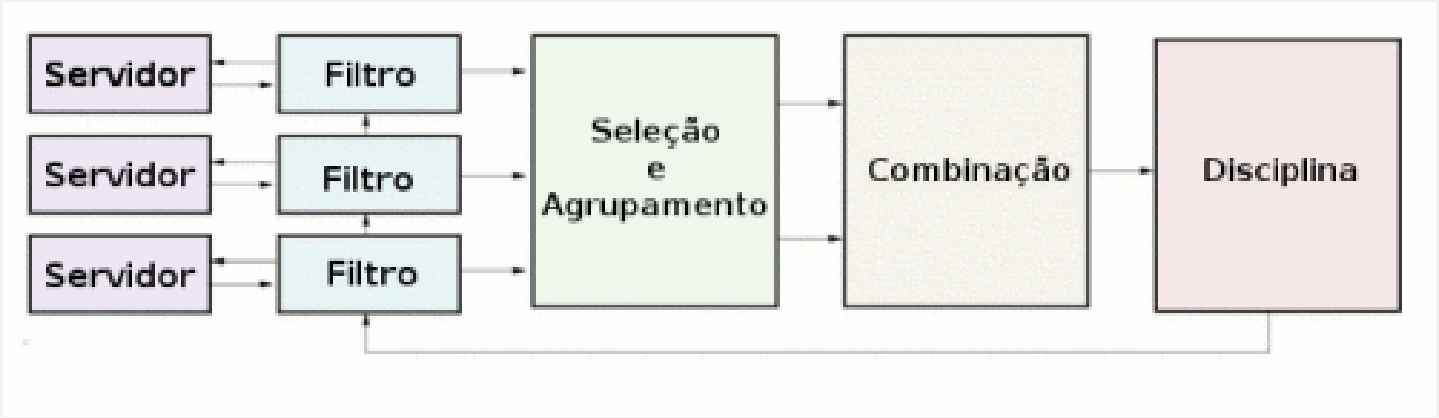
Parâmetros Globais

- O RFC 5905 define para o NTP versão 4 os seguintes parâmetros globais:

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

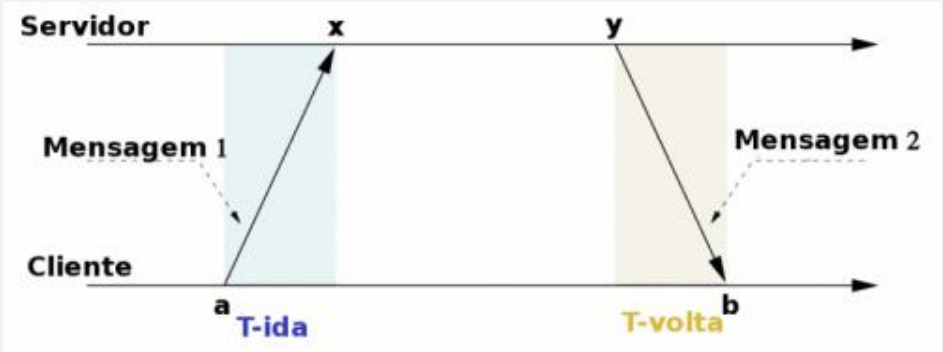
Funcionamento





Funcionamento – *Remote Server*

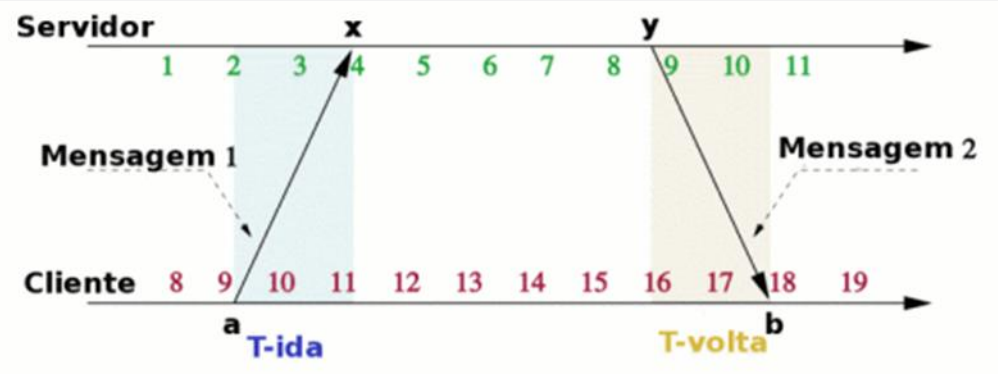
- Consideremos servidor e cliente com relógios não sincronizados. A troca de mensagens é a seguinte:
  - O **Cliente** lê seu relógio, que fornece o tempo **a**.
  - O **Cliente** envia a **Mensagem 1** com a informação de tempo **a** para o servidor.
  - O **Servidor** recebe a **Mensagem 1** e nesse instante lê seu relógio, que fornece o instante **x**.
  - O **Servidor** após algum tempo lê novamente seu relógio, que fornece o instante **y**.
  - O **Servidor** envia a **Mensagem 2** com **a**, **x** e **y** para o cliente.
  - O **Cliente** recebe a **Mensagem 2** e nesse instante lê seu relógio, que fornece o instante **b**.



