



ISA Server Topics

Articles & Tutorials

- Certification
- Configuration - Alt. Products & Platforms
- Configuration - General
- Configuration - Security
- General
- General Guides and Articles
- Installation & Planning
- Miscellaneous
- Non-ISAserver.org Tutorials
- Publishing

Authors

Books

Links

Message Boards

Newsletter Signup

Software

Featured Product



Featured Book



Pre-Order Today!

Poll

What would you like to see more of on ISAserver.org?

- Tutorials
- News
- Forum participation

Amy Babinchak's ISA/SBS Series: How to Synchronize SBS2003 Premium with an External Time Source

Site Search

Date Launched: Sep 30, 2004
 Last Updated: Sep 30, 2004
 Section: **Articles**
 Author: **Thomas Shinder**
Printable Version
 Rating: 4.6/5 - 20 Votes

1 2 3 4 5

Is the Windows Time Service on the SBS server giving your headaches? If so, Amy Babinchak has the cure! Check out this article for detailed advice on how to configure the SBS Windows Time Service and the ISA firewall to allow Time Service access to Internet Time Servers

**Amy Babinchak's ISA/SBS Series:
 How to Synchronize SBS2003 Premium with an External Time Source
 by
 Amy Babinchak**



**Harbor Computer Services
 Small Business Computer Specialists
 Office (248) 546-6056
 Mobile (248) 890-1794**

Got Questions?

Discuss this article at http://forums.isaserver.org/ultimatebb.cgi?ubb=get_topic:f=2:t=014031

Typically the need time synchronization is between your SBS server and the workstations. But, what happens when you need your SBS server to sync it's time with an external time source? In this article we'll show you how to configure SBS2003 Premium and ISA 2000 to synchronize with a public time server *and* provide the time for your workstations.

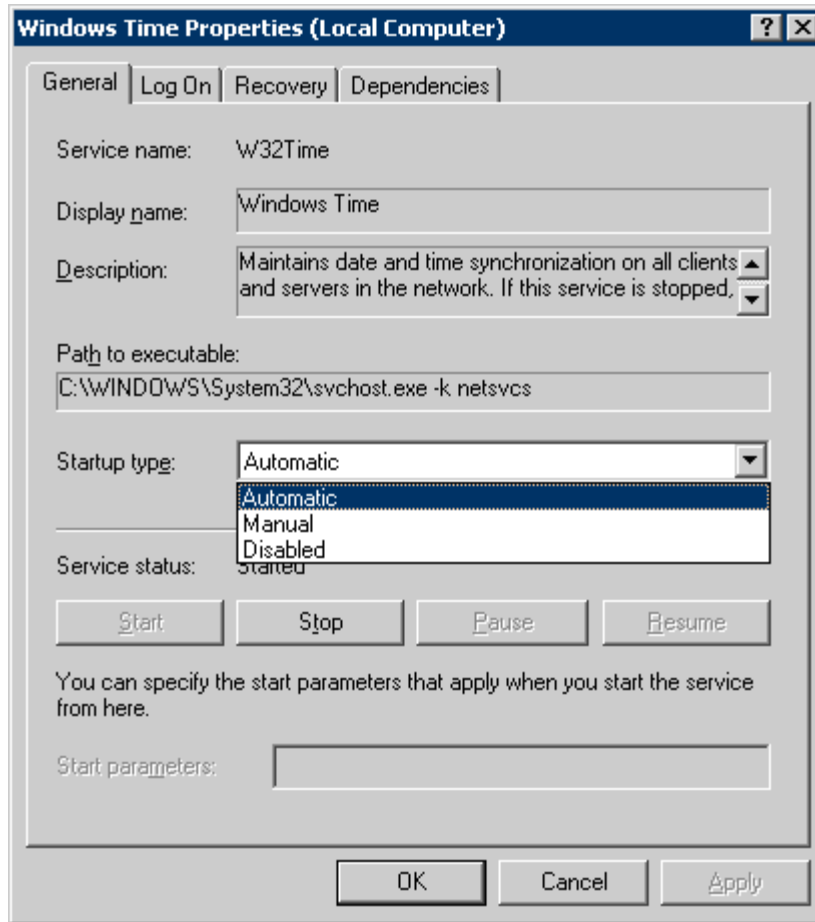
When working with Small Business Server we need to keep in mind all of things that SBS is. For this project we need to know that the Windows 2003 component of SBS2003 is the AD Forest Root and SBS2003 is also running ISA2000.

