Instalación y configuración de NTP

Oficina Nacional de Tecnologías de Información (ONTI)

ArCERT
Coordinación de Emergencias en Redes Teleinformáticas de Argentina
www.arcert.gov.ar

Agosto de 2006
versión 1.0

Resumen

Este documento es una introducción a la utilización del protocolo NTP y su configuración en las implementaciones más populares de la actualidad. Su objetivo es facilitar a los administradores de red de la APN una forma rápida de configurar NTP, a fin de que sea adoptado en todos los organismos, ya que su uso es necesario para una mejor correlación de eventos y bitácoras.

El temario incluye un acercamiento a la estructura jerárquica de sincronización y la configuración tanto del servidor como de los clientes en varios sistemas operativos.

Utilizaremos como base la distribución Debian, versión Sarge (o stable); aunque muchos de los conceptos vertidos en esta guía podrán ser aplicados a cualquier distribución de Linux, u otro sistema operativo tipo Unix (*BSD, Solaris, etc.). También se mostrará cómo configurar clientes NTP en plataformas Windows 2000 o superior.

En caso de dudas, corrección de errores o sugerencias para mejorar este documento envienos un correo electrónico a: **info@arcert.gov.ar**

Índice

1. ¿Qué es NTP?

NTP, o *Network Time Protocol*, es un protocolo diseñado para sincronizar los relojes de las computadoras a través de la red. La versión 3 de este protocolo es un *Internet Draft Standard*, formalizado en la **RFC 1305**. El protocolo NTP versión 4 es una importante revisión del estándar mencionado, y se encuentra en desarrollo, pero aún no ha sido formalizado en una RFC. Una versión simple de NTP (SNTP) versión 4 se describe en la **RFC 2030**.

2. Esquema de sincronización

Un servidor NTP primario, o *Stratum 1*, está conectado a un reloj de referencia de alta precisión. Esta referencia puede ser, por ejemplo, un reloj atómico, o un receptor de radio o GPS. Además, este servidor cuenta con software para manejar el protocolo NTP.

Otras computadoras, que funcionan como servidores *Stratum 2*, utilizan un software similar (usualmente el mismo), y consultan automáticamente al servidor primario para sincronizar su reloj. A su vez, éstos pueden sincronizar a otros servidores, que en este caso serán *Stratum 3*, y así podría seguirse hasta 16 niveles. La arquitectura también soporta que un cliente haga sus consultas a más de un servidor y puede haber comunicaciones entre servidores de un mismo *stratum*.

En la figura 1 puede verse un esquema de esta estructura.

Cuanto más alejado esté una computadora del reloj de referencia, o sea, cuanto más alto sea su *Stratum*, menos precisa será la sincronización. Sin embargo, cualquier *Stratum* siempre será suficiente para que el reloj no se aleje más de unos milisegundos de la hora real.

Hasta ahora definimos que una máquina, que llamaremos **cliente**, puede sincronizarse con otra o con alguna referencia externa, y también puede comportarse como **servidor**, y utilizarse para sincronizar otras. Siempre que

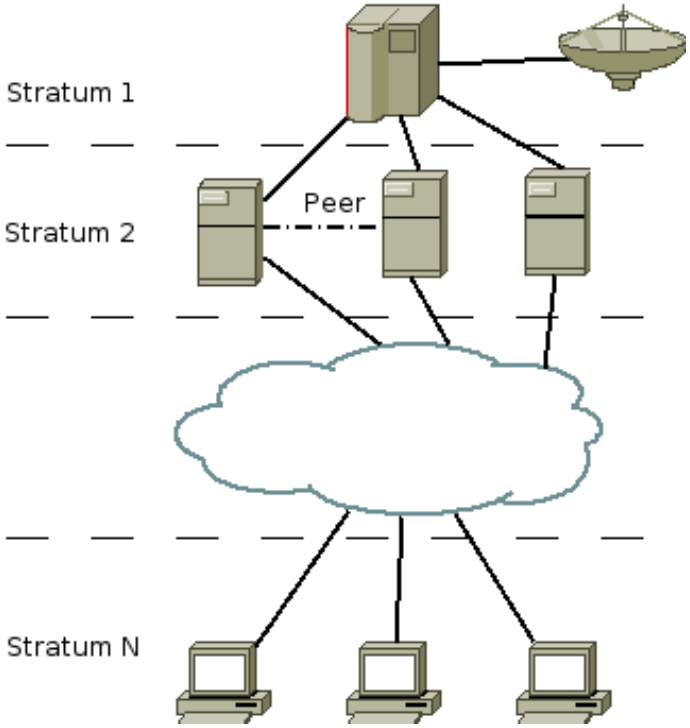

Figura 1: esquema jerárquico de NTP

haya una asociación entre dos máquinas, donde una se comporte como cliente, y otra como servidor, al cliente le corresponderá el *Stratum* inmediatamente superior al del servidor. Hay otra posibilidad, donde dos o más máquinas se configuran para comportarse entre sí como clientes o servidores, según quién esté más cerca de un reloj de referencia, o quién sea más confiable de acuerdo con el algoritmo que rige la sincronización por NTP. En este tipo de asociaciones, los servidores se llaman *Peers*.