Funcionamento - *Remote Server*

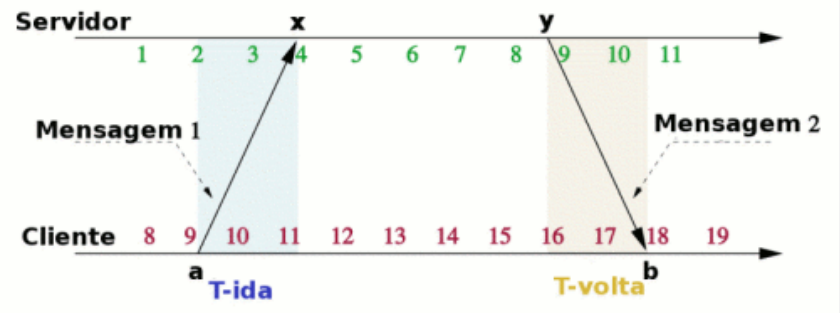
- Ao receber a **Mensagem 2**, o **Cliente** passa a conhecer os instantes **a**, **x**, **y** e **b**. Mas **a** e **b** estão numa escala de tempo, enquanto **x** e **y** em outra. O valor do incremento dessas escalas é o mesmo, mas os relógios não estão sincronizados.
- Não é possível, calcular o tempo que a **Mensagem 1** levou para ser transmitida ($\mathbf{T_{ida}}$), nem o tempo que a **Mensagem 2** gastou na rede ($\mathbf{T_{volta}}$). Contudo, o **tempo total** de ida e volta, ou **atraso** (também conhecido por ***Round Trip Time*** ou ***RTT***) que é a soma $\mathbf{T_{ida} + T_{volta}}$ pode ser calculado como:
- **atraso (RTT) = (b-a)-(y-x).**
- Considerando-se que o **tempo de ida é igual ao tempo de volta**, pode-se calcular o deslocamento entre o servidor e o relógio local como como:
- **deslocamento (offset) = x - (a + atraso/2) =**
  deslocamento (offset) = 1/2*[(x-a)+(y-b)].

Funcionamento - *Remote Server* - Exemplo



- O **Cliente** lê o relógio: **a=9**.
- O **Cliente** envia a **Mensagem 1 (a=9)**.
- O **Servidor** recebe a **Mensagem 1 (a=9)** e lê seu relógio: **x=4**.
- O **Servidor** algum tempo depois lê seu relógio novamente: **y=9**.
- O **Servidor** envia a **Mensagem 2 (a=9, x=4, y=9)**.
- O **Cliente** recebe a **Mensagem 2 (a=9, x=4, y=9)** e lê seu relógio: **b=18**.