To begin, make sure the Windows Time service is running on your SBS server. To do this, open **Server Management** and in the right pane click **Monitoring and Reporting**. Next click the **Services** link. This will open up a new window called **Services**. Scroll down to the Windows Time service. Right click on the **Windows Time service** and select **Properties**. The Windows Time Properties dialog box will open. (fig. 1) Click the drop down Menu for **Startup Type** and select **Automatic** from the list. If the server is not already started, click the **Start** button to start the service. Click **OK** to close the **Windows Time Properties** dialog box. Close the **Services** window.

Figure 1

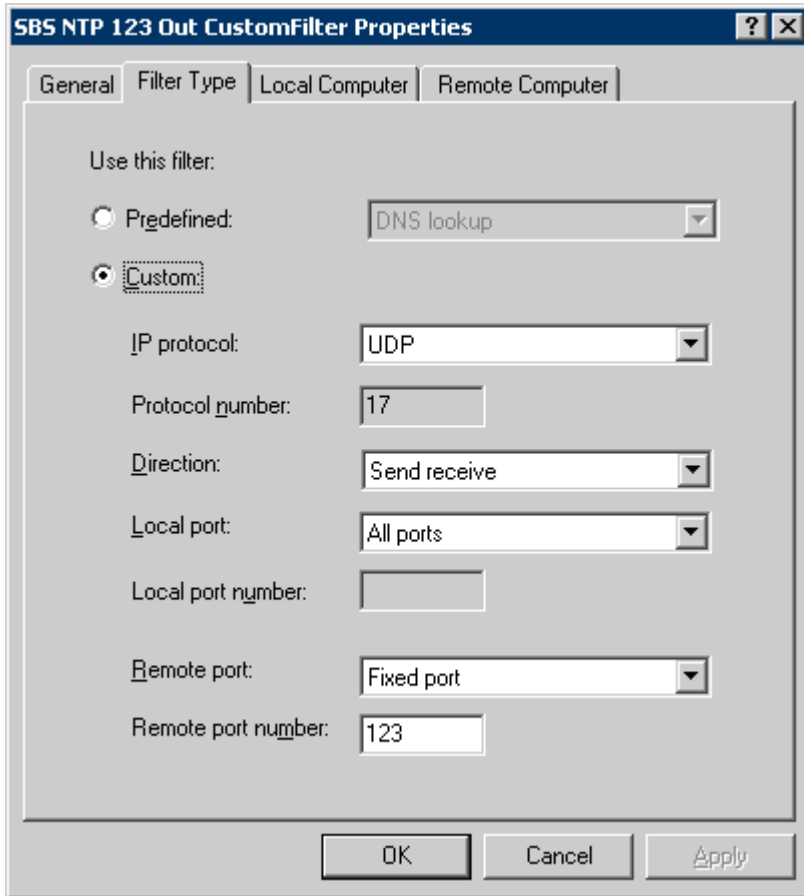
- Software reviews
- Case studies
- White papers
- FAQs
- Site customization
- Scripts & utils
- Other