Para utilizar NTP en una organización, recomendamos instalar un servidor que se sincronice con varias fuentes externas. Éste servidor será la única referencia horaria en la organización y todos los equipos estarán sincronizados con él. Opcionalmente, podría instalarse como fuente confiable un receptor GPS[1]. Esta última opción sólo es recomendada en los casos en los que se requieran niveles de redundancia y confiabilidad realmente altos, y queda fuera del alcance de este documento.

El servidor NTP instalado servirá para que todos los equipos de la organización lo utilicen para ajustar sus relojes. Este ajuste será de gran importancia ya que permitirá, entre otras, la correlación de eventos entre diferentes equipos.

La elección del equipo y el segmento de red donde se instale el servidor NTP queda a criterio de la administración de la red. Generalmente, el lugar más adecuado es la DMZ, o el lugar donde se encuentren los servidores que tienen contacto con el exterior. Sin embargo, como el protocolo NTP utiliza paquetes UDP para sincronizarse, y el cliente es quien envía un paquete para que el servidor responda, se podrá situar el servidor NTP en cualquier punto de la red. Los clientes internos de la red se podrán sincronizar directamente con este servidor. En el caso en que la organización posea gran cantidad de máquinas, o esté distribuida en varios sitios remotos, será conveniente la instalación de varios servidores, para que cada uno sirva de sincronizador a un área específica de cobertura.

Otras opciones para la utilización de un servidor NTP en una organización, son la instalación de software de NTP en el *firewall*, o en un *Router*. Se suele recomendar, por razones de seguridad, la conveniencia de no acumular servicios diferentes en el mismo equipamiento. Esta afirmación puede tener sus excepciones cuando la poca envergadura de la red no justifica más servidores y tráfico pasando a través del firewall.

[1] GPS: Sistema de posicionamiento global

3. Instalación de un Servidor

Para instalar un servidor NTP, recomendamos la utilización del software *NTPd*[2]. Todos los ejemplos que se muestran a continuación para la instalación de un servidor, corresponden a dicho software. Esta versión puede compilarse tanto en la mayoría de los sistemas *Unix-like*, como en las versiones Windows con tecnología NT.

La mayoría de las distribuciones GNU/Linux incluyen un paquete con este software. Para la instalación de un servidor NTP, recomendamos utilizar la distribución que mejor se adecúe a los procedimientos de la organización, y el paquete NTP correspondiente a la misma.

3.1. Configuración de peers/servidores

En lo que respecta a la configuración de un servidor NTP, nos referiremos siempre a la versión 4.2 o superior de NTPd. Normalmente (aunque esto puede variar según la distribución), el archivo de configuración utilizado es `/etc/ntp.conf`.

A continuación reproducimos un archivo de configuración básico:

```
server x.x.x.x
server 127.127.1.1 minpoll 4
fudge 127.127.1.1 stratum 10

driftfile /etc/ntp.drift
keys /etc/ntp.keys
```

A continuación describimos cada una de las sentencias mencionadas:

```
server x.x.x.x
```

Se le indica a nuestro equipo que sincronice su reloj con el servidor `x.x.x.x`. Se puede incluir cualquier cantidad de servidores de referencia, agregando líneas iguales a ésta. Esto es útil especialmente si este equipo será la principal referencia de tiempo en nuestra organización ya que en caso de que un servidor externo falle, o inclusive si enviase una hora errónea, el algoritmo del servidor NTP se encargará de elegir las mejores referencias disponibles. En caso de no disponer de una fuente confiable de hora, existen servidores NTP públicos que pueden usarse. En la sección '*Servidores NTP públicos*' se pueden encontrar las direcciones de las listas y sus opciones de configuración.

Si en lugar de actuar como cliente de un servidor, quisiésemos actuar como *peers*, el comando a utilizar deberá ser:

```
peer x.x.x.x
```

La siguiente línea indica que, además de sincronizar el reloj con el servidor externo mencionado en la línea anterior, se deberá utilizar un servidor *virtual* (el reloj interno de la máquina):

```
server 127.127.1.1 minpoll 4
```

Esto es necesario ya que en caso de no poder comunicarse con ninguna referencia externa, el servidor se considerará como *NO SINCRONIZADO*, y así se evitará que otros clientes puedan sincronizarse con él. El modificador `minpoll 4` indica que los pedidos de sincronización deberán realizarse cada 2^4 segundos, es decir 16 segundos. Este parámetro puede variar entre los valores 4 (16 segundos) y 17 (36,4 horas). Así se logra reducir significativamente el período de sincronización inicial del protocolo NTP para esta referencia.

Debido a que esta referencia no es exacta, la siguiente línea indica que se considere a la misma como de *Stratum 10*:

```
fudge 127.127.1.1 stratum 10
```

[2]NTPd puede obtenerse en `http://www.ntp.org`

Como en este caso (`server 127.127.1.1`) estamos utilizando el reloj interno del equipo en cuestión, que es eminentemente impreciso, es importante que el *Stratum* de esta referencia sea siempre mayor que cualquier otra referencia más precisa.