Funcionamento - *Remote Server* - Exemplo

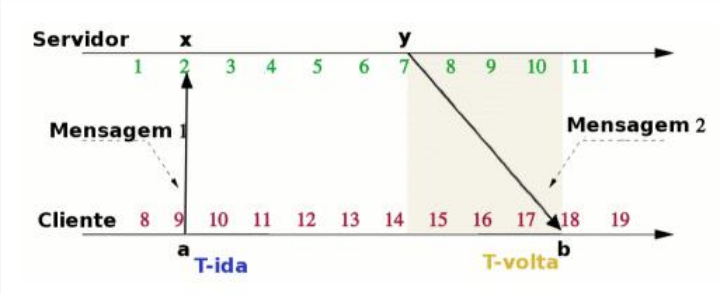


- É fácil observar que $\mathbf{T_{ida}=2}$ e $\mathbf{T_{volta}=2}$. Contudo, nem o **Cliente** nem o **Servidor** têm essa visão.
- O **Servidor** ao final da troca de mensagens descarta todas as informações sobre a mesma.
- O **Cliente** conhece as variáveis **a=9**, **x=4**, **y=9** e **b=18**, mas com delas é impossível calcular $\mathbf{T_{ida}}$ ou $\mathbf{T_{volta}}$.
- Contudo, é possível calcular o deslocamento:
  deslocamento =1/2*[(x-a)+(y-b)] =1/2*[(4-9)+(9-18)] = -14/2 = -7.
- Um deslocamento de **-7** significa que o relógio local do **Cliente** deve ser **atrasado 7 unidades de tempo** para se igualar ao do **Servidor**.

Funcionamento - *Remote Server* - Exemplo

- No exemplo anterior, consideramos que $\mathbf{T_{ida}}$ é igual ao $\mathbf{T_{volta}}$
- Mas isso nem sempre é verdade! Há atrasos aleatórios nas redes devido às filas de espera dos routers e switchs. Numa WAN ou na Internet as ligações a diferentes velocidades e rotas assimétricas, tráfego além de outros fatores, também causam diferenças entre estes dois tempos.
- No entanto, o NTP funciona exatamente dessa forma, considerando sempre que $\mathbf{T_{ida}}$ é igual ao $\mathbf{T_{volta}}$.
- E isso implica em erro…

Funcionamento - *Remote Server* - Exemplo



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

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

- O deslocamento está errado! Sabe-se que o valor correto é -7., contudo o valor calculado é -9. Isso deve-se a ao erro introduzido pela rede e que implica que o T_{ida} e T_{volta} não sejam iguais.

- No entanto, à partir do cálculo do deslocamento e do atraso, e levando em conta a limitação do método, que considera $T_{ida}=T_{volta}$, sabe-se que o deslocamento verdadeiro está entre:

  deslocamento - atraso/2 <= deslocamento verdadeiro <= deslocamento + atraso/2

  -9 -2 <= deslocamento verdadeiro <= -9 + 2

  -11 <= deslocamento verdadeiro <= -7

- Ou seja, dado um deslocamento de -9 e um atraso de 4, sabe-se que o valor verdadeiro do deslocamento é algo entre -11 e -7, mas não há como ter certeza de qual o valor..

