How to disable IPv6 or its components in Windows

https://support.microsoft.com/en-us/kb/929852

Important Internet Protocol version 6 (IPv6) is a mandatory part of Windows Vista and later versions. We do not recommend that you disable IPv6 or its components, or some Windows components may not function. Additionally, system startup will be delayed for 5 seconds if IPv6 is disabled by incorrectly setting the DisabledComponents registry setting to a value of 0xffffffff. The correct value should be 0xff. For more information, see the "What are Microsoft's recommendations about disabling IPv6?" question in IPv6 for Microsoft Windows: Frequently Asked Questions http://technet.microsoft.com/en-us/network/cc987595.aspx)

Automatically disable or re-enable IPv6 or its components

Click the **Download** button for the procedure that you want to run. Then, click Run or Open in the File Download dialog box, and then follow the steps in the easy fix wizard.

Disable IPv6	**Prefer IPv4 over IPv6 in prefix policies**	**Disable IPv6 on all nontunnel interfaces**	**Disable IPv6 on all tunnel interfaces**	**Disable IPv6 on nontunnel interfaces (except the loopback) and on IPv6 tunnel interface**
Re-enable IPv6	**Prefer IPv6 over IPv4 in prefix policies**	**Re-enable IPv6 on all nontunnel interfaces**	**Re-enable IPv6 on all tunnel interfaces**	**Re-enable IPv6 on nontunnel interfaces and on IPv6 tunnel interfaces**

Notes for wizard

- This wizard may be in English only. However, the automatic fix also works for other language versions of Windows.
- If you're not on the computer that has the problem, save the easy fix solution to a flash drive or a CD, and then run it on the computer that has the problem.

More information

See KB3014406 if you encounter startup delay after you disable IPv6 in Windows 7 SP1 or Windows Server 2008 R2 SP1.

Manually disable or re-enable IPv6 or its components

Disable IPv6
You can disable IPv6 on the host computer through the **DisabledComponents** registry value. The **DisabledComponents** registry value affects all network interfaces on the host.

Important Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, back up the registry for restoration in case problems occur.

To disable certain IPv6 components, follow these steps:

1. Click **Start**, type regedit in the **Start Search** box, and then click **regedit.exe** in the **Programs** list.
2. In the **User Account Control** dialog box, click **Continue**.
3. In Registry Editor, locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters

4. Double-click **DisabledComponents** to change the **DisabledComponents** entry.

   Note If the **DisabledComponents** entry is unavailable, you must create it. To do this, follow these steps:
   1. In the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
   2. Type DisabledComponents, and then press Enter.
   3. Double-click **DisabledComponents**.
5. Type any of the following values in the Value data field to configure the IPv6 protocol to the intended state, and then click **OK**:
   1. Type 0 to re-enable all IPv6 components (Windows default setting).
   2. Type 0xff to disable all IPv6 components except the IPv6 loopback interface. This value also configures Windows to prefer using IPv4 over IPv6 by changing entries in the prefix policy table. For more information, see Source and destination address selection.
   3. Type 0x20 to prefer IPv4 over IPv6 by changing entries in the prefix policy table.
   4. Type 0x10 to disable IPv6 on all nontunnel interfaces (both LAN and Point-to-Point Protocol [PPP] interfaces).
   5. Type 0x01 to disable IPv6 on all tunnel interfaces. These include Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 6to4, and Teredo.
   6. Type 0x11 to disable all IPv6 interfaces except for the IPv6 loopback interface.

Use the DisabledComponents registry value to verify whether IPv6 is disabled. To do this, run the following command at a Windows command prompt:

```
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters /v DisabledComponents
```

When you do this, you may receive the following error message:
ERROR: The system was unable to find the specified registry key or value.
If you receive this error message, the DisabledComponents registry value is not set. If the DisabledComponents value is set, it overrides the settings in the connection properties.

Disable IPv6 on a specific network adapter
You can do this by unbinding the adapter in the **Local Area Connection Properties** dialog box:

1. Click **Start**, and then click **Control Panel**.
2. Click **Network and Sharing Center**.
3. In the **View your active networks** area, click **Local Area Connection**, and then click **Properties**.
4. On the **Networking** tab, clear the **Internet Protocol Version 6 (TCP/IPv6)** check box, and then click **OK**.