Las siguientes dos líneas suelen estar ya incorporadas con la configuración por defecto que incluyen las diversas distribuciones.

```
driftfile /etc/ntp.drift
keys /etc/ntp.keys
```

La primera indica el archivo donde se guardará el factor de corrección necesario para mantener el reloj sincronizado. La segunda indica el archivo donde se guardarán las claves necesarias para autenticar conexiones, como se verá más adelante.

3.2. Configuración de restricciones

Hasta ahora configuramos nuestro servidor para sincronizarse con una referencia externa y/o interna. Además, con esta configuración mínima ya se encuentra en condiciones de brindar servicio para que cualquier otra máquina se sincronice con él.

El protocolo NTP no sólo sirve para sincronizar relojes. Adicionalmente tiene incluidos los comandos necesarios para consultar y modificar la configuración actual del servidor. Para evitar la ejecución de comandos indeseados, o la sincronización con relojes no autorizados, es conveniente la configuración de restricciones de acceso.

Para comenzar con un enfoque conservador, decidimos prohibir todo y habilitar sólo lo estrictamente necesario. Para realizar esta tarea incluimos la siguiente línea en el archivo de configuración:

```
restrict default ignore
```

Esto limitará todas las posibles conexiones, sin importar su origen. Para poder sincronizar el reloj con el servidor configurado oportunamente, debemos indicar explícitamente cuáles son las restricciones:

```
restrict x.x.x.x mask 255.255.255.255 noquery noserve
```

Con esta directiva estamos indicando las siguientes restricciones:

- noquery: no se podrán realizar conexiones administrativas, tanto para consulta como para modificación de parámetros.
- noserve: no se aceptarán pedidos de sincronización.

Luego, el servidor `x.x.x.x` sólo podrá ser utilizado para sincronizar la hora de nuestro servidor NTP.

Con esta configuración, ningún cliente podrá sincronizar su reloj con el de nuestro servidor. Suponiendo que dicho servidor será la referencia de toda la organización, y que el rango de IPs de la organización es `x.y.z.0/24` la siguiente línea indica que no se podrán realizar pedidos administrativos desde la red `x.y.z.0`, y que nuestro servidor no podrá sincronizarse con otro en dicha red:

```
restrict x.y.z.0 mask 255.255.255.0 noquery nopeer
```

Sin embargo, cualquier cliente dentro de este rango podrá utilizar el servidor para sincronizarse.

Por último, debemos configurar dos restricciones extra.

```
restrict 127.127.1.1 mask 255.255.255.255 noquery
restrict 127.0.0.1 mask 255.255.255.255 noserve nomodify
```

La primer línea permite sincronizar con el reloj *virtual* interno y la segunda permite realizar conexiones administrativas desde el mismo host con el objeto de supervisar el comportamiento del NTP, pero sin la posibilidad de realizar modificaciones en la configuración.

Para ver más opciones puede consultarse la documentación[3].

[3] `http://ntp.isc.org/Main/DocumentationIndex`

3.3. Autenticación

Para mejorar la seguridad de las conexiones con un servidor NTP, con el cual nos estemos sincronizando, es conveniente utilizar los mecanismos de autenticación disponibles en el protocolo NTP. Se disponen de varias opciones de autenticación. Por razones de compatibilidad entre versiones, ejemplificaremos solamente la utilización de claves simétricas. Sin embargo, le recordamos que existen esquemas más seguros[4].

Para que un cliente pueda autenticar las conexiones que realiza con un servidor, o entre *peers*, cada servidor dispone de una lista de pares (identificador, clave), donde el identificador es un número entre 1 y 65535, y la clave, una cadena de caracteres. Estas claves, en las versiones más recientes del software, pueden ser creadas con el siguiente comando:

```
ntp-keygen -M
```

Las claves se guardan en el archivo que se indique en la configuración (`/etc/ntp.conf`), en nuestro caso:

```
keys /etc/ntp.keys
```

Este archivo tendrá la siguiente forma:

```
#ID  TIPO  CLAVE
1       M  XXXXXXXXXXXXXX01
2       M  XXXXXXXXXXXXXX02
3       M  XXXXXXXXXXXXXX03
4       M  XXXXXXXXXXXXXX04
5       M  XXXXXXXXXXXXXX05
6       M  XXXXXXXXXXXXXX06
7       M  XXXXXXXXXXXXXX07
8       M  XXXXXXXXXXXXXX08
9       M  XXXXXXXXXXXXXX09
10      M  XXXXXXXXXXXXXX10
11      M  XXXXXXXXXXXXXX11
12      M  XXXXXXXXXXXXXX12
13      M  XXXXXXXXXXXXXX13
14      M  XXXXXXXXXXXXXX14
15      M  XXXXXXXXXXXXXX15
16      M  XXXXXXXXXXXXXX16
```

Una vez declaradas las claves, debemos definir cuales son las autorizadas para autenticar sesiones. Esta tarea se realiza incluyendo, en el archivo de configuración, la siguiente línea:

```
trustedkey 6 10 13
```

En este caso se indica que se podrán utilizar las claves 6, 10 y 13 del archivo de claves definidas.