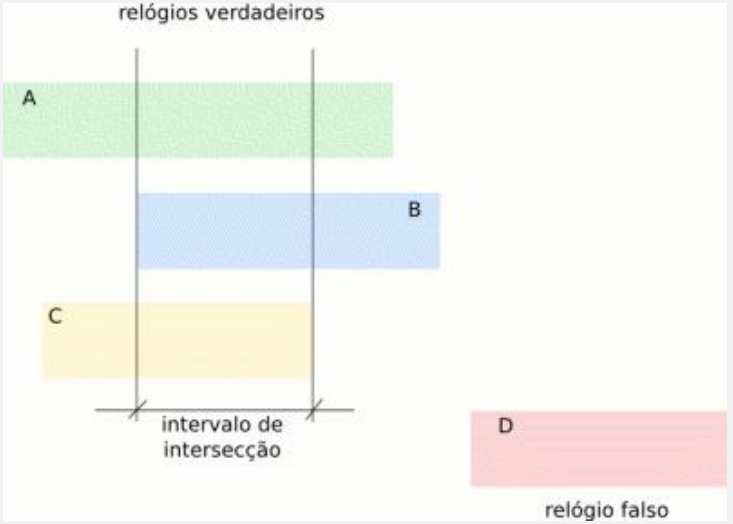
Funcionamento – *Peer/Poll*

- Através da troca de mensagens, o NTP consegue as informações de atraso e deslocamento de um servidor. Essa troca de mensagens não é realizada uma única vez, sendo que se repete periodicamente, num intervalo de tempo controlado pelo protocolo.
- No início da sincronização o cliente NTP faz uma consulta a cada servidor a cada 64s. Esse período varia ao longo do tempo, geralmente aumenta, até chegar a 1024s.
- Na realidade cada amostra é composta de 4 valores: atraso, deslocamento, dispersão e *timestamp*. O *timestamp* indica quando a amostra chegou e a dispersão é o erro estimado do relógio de servidor remoto, informada pelo servidor na mensagem NTP.
- A lista com os valores é ordenada em função do atraso. Considerando-se que as amostras com menor atraso são melhores porque provavelmente não se sujeitaram a filas de espera nos equipamentos de telecomunicações e assim estão mais próximas de garantir que o $\mathbf{T_{ida}}$ é igual ao $\mathbf{T_{volta}}$
- Os valores mais antigos são descartados, porque o valor de deslocamento pode já não corresponder à realidade, já que a exatidão do relógio local varia ao longo do tempo e das condições da rede.
- Após descartar as amostras antigas, resta uma lista com as amostras mais recentes e ordenadas em função do atraso. Da primeira entrada dessa lista são retiradas o atraso e deslocamento para o par cliente servidor (note-se que para cada par cliente - servidor há uma variável de cada tipo).

Funcionamento – *Selection and Cluster*

- Após na fase anterior se ter calculado os principais parâmetros referentes a cada um dos servidor é agora importante descobrir quais deles são confiáveis e quais não são.
- Os servidores que têm algum erro no tempo fornecido são chamados de **relógios falsos**.
- Os servidores que fornecem a hora corretamente são chamados de **relógios verdadeiros.**
- Para a seleção dos relógios, o NTP considera como verdadeiro o deslocamento que se encontra dentro de um determinado intervalo de confiança, calculado como:

intervalo de confiança = (deslocamento/2) + dispersão.

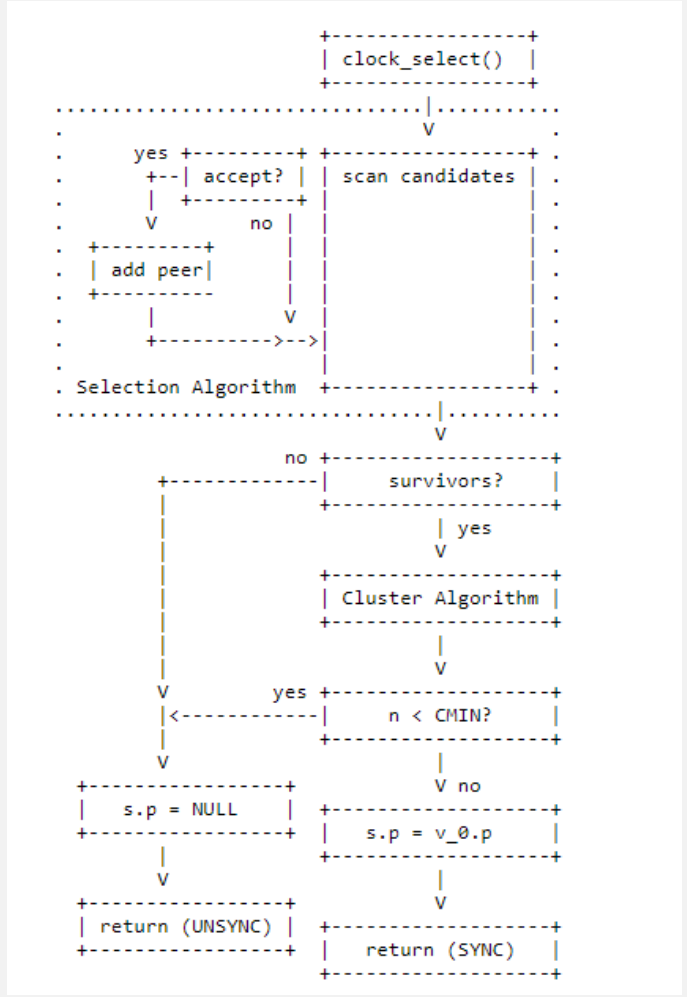


Funcionamento – *Selection and Cluster*

- Após terem sido escolhidos os relógios verdadeiros são utilizadas técnicas estatísticas, com o objetivo de selecionar os melhores.
- Os critérios de seleção utilizados são:
  - *Stratum.*
  - distância para a raiz.
  - variação (jitter).
- No processo alguns servidores são descartados, sendo chamados de relógios afastados.
- Os que permanecem são chamados de relógios sobreviventes.
- O melhor dos relógios sobreviventes é considerado como par do sistema (*system peer*).