Recommended Sites



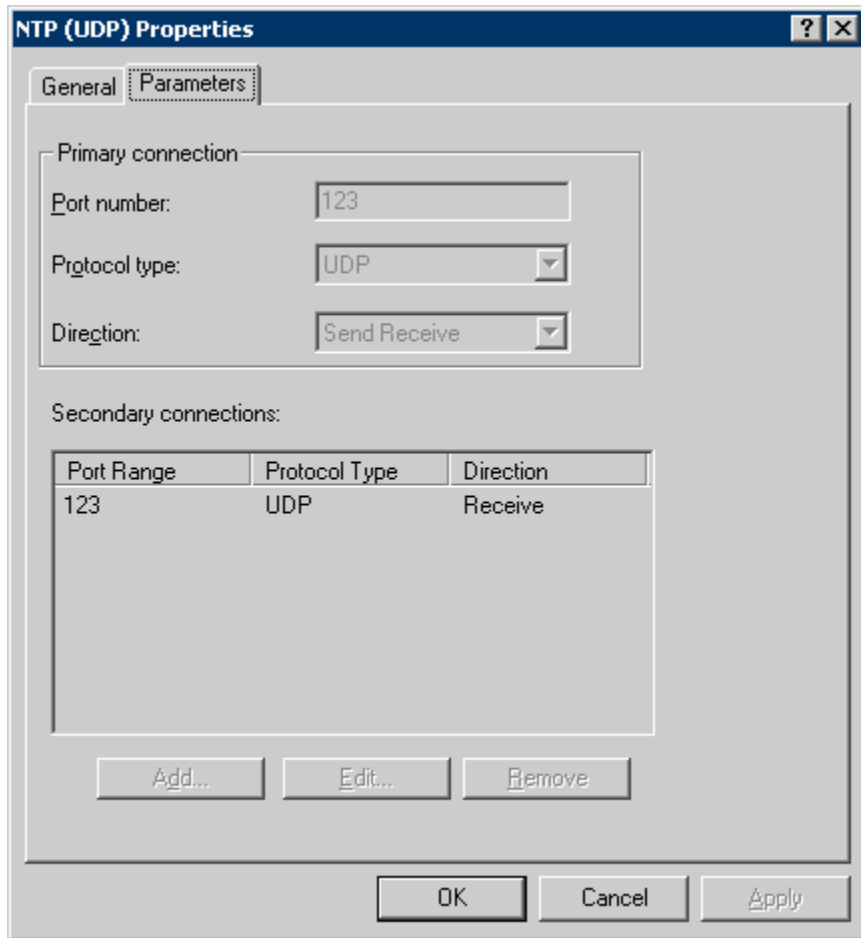
Now that the time service is running, the next step is to configure an ISA packet filter to allow the NTP packets through. To do this click on **Start, Programs, Microsoft ISA Server** and open the **ISA Management** console. Expand **Servers and Arrays**, <your server>, and **Access Policy**. Then click on the **IP Packet Filters** folder. In the right hand pane scroll down until you see the **SBS NTP 123 Out CustomFilter** item. Right click on this filter and choose **Properties**. The **SBS NTP 123 Out CustomFilter Properties** box will open. (fig. 2) Click on the **Filter Type** tab and make sure that your settings match those below in figure 2. Click **OK** to save your change and close the **Properties** box.

Figure 2:



Now we need to make sure that we have a corresponding Protocol Definition. To do this expand **Policy Elements** and click the **Protocol Definitions** folder. In the right hand pane scroll down to **NTP (UDP)**. Right click on the **NTP (UDP)** protocol definition and select **Properties**. The **NTP (UDP) Properties** box will open. Check to make sure that you setting match those of Figure 3.

Figure 3:



Click **OK** to exit the **NTP (UDP) Properties** box and save your changes.

Close the **ISA Server Manager** console.

Your time service is now working but it doesn't yet know where to find a public time server with which to synchronize. To determine which time server you would like to synchronize with, look on the Internet for free public time servers.

Microsoft Knowledgebase Article 262680 Titled: **A List of the Simple Network Time Protocol Time Servers That Are Available on the Internet** will be handy here. The KB article doesn't explain it very well, but you will want to select a Level 1 time server because your SBS server will be providing time services for your entire domain. Selecting one close to you and notifying them that you will be synchronizing with their server is good practice. Additional information on publicly available time servers, how they operate and information on how to get permission to sync with them is available here: <http://www.eecis.udel.edu/~mills/ntp/servers.html> Scroll down to the bottom of the page for a listing of available Level 1 servers. When you have selected a time server make note of the IP address and name of the server (FQDN).

Now open **Regedit**. (usual disclaimer here – backup the registry, making mistakes in here can really mess up your server, don't take my word for what you are about to do, be sure to verify what is written here with the Microsoft KB that it references.)

Have handy Microsoft Knowledgebase Article 816042 titled **How to configure the Windows Time service on a Windows Server 2003-based forest root PDC master computer**. Although the article doesn't reference SBS in its list of products that this article applies to, it should. Scroll down to the section titled: **Configuring the Windows Time service to use an external time source** and follow this through item 7. Item 7 should read Quit Registry Editor. The relevant section of the article is below for your reference. Note that in step 4 that here you can enter either the IP address of the time server or the DNS name. I prefer to use the IP address because I've found the DNS name to be unreliable.

Configuring the Windows Time service to use an external time source

To configure an internal time server to synchronize with an external time source, follow these steps:

1. Change the server type to NTP. To do this, follow these steps:

- a. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxPos

- b. In the right pane, right-click **MaxPosPhaseCorrection**, and then click **Modify**.
- c. In **Edit DWORD Value**, select **Decimal** in the **Base** box.
- d. In **Edit DWORD Value**, type *TimeInSeconds* in the **Value data** box, and then click **OK**.

Note *TimeInSeconds* is a placeholder for a reasonable value, such as 1 hour (3600) or 30 minutes (1800). The value that you select will depend upon the poll interval, network condition, and external time source.