Con esta configuración ya estamos en condiciones de prestar el servicio de sincronización a un cliente que requiera el uso de claves, siempre que utilice aquellas definidas con los identificadores 6, 10 o 13. El cliente deberá incluir en su archivo de definiciones de claves alguna que coincida tanto en el ID como en la clave, por ejemplo:

```
10 M XXXXXXXXXXXXXX10
```

En su configuración el cliente indicará, suponiendo que el IP del servidor es `x.x.x.x`:

```
server x.x.x.x key 10
restrict x.x.x.x notrust
trustedkey 10
```

Con esta configuración se establece:

- que se comunique con el servidor x.x.x.x utilizando la clave con ID 10.
- que no acepte actualizaciones sin utilizar claves.
- que la clave 10 es válida para autenticación.

[4] Muchos de estos sistemas están descriptos en `http://www.eecis.udel.edu/~mills/ntp/html/authopt.html`

3.4. Administración y Monitoreo

Mediante el programa `ntpdc`, se pueden realizar una gran cantidad de operaciones de control y modificación sobre el estado de un servidor NTP. En esta sección nos concentraremos únicamente en un comando que nos permitirá controlar el estado de las conexiones con los diferentes *peers*.

En la configuración de restricciones declaramos, con la siguiente línea, los permisos necesarios para realizar conexiones administrativas, pero sin acceso a modificar el estado del servidor.

```
restrict 127.0.0.1 mask 255.255.255.255 noserve nomodify
```

Es importante destacar que de esta manera cualquier usuario local puede realizar consultas.

El comando de `ntpdc` que utilizaremos será `dmpeers`, o simplemente `dmp`. En este caso, la opción `-n` indica que los *peers* se muestren con su número IP y no con su nombre. Luego de su ejecución, obtendremos datos similares a los siguientes:

```
$  ntpdc -n
ntpdc> dmp
     remote           local      st poll reach  delay   offset    disp
==============================================================================
 136.159.2.2     192.168.1.1      2  512  377 0.26065 -0.016737 0.00703
 10.10.10.10     0.0.0.5         16  256    0 0.00000  0.000000 0.00000
 127.127.1.1     127.0.0.1       10   16  377 0.00000  0.000000 0.00023
.129.240.64.3    192.168.1.1      2  512  377 0.28410  0.001402 0.00943
 128.4.40.12     192.168.1.1      2  512  377 0.19525  0.011909 0.00705
.217.11.227.68   192.168.1.1      2  512  377 0.27829  0.004482 0.00705
 203.21.37.18    192.168.1.1      2  512  376 0.40329 -0.009594 0.01186
 195.13.1.153    192.168.1.1      2  512  377 0.25836  0.064884 0.00703
 202.71.97.92    192.168.1.1      2  512  377 0.44801 -0.005677 0.00703
*200.47.200.151  192.168.1.1      2  512  377 0.00822  0.000786 0.00847
ntpdc>
```

En el ejemplo podemos ver los diferentes *peers* configurados, y el estado de sincronización de cada uno. En la segunda fila, aparece el servidor `10.10.10.10` (inexistente, y agregado intencionalmente), que no es accesible. Este hecho se puede determinar por los siguientes datos: la segunda columna indica una dirección local inválida (`0.0.0.5`), la tercer columna indica `stratum 16`, y la quinta columna indica que se han recibido 0 respuestas de éste servidor. En la tercer fila (`127.127.1.1`) se observan los datos del reloj local, como se muestra en la configuración de la sección '*Configuración de peers/servidores*'. Se puede ver que la dirección local de acceso a este servidor es la `127.0.0.1`, y que el *stratum* de este *peer* es igual a 10. El resto de los peers, todos de *stratum* 2, tienen como dirección IP local la correspondiente a la interfaz de red a través de la cual se comunican con el exterior.

Otros datos interesantes son los de la cuarta columna (`poll`), que indica cada cuantos segundos se realiza una consulta con el peer correspondiente, y la última columna (`disp` dispersión), que muestra uno de los parámetros del algoritmo de sincronización NTP. Éste parámetro debe llegar a ser menor a 1 para que el servidor de referencia pueda ser elegido para sincronizarnos con él.

Por último, los caracteres a la izquierda de la dirección de IP de los peers indican:
(`.`): que el servidor fue descartado (momentáneamente), del algoritmo de elección de servidor de sincronización.
(`*`): que actualmente nuestro equipo está sincronizando su reloj con este servidor.

3.5. Configuración del Firewall

El protocolo NTP utiliza paquetes UDP para enviar y recibir mensajes. El puerto asignado a NTP es el `123/udp`. Para que el protocolo funcione correctamente, deberemos permitir libremente la comunicación entre nuestro servidor NTP y los servidores de referencia para los paquetes UDP con origen y destino en el puerto `ntp/udp`.

Algunos clientes, para comunicarse con un servidor, utilizan un puerto no privilegiado (mayor a 1024) como origen de los paquetes (por ejemplo los clientes de Windows 2000 y Windows XP). Para esto deberemos permitir

también los paquetes con origen en los clientes con puerto de origen udp mayor a 1024, y destino en el servidor NTP y puerto destino 123/udp.

En ambos casos la comunicación es bidireccional, por lo tanto deberán tomarse los recaudos necesarios para que los paquetes de respuesta sean también aceptados por los filtros.

