

Windows Time Service

Mark E. Donaldson

Network time synchronization is an important function that ensures that time-sensitive programs such as messaging and financial applications operate properly in a Windows NT network. Time synchronization is also crucial in a Windows 2000 (Win2K) network because Win2K's authentication protocol, Kerberos 5, uses a timestamp as one security element that authenticates clients. In addition, Kerberos 5 uses client workstation time in its ticket-generation process.

Win2K provides a built-in, must-run Windows Time Service for time synchronization. This service is different from the NT time service, which is an optional service you can install from the Microsoft Windows NT Server 4.0 Resource Kit. Win2K also provides an enhanced Net Time command. Reviewing NT time synchronization will help you better understand the differences between Win2K and NT time synchronization and how to integrate time synchronization in a mixed Win2K and NT environment.

NT Time Service

NT's time-synchronization tools consist of a time service (i.e., TimeServ) and the Net Time command. Douglas Hugarth, a former Microsoft employee, originally developed and currently maintains the most recent version of TimeServ. TimeServ 1.55 is available on the Microsoft Windows NT Server 4.0 Resource Kit Supplement 4 CD-ROM, or you can download it from Microsoft's FTP site (<ftp://ftp.microsoft.com/reskit/y2kfix>). TimeServ 1.55 runs as an NT service that automatically synchronizes local system time between a standard time service provider and a time server in an NT domain. Net Time is a subcommand of the Net command in NT and Windows 9x. This command lets you manually synchronize local system time between a computer in the network and a time server in an NT domain or workgroup.

Using TimeServ and Net Time, you can set up a multi-tiered time-synchronization system in your NT network. Figure 1 illustrates this multi-tiered system. TimeServ lets you designate an NT computer as a master time server for your entire NT network. This master time server can obtain standard time from a time service provider—such as the National Institute of Standards and Technology (NIST), United States Naval Observatory (USNO), and several other international time service providers—through a modem dial-up. The master time server can also obtain time from NIST through the Internet and a Network Time Protocol (NTP) time server. The primary time server in the center of the multi-tiered time-synchronization hierarchy obtains time from the master time server and works as a time source for the secondary time server and client workstations. You generally configure one or more NT servers as a primary time server in each of your company's major geographical locations, each master account domain, or each domain, and enable the server to be a time source (i.e., a system that provides accurate time). Secondary time servers and workstations at the bottom of the time-synchronization hierarchy retrieve time from a time source. All NT servers except the master and primary time servers in your network can be secondary time servers.

The TimeServ service consists of three files: `timeserv.exe`, `timeserv.dll`, and `timeserv.ini`. You save `timeserv.exe` and `timeserv.dll` in the `C:\winnt\system32` directory, and `timeserv.ini` in the `C:\winnt` directory. You customize the `timeserv.ini` file to define an NT server as a master, primary, or secondary time server. The three sample `timeserv.ini` files in Figure 1 specify that the master time server obtain the time from an NTP server, the primary time servers get the time from the master time server and play the role of a time source, and the secondary time servers retrieve time from the primary time servers in the domain. After you configure the `timeserv.ini` file, you can install TimeServ at a command prompt. Simply enter the `timeserv automatic` command, which tells NT to automatically start TimeServ when you boot NT. Alternatively, you can run the `time manual` command, which tells

Windows Time Service

Mark E. Donaldson

NT that you will manually start TimeServ. If you modify timeserv.ini after you install TimeServ, you must stop TimeServ, enter the timeserv update command at a command prompt, and restart TimeServ to use the new configuration. If you set **TimeSource=yes** in timeserv.ini, you must reboot the server after the TimeServ command runs. Another way to enable a time source on an NT machine is to manually add the TimeSource Registry parameter with a REG_DWORD value of 1 to the:

HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\LanmanServer\Parameters

subkey. This modification also requires a reboot. To remove TimeServ, you can use the resource kit's Delsrv command. However, to disable the time source function, you must manually delete the Registry **TimeSource** parameter or change its value to 0, then reboot.

In early 1999, before the company certified that TimeServ was Y2K compliant, Microsoft released a new NT time service, Windows Time Service (i.e., W32Time). You can download this service, which is basically a subset of TimeServ, from <ftp://ftp.microsoft.com/reskit/y2kfix>. W32Time doesn't support modem dial-up and TCP-based Internet time retrieval from NIST in a master time server. The master time server can obtain time only from an NTP server. Primary and secondary time servers using W32Time work the same way servers using TimeServ do. However, a W32Time time server can be an NTP server; TimeServ doesn't offer that functionality. W32Time comes with three files: w32time.exe, w32time.dll, and w32time.ini. You use these files in the same way that you use TimeServ's files. To enable a time server as an NTP server, you need to set the w32time.ini LocalNTP parameter to yes on the server. This feature is useful for time synchronization in a mixed Win2K and NT environment.