- e. Locate and then click the following registry subkey:

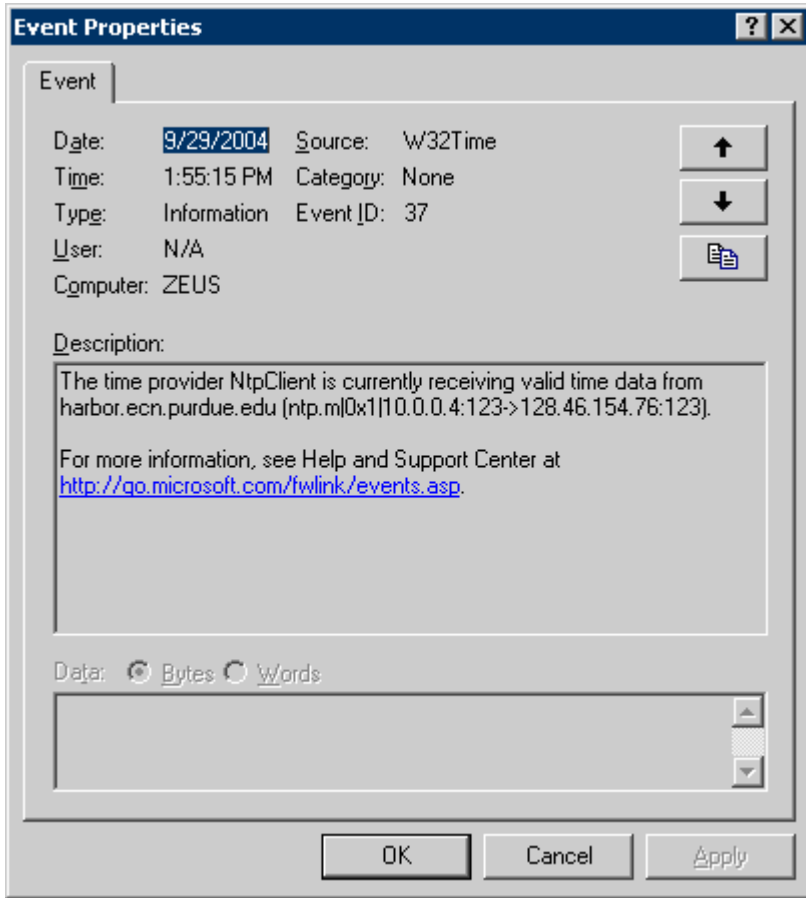
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxNeg

- f. In the right pane, right-click **MaxNegPhaseCorrection**, and then click **Modify**.
- g. In **Edit DWORD Value**, select **Decimal** in the **Base** box.
- h. In **Edit DWORD Value**, type *TimeInSeconds* in the **Value data** box, and then click **OK**.

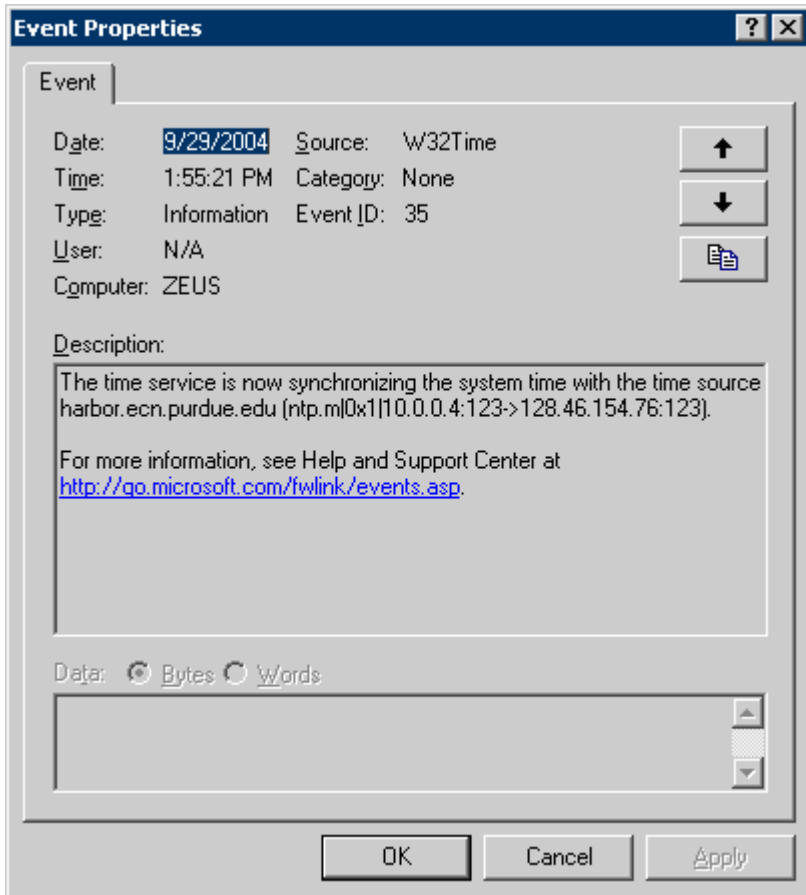
Note *TimeInSeconds* is a placeholder for a reasonable value, such as 1 hour (3600) or 30 minutes (1800). The value that you select will depend upon the poll interval, network condition, and external time source.