4. Instalación de clientes

4.1. Unix y GNU/Linux

El programa utilizado como cliente NTP en las diferentes versiones de sistemas operativos derivados de Unix (Linux, *BSD, *UX, etc.) puede ser el mismo que se utiliza como servidor. La instalación dependerá de la distribución utilizada (en la mayoría de las distribuciones de Linux existe como paquete), y en algunas deberá ser compilado.

4.1.1. NTPd

La configuración es similar a la de un servidor, pero con algunas consideraciones especiales.

Configuración del servidor de referencia: La autenticación en los clientes ntpd sigue las mismas condiciones que en el servidor, por lo que la inicialización de las claves se realizará de la misma manera que se muestra en la sección '*Configuración de peers/servidores*'.

Para definir cuál será el servidor que nos sirva de referencia y con el cual podamos sincronizar el reloj de nuestro equipo, deberemos utilizar la siguiente línea de configuración, al igual que para un servidor, en el archivo `ntpd.conf`:

```
trustedkey 52
server w.x.y.z key 52
```

Restricciones: Al igual que en un servidor, se deberán considerar las siguientes restricciones generales:

```
restrict default ignore
restrict 127.0.0.1 mask 255.255.255.255 noserve nomodify
```

La segunda línea permite hacer consultas de control desde la máquina local. Para que las respuestas del servidor tengan permitida la entrada, hay que agregar la siguiente línea (donde `w.x.y.z` es la ip del servidor contra el que sincronizaremos):

```
restrict w.x.y.z mask 255.255.255.255 noquery nopeer
```

4.1.2. ntpdate

El programa *ntpd* mantiene sincronizado constantemente el reloj de una máquina utilizando una referencia externa, y realiza ajustes en la velocidad del reloj para que las diferencias sean cada vez menores. Así, el reloj del cliente nunca retrocederá y las horas convergerán en el futuro. Otra opción es realizar una sincronización por única vez (o cierta cantidad de veces por día). La sincronización realizada de esta manera hace que la hora se ajuste totalmente con la respuesta del pedido. Esto puede hacer que la hora retroceda, algo poco deseable.

De todas maneras suele usarse, ya que es una forma muy sencilla de sincronización y aceptable en la mayoría de los casos. Para este fin existe el programa *ntpdate*. Se ejecuta directamente con los siguientes parámetros:

```
ntpdate w.x.y.z
```

El cliente se sincronizará con el servidor ubicado en `w.x.y.z`. Opcionalmente, podría utilizarse `crontab` para repetir la ejecución del comando `ntpdate`, por ejemplo cada 3 horas:

```
* */3 * * *   root    /usr/sbin/ntpdate w.x.y.z
```

4.1.3. OpenNTP

Como alternativa a *ntpd* en los sistemas operativos Unix, se puede usar el programa *OpenNTPD*[5]. Este programa implementa el protocolo SNTP y provee funcionalidad tanto de cliente como de servidor.

OpenNTPD es un programa fácil de configurar, con pocos requerimientos de memoria, simple, seguro y compatible con NTP.

Si bien el RFC 2030 recomienda usar las implementaciones de SNTP sólo cuando el equipo actúe como cliente, en casos donde no se requiera una precisión de microsegundos es posible usarlo también como servidor. Se recomienda evaluar los requerimientos particulares de cada red antes de decidir que opción es más conveniente.

El archivo de configuración (`/etc/openntpd/ntpd.conf` en el caso de Debian) debe contener una o más lineas líneas como ésta:

```
server w.x.y.z
```

Esto sincronizará con la IP `w.x.y.z` o, si se especifica un FQDN, la primer resolución válida. Es recomendable declarar varios servidores de sincronización.

Si un FQDN engloba varias IPs y se desea sincronizar con todas ellas, la sentecia a utilizar es `servers`, de la siguiente manera:

```
servers pool.ntp.org
```

OpenNTP puede funcionar en modo servidor agregando la dirección donde se quiere que el servidor escuche, por ejemplo:

```
listen on 192.168.4.1
```

4.2. Windows 2000

El sistema operativo *Windows 2000* tiene incorporado el protocolo SNTP v2 en el servicio *Horario de Windows* (Windows Time), accesible desde la consola de administración de servicios. Para que se realicen actualizaciones automáticas, hay que asegurarse que el servicio se inicie automáticamente, como puede verse en la figura 2.

Para indicar cual será el servidor con el cual se sincronizará el equipo, se debe ejecutar el siguiente comando con privilegios de administrador, utilizando una ventana de símbolo de sistema:

```
net time /setsntp:w.x.y.z
```

Se puede verificar el servidor configurado con el siguiente comando:

```
net time /querysntp
```

Un ejemplo de ambas operaciones puede verse en la figura 3.

4.3. Windows XP

Para configurar un cliente *Windows XP*, existe una nueva solapa en el cuadro de configuración de *Fecha y Hora* accesible sólo con privilegios de administrador. Se deberá completar como se ve en la figura 4.

4.4. Routers

Muchos routers tienen soporte para correr el protocolo NTP como servidores.