NT and Win9x Net Time

NT workstations can use TimeServ and W32Time to be secondary time servers in a time-synchronization hierarchy, as Figure 1 shows. However, you might prefer not to install a new service on each workstation. Alternatively, you can use NT or Win9x's Net Time command to synchronize time with a time source in the network. You simply enter one of the following Net Time commands at a command prompt:

Net Time /set /y synchronizes a workstation's time to a time source in the workstation's domain.

Net Time \\time_server_name /set /y synchronizes a workstation's time to a specific time server.

Net Time /domain:domain_name /set /y synchronizes a workstation's time to a time source in a specific domain.

These commands synchronize a workstation's system time each time a user logs on to the domain from the workstation. Microsoft confirmed that the last command doesn't work in NT as expected. The command synchronizes a workstation's time with the domain's PDC instead of with a time source. Although Microsoft hasn't provided a fix, Win2K's Net Time command doesn't have this problem and uses a new /rtsdomain switch to specify a time source lookup in a specific domain.

In addition, Win9x's Net Time command doesn't work correctly when a time source and client are in different time zones. For example, if the current time of the time source in Chicago is 8:00 a.m.

Windows Time Service

Mark E. Donaldson

central time, Net Time sets the time clock on a Win9x computer in Los Angeles to 8:00 a.m. Pacific time instead of 6:00 a.m. Pacific time. Microsoft released a fix for this problem—Nettime—in the Microsoft Windows 98 Resource Kit and the Microsoft Windows NT Server 4.0 Resource Kit Supplement 3 or later. To use Nettime, you need to copy the nettime.exe and rtzone.exe files to C:\winnt\system32 or another searchable directory. You use Nettime in the same way you use Net Time, but you don't need to include the /set and /y switches to set the system time.

Win2K Time Service

For Win2K, Microsoft developed a new time service that has the same name as NT's time service—Windows Time Service (i.e., W32Time). Win2K preinstalls this service as a required service on servers and workstations, and W32Time automatically starts after you boot Win2K. By default, Win2K W32Time can automatically synchronize time on all Win2K computers; however, you must specify an NTP time server that the master time server (called the authoritative time server in Win2K) synchronizes time with.

W32Time consists of two types of synchronization: NT5DS and NTP. NT5DS uses the Active Directory (AD) domain hierarchy for time synchronization, and NTP synchronization lets you manually specify the NTP servers, Win2K domain controllers, and Win2K computers (i.e., if you set the **LocalNTP** parameter to 1 on the computers) that a system synchronizes time with.

W32Time uses Simple Network Time Protocol (SNTP—a subnet of NTP) for time synchronization. SNTP and NTP use the same network-packet format. The main difference between SNTP and NTP is that SNTP doesn't provide the error-check and filtering functions that NTP provides.

Win2K W32Time uses the AD domain hierarchy as its time-synchronization hierarchy. **The PDC of the root domain of the AD forest is the authoritative time server of the Win2K network. This PDC synchronizes time from the external NTP time server of a standard time provider. All other domain controllers in the root domain synchronize time from the PDC of the root domain.** The PDC of a child domain synchronizes time with a domain controller of its parent domain. For example, in Figure 2, the PDC of the domain ny.acme.com obtains time from a domain controller in the parent domain acme.com. A domain controller in a child domain synchronizes time from either a domain controller in its parent domain or the PDC of the child domain. For example, a domain controller in the domain ny.acme.com obtains time from a domain controller in the domain acme.com or the PDC of the domain ny.acme.com. **All Win2K member servers and workstations obtain time from any domain controller in the local domain.**

For the authoritative time server to obtain accurate time, you need to define one or more external NTP time servers on the PDC of the root domain of the forest. You can use Win2K's new Net Time command to do so. For example, if you want to use the three NTP time servers at USNO as the time servers for your authoritative time server, win2kdc1.acme.com, enter the following command at a DOS prompt on your Win2K workstation:

```
net time \\win2kdc1.acme.com /setsntp:"192.5.41.209 192.4.41.40 192.5.41.41"
```

This command makes a Registry change for the W32Time service. If you physically enter the command on the authoritative time server, you don't need to specify the name of the authoritative time server in the command. After you use the Net Stop w32time and Net Start w32time commands to restart the service, the authoritative time service will obtain standard time from one of the three

Windows Time Service

Mark E. Donaldson

USNO time servers. Using at least two servers as authoritative time servers provides fault tolerance. If one server is not available, W32Time will try to synchronize time from the next available NTP server. SNTP and NTP use UDP port 123. You need to open this port in your Internet firewall so that your authoritative time server can obtain time from an Internet NTP server.

In addition to synchronizing with a domain controller in its parent domain or the PDC of its own domain, a domain controller in a child domain can synchronize time from another domain controller in the local domain. However, the local domain controller must have the reliable time source flag set to on in its W32Time Registry key. By default, this flag is off. You can enable the flag on a domain controller only if you directly attach the domain controller to a hardware clock. To turn on the flag, you need to add the **ReliableTimeSource** Registry parameter with a REG_DWORD value of 1 to the:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

subkey.