Funcionamento - *Combine*

- Se o *system peer* for determinado pelo algoritmo da fase anterior já não entra nesta etapa.
- Para os outros casos em que há mais do que um sobrevivente e nenhum deles foi configurado como *system peer* é calcula uma média ponderada dos deslocamentos dos relógios, com o objetivo de aumentar a exatidão.



Funcionamento - *Discipline*

- O processo controla a fase e a frequência do relógio do sistema.
- O controle baseado na fase é melhor para as ocasiões onde há uma grande variação (*jitter*). Essa abordagem procura minimizar o erro no tempo, controlando indiretamente a frequência.
- O controle baseado na frequência é melhor para quando há instabilidades na frequência. A abordagem controla diretamente a frequência, e indiretamente o erro no tempo.
- O NTP disciplina o relógio local de forma contínua, mesmo em períodos onde não é possível consultar servidores de tempo.
- Assim:
  - São sempre que possível evitados saltos no tempo. O tempo é ajustado de uma forma gradual com a variação da frequência local do relógio.
  - Se a diferença for maior do que 128ms o NTP só proceder ao acerto do relógio se a mesma persistir por um período maior que 900s (15min).
  - Se a diferença for maior que 1000s (~16,7min) o algoritmo aborta a sua execução, considerando que algo muito errado aconteceu. As diferenças dessa ordem ou maiores devem ser corrigidas manualmente antes de se executar novamente a consulta NTP.

Segurança

- Em qualquer serviço de telecomunicações devemos garantir o seguintes aspetos no que diz respeito à informação:
  - integridade,
  - disponibilidade,
  - autenticidade;
  - confidencialidade.
- Os algoritmos vistos anteriormente, aliados à correta configuração do sistema, com um número suficiente de fontes de tempo com referências primárias independentes, garantem de forma satisfatória a integridade e disponibilidade do serviço.
- Os algoritmos de criptografia visam garantir a autenticidade da informação. Ou seja, têm o objetivo de assegurar ao cliente de que o servidor é quem ele diz ser.
- A confidencialidade não é considerada um problema no contexto do NTP. Ou seja, a informação de tempo irá "andar" na rede de forma aberta.
- As razões principais para o NTP funcionar dessa forma são:
  - o tempo é uma informação pública, não há razão para o esconder;
  - encriptar a informação iria introduzir complexidade e tempo de processamento tanto no servidor como no cliente o que iria degradar o desempenho do sistema, fazendo-o menos exato.

Segurança

- Existem basicamente dois métodos no NTP para realizar a autenticação:
  - chave simétrica (*symmetric key*)
  - chave pública (*autokey*).
- A autenticação por chave simétrica é o esquema utilizado originalmente na versão 3 do NTP, mas mantido da versão 4.
- Um conjunto de chaves deve ser gerado e partilhado pelo servidor e pelo cliente. O NTP não fornece meios para a transmissão ou armazenamento seguro das chaves sendo que isso deve ser feito com outros recursos.
- Chaves simétricas podem ser usadas para:
  - autenticar servidores ou pares no modo simétrico ativo;
  - autenticar pares no modo simétrico passivo ou servidores *broadcast* ou *multicast*;
  - autenticar requisições dos programas de monitoração e controlo.

Segurança

- **Autenticação por Chave Pública (*Autokey*)**
  - Na versão 4 do NTP é suportada uma nova forma de autenticação, baseada em chaves públicas e num protocolo que foi chamado de *autokey*.
  - A integridade dos pacotes é verificada através de chaves MD5 e a autenticidade das fontes de tempo é averiguada por meio de assinaturas digitais e vários esquemas de autenticação.
  - Esquemas de identificação (*identity schemes*) baseados em trocas do tipo desafio/resposta são usados para evitar vários tipos de ataques aos quais o método de chaves simétricas é potencialmente vulnerável.
  - A autenticação é baseada em **grupos de segurança** (*security groups*). Pode-se entender um **grupo de segurança** como um conjunto de servidores e clientes NTP que compartilha os mesmos métodos de autenticação, tendo na sua raiz um ou mais servidores considerados confiáveis, e administrados por uma mesma entidade.
  - Um grupo de segurança não tem de ter obrigatoriamente na sua raiz servidores stratum1, mas pode ser cliente de outros grupos de segurança onde exista esse servidor.

Dúvidas

Bibliografia

- 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