Guidance for configuring IPv6 in Windows for advanced users

Applies to: Windows 10, version 1909, Windows Server, version 1909 (Datacenter, Standard), Windows 10, version 1903, More

Introduction

Windows Vista, Windows Server 2008, and later versions of Windows implement RFC 3484 and use a prefix table to determine which address to use when multiple addresses are available for a Domain Name System (DNS) name.

By default, Windows favors IPv6 global unicast addresses over IPv4 addresses.

Summary

It is common for IT administrators to want to disable IPv6. This is often because of some unknown, networking-related issue, such as a name resolution issue.

Important Internet Protocol version 6 (IPv6) is a mandatory part of Windows Vista and Windows Server 2008 and newer versions. We do

not recommend that you disable IPv6 or its components. If you do, some Windows components may not function.

We recommend that you use "Prefer IPv4 over IPv6" in prefix policies instead of disabling IPV6.

Automatically disable or re-enable IPv6 or its components

To automatically disable or re-enable IPv6 or its components, follow these steps:

1. Click the **Download** button for the procedure that you want to run.
2. Click **Run** or **Open** in the **File Download** dialog box.
3. Follow the steps in the easy fix wizard.

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
Download	Download	Download	Download

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
Download	Download	Download	Download

Notes for wizard

Use registry key to configure IPv6

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 configure IPv6, modify the following registry value based on the following table.

```
Location:          HKEY_LOCAL_MACHINE\SYSTEM\CurrentContr
olSet\Services\Tcpip6\Parameters\
Name:              DisabledComponents
Type:              REG_DWORD
Min Value:         0x00
Max Value:         0xFF (IPv6 disabled)
```

IPv6 Functionality	Registry value	Comments
Prefer IPv4 over IPv6	Dec 32 Hex 0x20 Bin xx1x xxxx	Recommended instead of disabling it.
Disable IPv6	Dec 255 Hex 0xFF Bin 1111 1111	See KB3014406 if you encounter startup delay after you disable IPv6 in Windows 7 SP1 or Windows Server 2008 R2 SP1. 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. 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.
disable IPv6 on all nontunnel interfaces	Dec 16 Hex 0x10 Bin xxx1 xxxx	
disable IPv6 on all tunnel interfaces	Dec 1 Hex 0x01 Bin xxxx xxx1	
disable IPv6 on all nontunnel interfaces (except the loopback) and on IPv6 tunnel interface	Dec 17 Hex 0x11 Bin xxx1 xxx1	

prefer IPv6 over IPv4	Bin xx0x xxxx	
re-enable IPv6 on all nontunnel interfaces	Bin xxx0 xxxx	
re-enable IPv6 on all tunnel interfaces	Bin xxx xxx0	
Re-enable IPv6 on nontunnel interfaces and on IPv6 tunnel interfaces	Bin xxx0 xxx0	

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 0 or 32 causes the Routing and Remote Access service to fail after this change takes effect.

By default, the 6to4 tunneling protocol is enabled in Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 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 dynamically registers 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.

You can also follow these steps to modify the registry key:

1. Open an administrative Command Prompt window.
2. Run the following command:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\Tcpip6\Parameters" /v DisabledComponents /
t REG_DWORD /d <value> /f
```

Note Replace the value with the corresponding value in the previous table.

How to calculate the registry value

Windows use bitmasks to check the **DisabledComponents** values and determine whether a component should be disabled.

To learn which component each bit (from low to high) controls, refer to the following table.

Tunnel	Disable tunnel interfaces
Tunnel6to4	Disable 6to4 interfaces
TunnelIsatap	Disable Isatap interfaces
TunnelTeredo	Disable Teredo interfaces
Native	Disable native interfaces (also PPP)
PreferIpv4	Prefer IPv4 in default prefix policy
TunnelCp	Disable CP interfaces
TunnelIpTls	Disable IP-TLS interfaces

For each bit, 0 means false and 1 means true. Refer to the following table for an example.

	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
Disable tunnel interfaces	0	0	1	1
	0	0	0	0

Disable 6to4 interfaces				
Disable Isatap interfaces	0	0	0	0
Disable Teredo interfaces	0	0	0	0
Disable native interfaces (also PPP)	0	1	0	1
Prefer IPv4 in default prefix policy.	1	0	0	0
Disable CP interfaces	0	0	0	0
Disable IP-TLS interfaces	0	0	0	0
Binary	0010 0000	0001 0000	0000 0001	0001 0001
Hexadecimal	0x20	0x10	0x01	0x11

Reference

For more information, see the following article:

969029 The functionality for source IP address selection in Windows Server 2008 and in Windows Vista differs from the corresponding functionality in earlier versions of Windows

For information about RFC 3484, see Default Address Selection for Internet Protocol version 6 (IPv6).

For more informaiton about how to set IPv4 precedence over IPv6, see Using SIO_ADDRESS_LIST_SORT.

For information about RFC 4291, see IP Version 6 Addressing Architecture.

For more informaiton about the related issues, see the articles below:

Example 1: On Domain Controllers, you might run into where LDAP over UDP 389 will stop working.
See 816103 How to use Portqry to troubleshoot Active Directory connectivity issues

Example 2: Exchange Server 2010, you might run into problems where Exchange will stop working.
See Arguments against disabling IPv6 and Disabling IPv6 And Exchange – Going All The Way.

Example 3: Failover Clusters
See What is a Microsoft Failover Cluster Virtual Adapter anyway? and Failover Clustering and IPv6 in Windows Server 2012 R2.

Tools to help with network trace

Microsoft Message Analyzer

Microsoft Network Monitor 3.4 (archive)
Warning Netmon 3.4 is not compatible with Windows Server 2012 or newer OS when LBFO NIC teaming is enabled. Instead, use "Message Analyzer."

Last Updated: Nov 12, 2019