Note The **Internet Protocol Version 6 (TCP/IPv6)** check box affects only the specific network adapter and will unbind IPv6 from the selected network adapter. To disable IPv6 on the host, use the **DisabledComponents** registry value. The **DisabledComponents** registry value does not affect the state of the check box. Therefore, even if the **DisabledComponents** registry key is set to disable IPv6, the check box in the **Networking** tab for each interface can still be checked. This is expected behavior.

Prefer IPv6 over IPv4 in prefix policies

1. Find the current value data of DisabledComponents.
2. Change the data to binary data. It will be a 32-bit binary value.

3. Find the sixth bit of the data, and then set it to 0. Do not change any other bits. For example, if the current data is 11111111111111111111111111111111, the new data should be 11111111111111111111111111011111.
4. Change the data from binary to hexadecimal.
5. Set the hexadecimal value as the new value data for DisabledComponents.

Re-enable IPv6 on all nontunnel interfaces

1. Find the current value data of DisabledComponents.
2. Change the data to binary data. It will be a 32-bit binary value.
3. Find the fifth bit of the data, and then set it to 0. Do not change any other bits. For example, if the source data is 11111111111111111111111111111111, the new data should be 11111111111111111111111111101111.
4. Change the data from binary to hexadecimal.
5. Set the hexadecimal value as the new value data for DisabledComponents.

Re-enable IPv6 on all tunnel interfaces

1. Find the current value data of DisabledComponents.
2. Change the data to binary data. It will be a 32-bit binary value.
3. Find the first bit of the data, and then set it to 0. Do not change any other bits. For example, if the source data is 11111111111111111111111111111111, the new data should be 11111111111111111111111111111110.
4. Change the data from binary to hexadecimal.
5. Set the hexadecimal value as the new value data for DisabledComponents.

Re-enable all IPv6 interfaces except for the IPv6 loopback interface

1. Find the current value data of DisabledComponents.
2. Change the data to binary data. It will be a 32-bit binary value.
3. Find the first bit of the data and the fifth bit of the data, and then set them both to 0. Do not touch any other bits. For example, if current data is 11111111111111111111111111111111, the new data should be 11111111111111111111111111101110.
4. Change the data from binary to hexadecimal.
5. Set the hexadecimal value as the new value data for DisabledComponents.

Notes

- Administrators must create an .admx file to expose the settings in step 5 in a Group Policy setting.
- You must restart your computer for these changes to take effect.
- value other than 0x0 or 0x20 causes the Routing and Remote Access service to fail after this change takes effect.

About the 6to4 tunneling protocol

By default, the 6to4 tunneling protocol is enabled in Windows 7, Windows Vista, Windows Server 2008 R2, and Windows Server 2008 when an interface is assigned a public IPv4 address (that is, an IPv4 address that is not in the ranges 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16). 6to4 automatically assigns an IPv6 address to the 6to4 tunneling interface for each such address that is assigned, and 6to4

will dynamically register these IPv6 addresses on the assigned DNS server. If this behavior is not desired, we recommend that you disable IPv6 tunnel interfaces on the affected hosts.
Properties

Article ID: 929852 - Last Review: 09/25/2015 09:06:00 - Revision: 34.0

Applies to

- Windows 7 Enterprise
- Windows 7 Home Basic
- Windows 7 Home Premium
- Windows 7 Professional
- Windows 7 Ultimate
- Windows 7 Starter
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Standard
- Windows Vista Enterprise
- Windows Vista Enterprise 64-bit Edition
- Windows Vista Home Basic 64-bit Edition
- Windows Vista Home Premium 64-bit Edition
- Windows Vista Ultimate 64-bit Edition
- Windows Vista Business
- Windows Vista Business 64-bit Edition
- Windows Vista Home Basic
- Windows Vista Home Premium
- Windows Vista Starter
- Windows Vista Ultimate
- Windows Server 2008 Datacenter
- Windows Server 2008 Enterprise
- Windows Server 2008 Standard
- Windows Server 2012 R2 Standard
- Windows Server 2012 Standard
- Windows Server 2012 Datacenter
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 R2 Essentials
- Windows Server 2012 R2 for Embedded Systems
- Windows Server 2012 R2 Foundation

Keywords:

- kbnetwork kbregistry kbexpertiseinter kbhowto kbinfo kbfixme kbmsifixme kbconsumer kbquadranttechsupp KB929852