2020

Sistemas Distribuidos

Seguridad 2

Francisco Joaquín Murcia Gómez
48734281H
Universidad de Alicante

Contenido

Introduccion

Hoy en día el desarrollo de los sistemas de información en la red requiere referencias de tiempo confiables y precisas para una correcta sincronización y eficiencia. Los relojes internos instalados equipos informáticos están limitados por el tiempo impreciso que generalmente se establece en minutos. Una mala sincronización de tiempo o falta de precisión de este puede suponer por ejemplo desorganización en procesos industriales, fallos de actualizaciones…

Para evitar esto existen protocolos para aumentar esa eficiencia existen protocolos como:

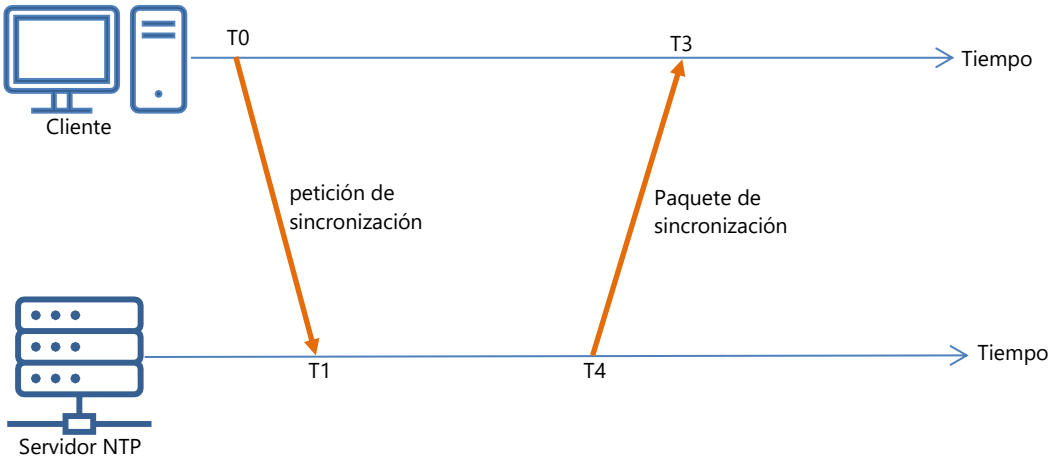
- **NTP** Network Time Protocol
  - Exactitud en microsegundos
- **SNTP** Simple Network Time Protocol
  - Exactitud en microsegundos
- **PTP** Precision Time Protocol (IEEE 1588)
  - Exactitud en nanosegundos

Protocolos de obtención del valor de tiempo

En primer lugar, hay que aclarar que los protocolos NTP y SNTP es el mismo protocolo, pero SNTP (como su nombre indica) es una versión más simple de NTP al ser el "mismo protocolo" ambos protocolos son interoperables, ambos protocolos usan la hora internacional (UTP) como referencia

NTP

NTP esta detallado en la RFC 958, utiliza una arquitectura cliente servidor que se basa en UDP en el puerto 123, su funcionamiento es simple:



1. El cliente envía una petición de sincronización
2. Si la diferencia de tiempo entre T0 y T1 es menor a 17 minutos hay sincronización
3. El servidor envía el paquete de sincronización
4. Una vez recibido el paquete cada minuto se va ajustando el desfase entre ambos hasta aproximarse a 128ms
5. Una vez llegado a 128ms el desfase se ajusta cada 17 minutos

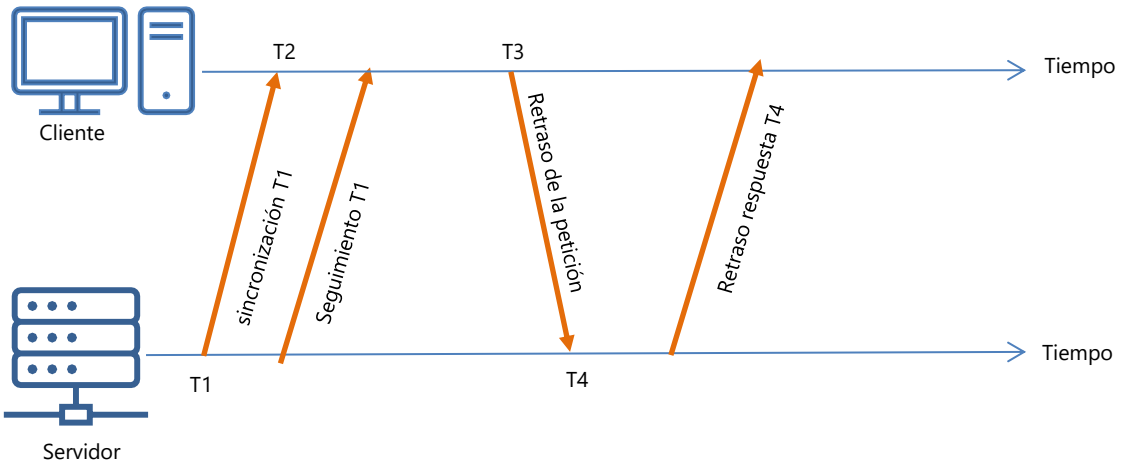
NTP es un protocolo ampliamente usado en Servidores Windows y Linux, también, es fácilmente segurizable ya que emplea el protocolo TLS, la versión actual es NTPv4