En particular, los routers Cisco incorporan el protocolo NTP como parte del sistema operativo *IOS*. En esta sección nos ocuparemos de éstos, siempre refiriéndonos a las versiones de *IOS* 12.1 o posteriores.

[5] `http://www.openntpd.org/`

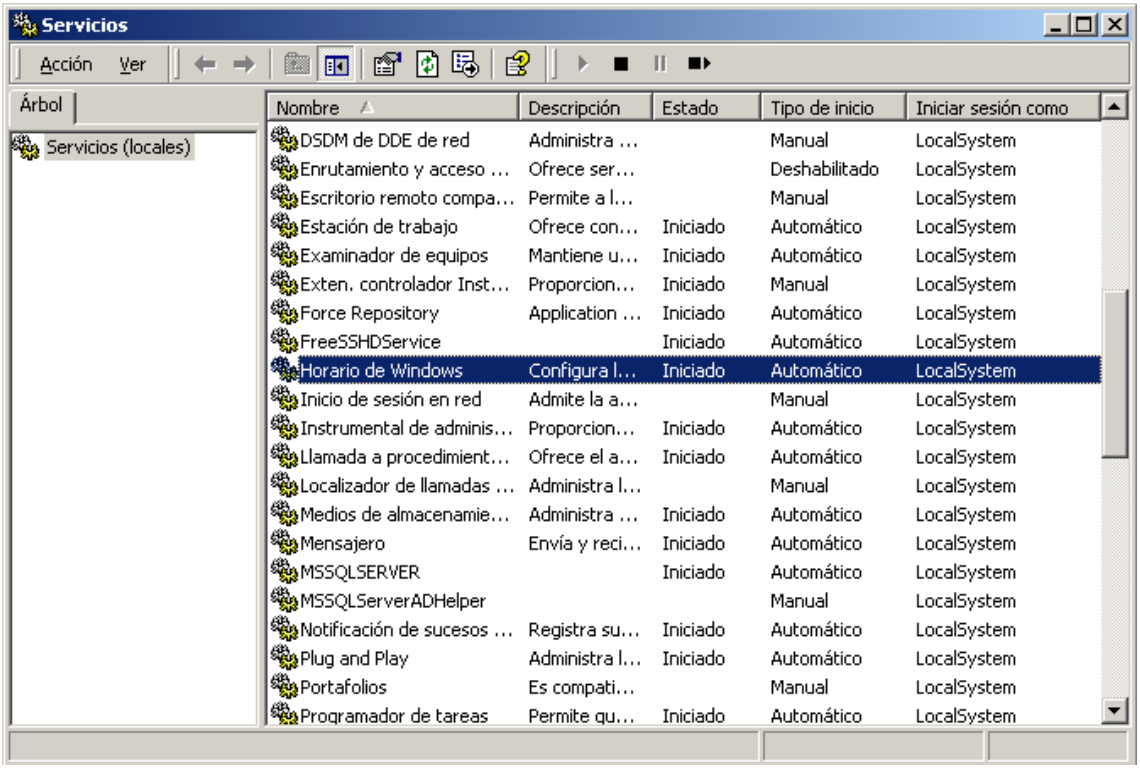

Figura 2: Configuración en Windows 2000

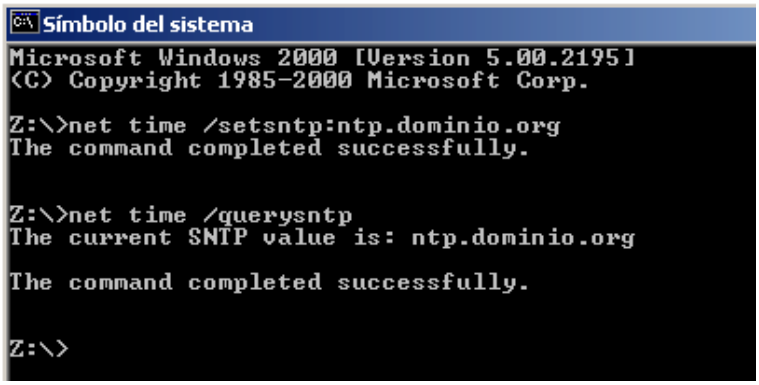

Figura 3: Ejemplo de configuración en Windows 2000

Configuración: En los routers low-end de Cisco (1003/4/5, 1600, 1720 o 1750), puede utilizarse el siguiente comando, en modo de configuración, para utilizar la versión simplificada de NTP (SNTP) para sincronizar el reloj del router con un servidor externo (en este caso con IP `w.x.y.z`):

```
sntp server w.x.y.z
```

Para el resto de los routers que utilicen IOS, se deberá utilizar la siguiente línea de configuración:

```
ntp server w.x.y.z [version] [key id]
```

Donde los parámetros `[version]` y `[key id]` son opcionales. De esta manera el router Cisco se encuentra configurado para utilizar al servidor `w.x.y.z` como referencia, y como servidor NTP para quien lo requiera.