A Win2K time server can be a parent domain controller, local domain PDC, or local domain controller. A domain controller uses a complicated algorithm to determine the best system to synchronize time from. When a domain controller needs to synchronize time, it sends the network as many as three queries requesting information about other domain controllers. Another domain controller responds with information that tells whether that domain controller is in the same AD site (i.e., in-site) or a different AD site (i.e., out-site) as the requesting domain controller. In addition, the responding domain controller tells whether it's a reliable time source, whether it's in the parent or local domain of the requesting domain controller, and whether it's a PDC. Based on this information, the requesting domain controller uses the following order of preference to select a time server:

1. Parent domain controller that is in-site and a reliable time source
2. Local domain controller that is in-site and a reliable time source
3. Parent domain controller that is in-site
4. Local domain PDC that is in-site
5. Parent domain controller that is out-site and a reliable time source
6. Local domain controller that is out-site and a reliable time source
7. Parent domain controller that is out-site
8. Local domain PDC that is out-site

Customizing Win2K Time Service

Win2K time synchronization automatically works with minimal manual configuration. However, in certain circumstances, you might want to customize Win2K W32Time (e.g., if you're using a Win2K Server system as an SNTP server to avoid synchronization across sites). To customize W32Time, you manually modify the Registry settings in the:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

subkey. You need to restart the W32Time service for a change to take effect.

By default, when you start W32Time, the service synchronizes system time every 45 minutes until the time successfully synchronizes (i.e., the local system time matches the time source's time) three times. Thereafter, the service synchronizes every 8 hours. If you want the computer to synchronize

Windows Time Service

Mark E. Donaldson

time every hour, you can change the Period parameter from the default REG_SZ string value **SpecialSkew** to REG_DWORD decimal value 24. You can also use a W32Time understandable string value to define synchronization frequency in the Period parameter. For example, you can set **DailySpecialSkew** to synchronize system time every 45 minutes until successful, then to synchronize once daily; **WeeklySpecialSkew** to synchronize every 7 days; **TridailySpecialSkew** to synchronize every 3 days; and **BidailySpecialSkew** to synchronize every 2 days.

By default, when a Win2K domain controller's W32Time service starts, the domain controller automatically works as an SNTP server regardless of whether the **LocalNTP** parameter's REG_DWORD value is 0 or 1. However, for a Win2K member server or workstation to function as an SNTP server, you must modify the **LocalNTP** parameter's default value from 0 to 1.

If you have multiple AD sites and the network bandwidth between the sites is limited and expensive, you can modify the **AvoidTimeSyncOnWan** parameter to save WAN bandwidth. Changing the parameter's value from 0 to 1 prevents a Win2K computer from synchronizing time with a time source in a different site.

By default, a Win2K domain controller is a time source. You can enable a Win2K member server or workstation to be a time source by adding the TimeSource parameter with the REG_DWORD value of 1 to the:

```
HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\LanmanServer\Parameters
```

subkey.

In your Win2K network, only the authoritative time server uses NTP synchronization. You can configure other Win2K computers in your network to use NTP synchronization. To set up this configuration, manually change the Type parameter of the:

```
HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\W32Time\Parameters
```

subkey from NT5DS to NTP and add the NTP server DNS names or IP addresses as a REG_SZ string value to the NtpServer parameter. Alternatively, you can use Win2K's Net Time command to configure W32Time to use an NTP server, and the command will automatically modify the necessary Registry parameters.

Win2K Net Time

Win2K's Net Time command lets you manually synchronize a computer's time with another Windows computer, a PDC, or a time source in the computer's local domain or another domain. In addition, this command lets you easily define, without touching the system's Registry, which NTP servers a system's W32Time service will use. Win2K Net Time uses remote procedure call (RPC) packets for time synchronization, and the command doesn't require NTP.

You can use Win2K's Net Time command to synchronize time with a time source in the network and perform other synchronization functions. Simply enter one of the following commands at a system's DOS prompt:

Windows Time Service

Mark E. Donaldson

`Net Time /set /y` synchronizes time with a time source in the local domain.

`Net Time /rtsdomain:domain_name /set /y` synchronizes time with a time source in a different domain.

`Net Time /domain:domain_name /set /y` synchronizes time with the PDC of the domain you specify.

`Net Time \\computer_name /setsntp:ntp_server_names_or_IP_addresses` synchronizes time with an NTP server.

`Net Time \\computer_name /setsntp` changes the W32Time synchronization type from NTP to NT5DS.

`Net Time \\computer_name/queriesntp` lets you query to discover whether a specific computer is using NTP servers and which NTP servers the computer is using.

You can also use the Net Time command to synchronize time from a specific computer:

```
Net Time \\win2kdcl.acme.com /set /y
```

If you don't use the /set and /y switches in the Net Time command, the command displays only the time it obtains from the time source. If you use the /set switch without the /y switch, the command prompts you to change your system time.