SNTP

SNTP es la versión simplificada de NTP como ya hemos comentado, pero omite varios pasos de la sincronización y varias partes de este paquete, ya que sincroniza periódicamente, esto es útil para dispositivos con bajos recursos, también SMTP no emplea los mismos algoritmos que NTP para garantizar la máxima exactitud, también peca de seguridad, ya que no está cifrado, versión actual es SNTPv4, cabe destacar

PTP

PTP es el más preciso de los dos anteriores ya que como ya se comentó se ajusta al nanosegundo, otra diferencia es que esta vez es el servidor el que pide la sincronización, también es que requiere un hardware especifico, también está diseñado para redes LAN. PTP emplea UDP en el puerto 319 y 320, Este protocolo emplea mecanismos de seguridad ya integrados, por estos motivos se emplean en transacciones bancares, cabe destacar que este sistema es de pago, su funcionamiento sería el siguiente:



1. El servidor envía un mensaje de sincronización T1 y el cliente guarda el momento de la llegada T2
2. Servidor envía un mensaje de con el tiempo en el que envió la sincronización T1 y cliente añade la diferencia de tiempos a su reloj interno
3. El cliente envía un mensaje al servidor y guarda el instante T3 y servidor guarda la llegada como T4
4. Por ultimo el servidor envía el tiempo T4 y el cliente calcula el retraso con (t3+t2-t1-t4)/2

Diferencias

NTP	SNTP	PTP
Precisión al microsegundo		Precisión al nanosegundo
Alta exactitud	Beja exactitud	Alta exactitud
Fácilmente securizable con TLS	Carece de seguridad	Mecanismos de autenticación y seguridad integrados
Uso de relojes maestros		Uso de relojes maestros
Interoperabilidad entre ellos		

Seguridad en NTP

Al emplear UDP NTP es un blanco fácil para diversos tipos de ataques, especialmente al DDoS, por ejemplo, Durante el año 2013 se generalizo el uso de ataques de denegación de tráfico para NTP, estos hacen un "ataque de reflejo" que envían un paquete con una dirección IP falsa., después, lo amplifican realizando un ataque de denegación de servicio (DDoS) fuera de juego temporalmente la conexión de todas las direcciones de la red

Para evitar esto multitud de desarrolladores ha securizado el protocolo, ya sea como por ejemplo "tlsdate" que fue una remodelación de NTP creada por Jacob Appelbaum en vez de usar UDP emplea TCP y cifra las conexiones con TLS

De todas formas, la versión reciente (NTPv4) emplea por defecto un sistema de autenticación por clave

En conclusión, los requisitos fundamentales para usar NTP de forma segura son:

- El cifrado de mensajes
- Securizado de los puertos (uso de TCP)
- Uso de las últimas versiones de NTP
- Uso de sistemas de autenticación

Conclusiones

Como ya hemos observado el uso de una buena sincronización de tiempo es fundamental para muchos procesos (industriales, seguridad, bancos, etc.) por ello hay que saber elegir el mejor sistema de valor de tiempo, tenemos:

- **NTP** que nos da una alta exactitud al microsegundo, es gratuito, pero no trae mucha seguridad por defecto, hay que implementarla
- **SNTP** igual que NTP, pero no trae nada se seguridad, es menos exacto que su homólogo y es el que menos recursos consumen
- **PTP** implementa seguridad por defecto (autenticación y cifrado), posee una alta exactitud al nanosegundo, pero es de pago y requiere hardware especifico

Personalmente usaría PTP por ejemplo para sistemas de transacciones de dinero o guiado de satélites ya que requieren de alta precisión y seguridad.

Usaria SNTP para sistemas embebidos ya que no disponen de mucha capacidad de procesamiento

Finalmente usaría la versión securizada de NTP "tlsdate" ya mencionada para el uso de un servidor de una empresa estándar que controle la videovigilancia, los terminales etc

Bibliografia

INCIBE-CERT-Instituto Nacional de Ciberseguridad | NTP, SNTP y PTP: ¿qué sincronización de tiempo necesito?

Galleon | SNTP y NTP? Esa es la pregunta - Razones por las que debe utilizar NTP sobre SNTP

IONOS | NTP: el protocolo de sincronización para sistemas de TI

Galleon | Seguridad NTP

RedIRIS | NTP : no solo para la hora.

Panda | ¡Cuidado! Los riesgos de los protocolos BGP, FTP y NTP

IEEE1588 | Página oficial del protocolo PTP

MentaData sistemas de información | PTP (IEEE 1588) vs NTP

Tecnozero | Servidor NTP o Servidor de hora

ntp.org | pagina oficial de NTP