Para configurar la zona horaria del router correspondiente a la de Argentina debemos utilizar el comando `clock timezone` de la siguiente manera:

```
clock timezone ART -03
```

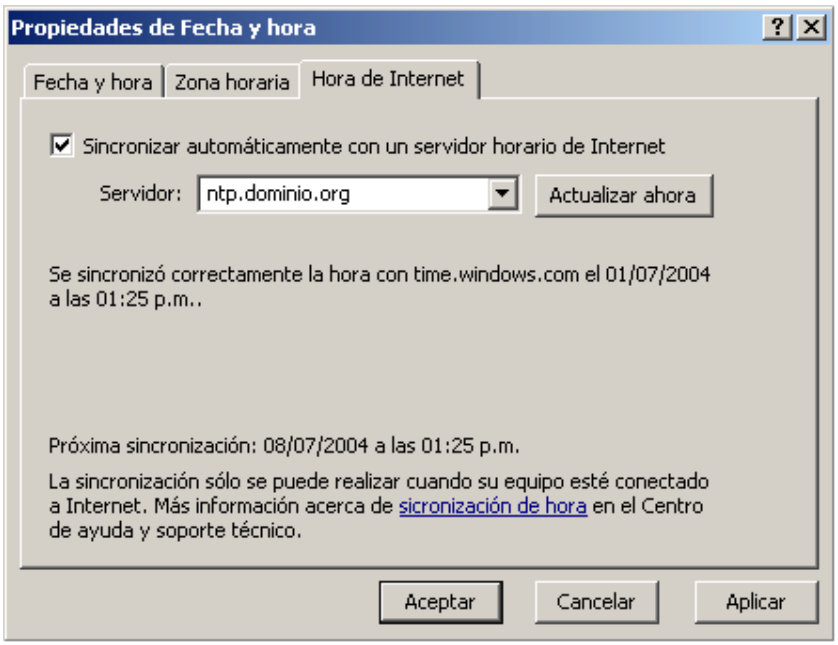

Figura 4: Ejemplo de configuración en Windows XP

Seguridad: Al igual que en el `ntpd`, disponemos del método de autenticación utilizando MD5 definido por el protocolo NTP. Las claves definidas que sean configuradas como `trusted`, serán las que definirán los servidores que pueden ser utilizados para sincronizar el reloj. La configuración utilizada para habilitar la autenticación es la siguiente:

```
ntp authenticate
ntp authentication-key <number> md5 <value>
ntp trusted-key <number>
```

Estas claves son las que se deberán utilizar en la definición de `ntp server` de la sección anterior.
Para configurar restricciones, similares a las del programa `ntpd`, se utiliza la siguiente configuración:

```
ntp access-group {query-only | serve-only | serve | peer } <access-list-number>
```

La opción `peer` permite utilizar los IPs que pasen el `access-list`[6] configurado como servidores NTP. Estos IPs también podrán realizar todo tipo de conexiones NTP que realicen cambios en nuestro router, por lo tanto deberá utilizarse con cuidado. En el otro extremo, `query-only` sólo permitirá a los IPs que coincidan con el `access-list` utilizar el router como servidor NTP, sin realizar ningún tipo de cambio.
Otra opción de restricción consiste en deshabilitar por completo el protocolo NTP en una interfaz de red. Para ello, en modo de configuración de interfaz, deberá utilizarse la siguiente línea de configuración:

```
ntp disable
```

Para más información sobre configuración de routers Cisco, consultar la documentación incluida con la distribución del IOS utilizado, o en `http://www.cisco.com`.

5. Ejemplos prácticos de configuración

A continuación mostramos un ejemplo completo de configuración siguiendo el esquema de la figura 5.

[6]Este documento no tiene por objetivo explicar el funcionamiento y la configuración de ACLs. Más información: `http://www.cisco.com/warp/public/707/confaccesslists.pdf`