7. Quit Registry Editor.

Almost done. The only step left is to restart the Windows Time service. Once you have restarted the Windows Time service you should see the following happy time service events in the System Event log.



And



How to configure an authoritative time server in Windows Server 2003

Important This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, click the following article number to view the article in the Microsoft Knowledge Base:

[256986](#) Description of the Microsoft Windows Registry

Article ID
Last Review
Revision

IN THIS TASK

- [INTRODUCTION](#)
- [Configuring the Windows Time service to use an internal hardware clock](#)
- [Configuring the Windows Time service to use an external time source](#)
- [Troubleshooting](#)

MORE INFORMATION

- [Reliable time source configuration](#)
- [Manually-specified synchronization](#)
- [All available synchronization mechanisms](#)
- [Windows Time service registry entries](#)
- [REFERENCES](#)

INTRODUCTION

Windows includes W32Time, the Time Service tool that is required by the Kerberos authentication protocol. The purpose of the Windows Time service is to make sure that all computers that are running Microsoft Windows 2000 or later versions in an organization use a common time.

To guarantee appropriate common time usage, the Windows Time service uses a hierarchical relationship that controls authority, and the service does not permit loops. By default, Windows-based computers use the following hierarchy:

- All client desktop computers nominate the authenticating domain controller as their in-bound time partner.
- All member servers follow the same process that client desktop computers follow.
- All domain controllers in a domain nominate the primary domain controller (PDC) operations master as their in-bound time partner.
- All PDC operations masters follow the hierarchy of domains in the selection of their in-bound time partner.

In this hierarchy, the PDC operations master at the root of the forest becomes authoritative for the organization. We highly recommend the authoritative time server to gather the time from a hardware source. When you configure the authoritative time server to sync with a hardware source, there is no authentication. We also recommend that you reduce your time correction settings for your servers and stand-alone servers. The recommendations provide more accuracy and security to your domain.

[back to the top](#)

Configuring the Windows Time service to use an internal hardware clock

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. We cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

To configure the PDC master without using an external time source, change the announce flag on the PDC master. The PDC master is the forest root PDC master role for the domain. This configuration forces the PDC master to announce itself as a reliable time source using a complementary metal oxide semiconductor (CMOS) clock. To configure the PDC master by using an internal hardware clock, follow the following steps:

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags

3. In the right pane, right-click **AnnounceFlags**, and then click **Modify**.
4. In **Edit DWORD Value**, type **A** in the **Value data** box, and then click **OK**.
5. Quit Registry Editor.
6. At the command prompt, type the following command to restart the Windows Time service, and then press ENTER:

net stop w32time && net start w32time

Note The PDC master must not be configured to synchronize with itself. If the PDC master is configured to synchronize with itself, the logged in the Application log:

The time provider NtpClient cannot reach or is currently receiving invalid time data from 192.168.1.1 (ntp.m|0x0|192.168.1.1:123->'

No response has been received from Manual peer 192.168.1.1 after 8 attempts to contact it. This peer will be discarded as a time source attempt to discover a new peer from which to synchronize.

The time provider NtpClient is configured to acquire time from one or more time sources, however none of the sources are currently a contact a source will be made for 960 minutes. NtpClient has no source of accurate time.

When the PDC master runs without using an external time source, the following event is logged in the Application log:

Time Provider NtpClient: This machine is configured to use the domain hierarchy to determine its time source, but it is the PDC emulator the root of the forest, so there is no machine above it in the domain hierarchy to use as a time source. It is recommended that you either time service in the root domain, or manually configure the PDC to synchronize with an external time source. Otherwise, this machine authoritative time source in the domain hierarchy. If an external time source is not configured or used for this computer, you may check NtpClient.