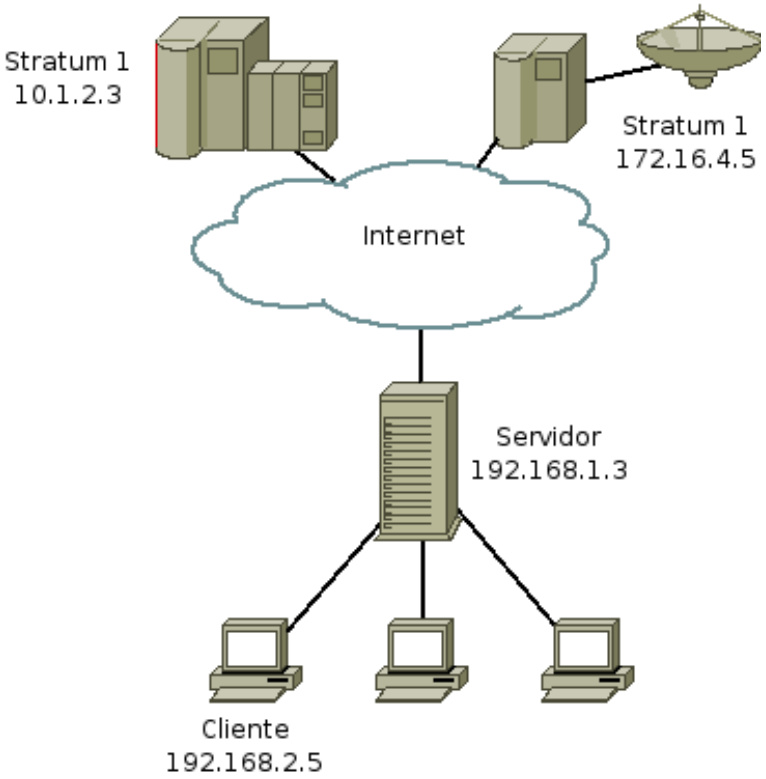

Figura 5: Topología utilizada para el ejemplo

5.1. ntpd como servidor

ntp.key:

```
#ID  TIPO  CLAVE
1       M  XXXXX01XXXXXXX01
2       M  XXXXX02XXXXXXX02
3       M  XXXXX03XXXXXXX03
4       M  XXXXX04XXXXXXX04
5       M  XXXXX05XXXXXXX05
6       M  XXXXX06XXXXXXX06
7       M  XXXXX07XXXXXXX07
8       M  XXXXX08XXXXXXX08
9       M  XXXXX09XXXXXXX09
10      M  XXXXX10XXXXXXX10
11      M  XXXXX11XXXXXXX11
12      M  XXXXX12XXXXXXX12
13      M  XXXXX13XXXXXXX13
14      M  XXXXX14XXXXXXX14
15      M  XXXXX15XXXXXXX15
16      M  XXXXX16XXXXXXX16
```

ntp.conf:

```
# archivo donde se guardará el factor de corrección
driftfile /etc/ntp.drift

# reloj local
```

```
server 127.127.1.1 minpoll 4
fudge 127.127.1.1 stratum 10

# servidores
server 10.1.2.3
server 172.16.4.5

# restricciones por defecto, ignorar todo
restrict default ignore

# acceso desde la misma máquina
restrict 127.0.0.1 mask 255.255.255.255

# acceso a los servidores de referencia
restrict 10.1.2.3 noquery noserve
restrict 172.16.4.5 noquery noserve

# acceso desde la red local. Permite a los clientes sincronizarse
restrict 192.168.2.0 mask 255.255.255.0 noquery nopeer

# Claves habilitadas para comunicarse con nosotros.
keys /etc/ntp.key
trustedkey 7
trustedkey 8
trustedkey 9
```

En este ejemplo, y debido a que los servidores de referencia son externos y públicos, no utilizamos autenticación. En caso de que los servidores externos provean algún método de autenticación, es altamente conveniente que sea utilizado.

5.2. ntpd como cliente

ntp.key:

```
# Sólo las claves necesarias
#ID TIPO CLAVE
8 M XXXXX08XXXXXXX08
```

ntp.conf:

```
# archivo donde se guardará el factor de corrección
driftfile /etc/ntp.drift

# servidores, utilizando autenticación
server 192.168.1.3 key 8

# restricciones por defecto, ignorar todo
restrict default ignore

# acceso desde la misma máquina, para supervisión.
restrict 127.0.0.1 mask 255.255.255.255

# acceso al servidor de referencia
restrict 192.168.1.3 noquery noserve

# Claves habilitadas para sincronizar.
```

```
keys /etc/ntp.key
trustedkey 8
```

6. Servidores NTP públicos

Existen alrededor del mundo varios servidores que brindan servicio de NTP al público. Ninguno de estos servidores garantiza la continuidad ni la exactitud del servicio, y algunos requieren ciertas condiciones para iniciar la sincronización. Las listas de servidores públicos puede encontrarse en la sección '*Más información*'. Es recomendable utilizar únicamente servidores de *Stratum 2*, reservando los *Stratum 1* para las grandes organizaciones que necesiten implementar sus propios servidores *Stratum 2* por razones de escala.

6.1. Pool Servers

Los *pool servers* utilizan *DNS round-robin* para configurar varios servidores diferentes y balancear la carga. Se puede consultar la lista de *pool servers* en `http://ntp.isc.org/bin/view/Servers/NTPPoolServers` clasificados por región.

Para configurar un pool específico en su servidor `ntpd`, por ejemplo en Sudamérica, deberá definir una lista en el archivo de configuración de la siguiente manera:

```
server 0.south-america.pool.ntp.org
server 1.south-america.pool.ntp.org
server 2.south-america.pool.ntp.org
```

7. Más información

Puede encontrarse información adicional en:

- Página de la implementación oficial de referencia del protocolo NTP - `http://www.ntp.org`
- Página oficial de los manuales de OpenNTP - `http://www.openntpd.org/manual.html`
- RFC 1305 - `http://www.rfc-editor.org/rfc/rfc1305.txt`
- RFC 2030 - `http://www.rfc-editor.org/rfc/rfc2030.txt`
- Servicios NTP públicos - `http://ntp.isc.org/`
- Lista de servidores NTP públicos de *Stratum* 1 - `http://ntp.isc.org/bin/view/Servers/StratumOneTime`
- Lista de servidores NTP públicos de *Stratum* 2 - `http://ntp.isc.org/bin/view/Servers/StratumTwoTime`
- Configuración de Routers cisco en - `http://www.cisco.com`
- Clientes NTP y SNTP para versiones de MS Windows anteriores a Windows 2000 en - `http://www.tucows.com` y `http://www.download.com`