This text is a reminder to use an external time source and can be ignored.

[back to the top](#)

Configuring the Windows Time service to use an external time source

To configure an internal time server to synchronize with an external time source, follow these steps:

1. Change the server type to NTP. To do this, follow these steps:

- a. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
- b. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type

Was NoSync

- c. In the right pane, right-click **Type**, and then click **Modify**.
- d. In **Edit Value**, type **NTP** in the **Value data** box, and then click **OK**.

2. Set AnnounceFlags to 5. To do this, follow these steps:

- a. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags

- b. In the right pane, right-click **AnnounceFlags**, and then click **Modify**.
- c. In **Edit DWORD Value**, type **5** in the **Value data** box, and then click **OK**.

Was "a"

3. Enable NTPServer. To do this, follow these steps:

- a. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer\Enabled

- b. In the right pane, right-click **Enabled**, and then click **Modify**.
- c. In **Edit DWORD Value**, type **1** in the **Value data** box, and then click **OK**.

4. Specify the time sources. To do this, follow these steps:

- a. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\NtpServer

- b. In the right pane, right-click **NtpServer**, and then click **Modify**.
- c. In **Edit Value**, type *Peers* in the **Value data** box, and then click **OK**.

was time.windows.com,0x1

ntp2.usno.navy.mil USE 192.5.41.209

Note *Peers* is a placeholder for a space-delimited list of peers from which your computer obtains time stamps. Each DNS name must be unique. You must append **,0x1** to the end of each DNS name. If you do not append **,0x1** to the end of each DNS name made in step 5 will not take effect.

5. Select the poll interval. To do this, follow these steps:

a. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval

b. In the right pane, right-click **SpecialPollInterval**, and then click **Modify**.

was e10 e10=1 hour hex

c. In **Edit DWORD Value**, type *TimeInSeconds* in the **Value data** box, and then click **OK**.

Note *TimeInSeconds* is a placeholder for the number of seconds that you want between each poll. A recommended value is 900. This value configures the Time Server to poll every 15 minutes.

6. Configure the time correction settings. To do this, follow these steps:

a. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxPosPhaseCorrection

b. In the right pane, right-click **MaxPosPhaseCorrection**, and then click **Modify**.

c. In **Edit DWORD Value**, click to select **Decimal** in the **Base** box.

d. In **Edit DWORD Value**, type *TimeInSeconds* in the **Value data** box, and then click **OK**.

Note *TimeInSeconds* is a placeholder for a reasonable value, such as 1 hour (3600) or 30 minutes (1800). The value that you depend upon the poll interval, network condition, and external time source.

e. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxNegPhaseCorrection

f. In the right pane, right-click **MaxNegPhaseCorrection**, and then click **Modify**.

g. In **Edit DWORD Value**, click to select **Decimal** in the **Base** box.

h. In **Edit DWORD Value**, type *TimeInSeconds* in the **Value data** box, and then click **OK**.

Note *TimeInSeconds* is a placeholder for a reasonable value, such as 1 hour (3600) or 30 minutes (1800). The value that you depend upon the poll interval, network condition, and external time source.

7. Quit Registry Editor.

8. At the command prompt, type the following command to restart the Windows Time service, and then press ENTER:

```
net stop w32time && net start w32time
```

Troubleshooting

For the Windows Time service to function correctly, the networking infrastructure must function correctly. The most common problems with the Windows Time service include the following:

- There is a problem with TCP/IP connectivity, such as a dead gateway.
- The Name Resolution service is not working correctly.
- The network is experiencing high volume delays, especially when synchronization occurs over high-latency wide area network (WAN).
- The Windows Time service is trying to synchronize with inaccurate time sources.

We recommend that you use the Netdiag.exe utility to troubleshoot network-related issues. Netdiag.exe is part of the Windows Server package. See Tools Help for a complete list of command-line parameters that you can use with Netdiag.exe. If your problem is still not resolved, contact Microsoft Support Services when you turn on the Windows Time service debug log.

For a complete list of Microsoft Product Support Services phone numbers and information about support costs, visit the following Microsoft Support Services page:

[http://support.microsoft.com/default.aspx?scid=fh;\[LN\];CONTACTMS](http://support.microsoft.com/default.aspx?scid=fh;[LN];CONTACTMS)

Note In special cases, charges that are ordinarily incurred for support calls may be canceled if a Microsoft Support Professional determines that the problem is a Microsoft product issue.