Smart multi-homed name resolution is a DNS related feature that Microsoft introduced in Windows 8 and implemented in Windows 10 as well.

The feature is designed to speed up DNS resolution on a device running Windows 8 or newer by sending DNS requests across all available network adapters. Microsoft refined the feature in Windows 10 as it selects the information that is returned the fastest automatically.

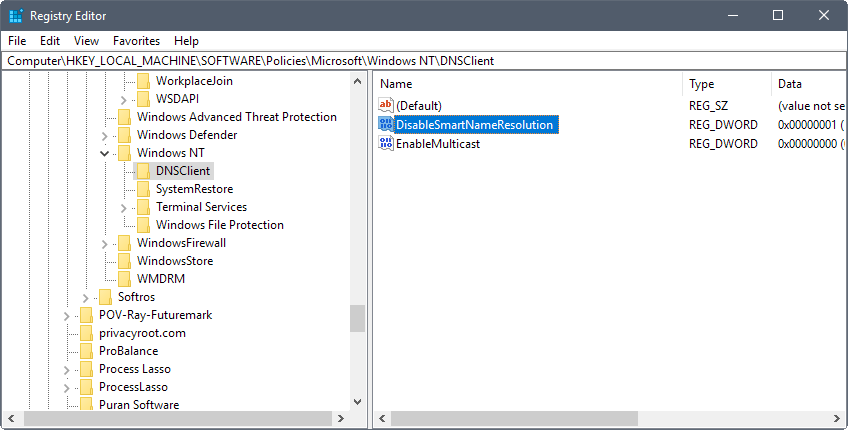
While the feature makes sense from a performance point of view, it introduces an issue from a privacy one.

If you connect to a VPN network on a Windows machine for instance, smart multi-homed name resolution may lead to DNS leakage. Since requests are sent out to all network adapters at the same time, all configured DNS servers receive the requests and with them information on the sites that you visit.

Turn off smart multi-homed name resolution in Windows

Microsoft introduced a Registry key and policy to manage the feature in Windows 8.

Registry (Windows 8.x only)

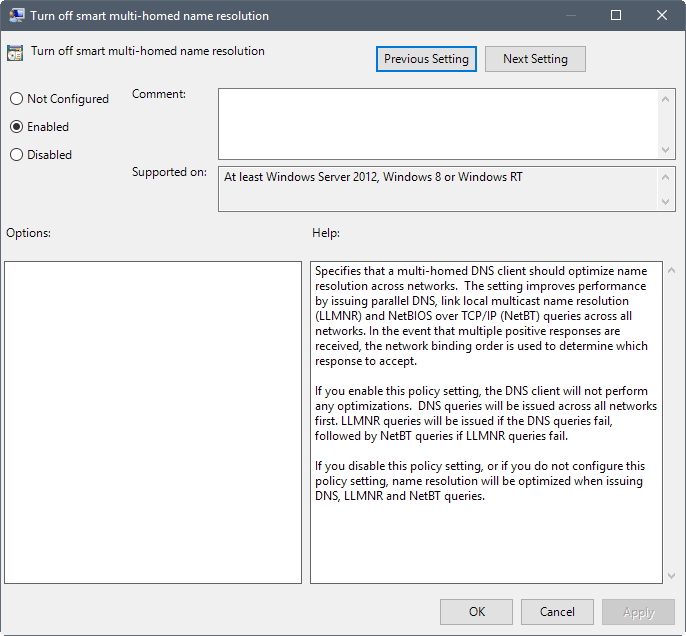


**Note**: manipulating the Registry may lead to issues if done incorrectly. It is suggested that you create a backup of the Windows Registry before you continue. This can be done by selecting a Registry Hive in the Registry Editor, and then File > Export from the menu bar.

1. Open the Windows Registry Editor. One easy option to do that is to tap on the Windows-key, type regedit.exe, and hit the Enter-key.  Windows throws an UAC prompt which you need to confirm.
2. Go to HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient
3. If the Dword value DisableSmartNameResolution exists already, make sure it is set to 1.
4. If it does not exist, right-click on DNSClient, and select New > Dword (32-bit) Value from the menu.
5. Name it DisableSmartNameResolution.
6. Set its value to 1. You may turn the feature back on at any time by setting the value to 0, or by deleting the Dword value.
7. Go to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
8. If the Dword value DisableParallelAandAAAA  exists already, make sure its value is set to 1.
9. If the value does not exist, right-click on Parameters, and select New > Dword (32-bit) Value.
10. Name it DisableParallelAandAAAA.
11. Set the value of the Dword to 1. You can turn the feature back on by setting the value to 0, or by deleting the value.

I have created a Registry file that makes both changes to the Windows Registry when executed. You can download it with a click on the following link: [disable-smart-name-resolution.zip](https://www.ghacks.net/download/136552/)

Group Policy (Windows 8 and Windows 10)



The Registry key that worked under Windows 8 does not seem to work under Windows 10 anymore. Windows 10 users and admins may set a policy however to turn the feature off.

Specifies that a multi-homed DNS client should optimize name resolution across networks. The setting improves performance by issuing parallel DNS, link local multicast name resolution (LLMNR) and NetBIOS over TCP/IP (NetBT) queries across all networks. In the event that multiple positive responses are received, the network binding order is used to determine which response to accept.

Note that the Group Policy Editor is only available in professional editions of Windows 10. Windows 10 Home users may want to [check out Policy Plus](https://www.ghacks.net/2017/07/25/policy-plus-brings-group-policy-to-all-windows-editions/) that introduces policy editing to Home editions of Windows 10.

1. Do the following to open the Group Policy Editor in Windows: Tap on the Windows-key on the keyboard, type gpedit.msc, and hit the Enter-key on the keyboard.
2. Go to Computer Configuration > Administrative Templates > Network > DNS Client > Turn off smart multi-homed name resolution.
3. Set the policy to enabled, to disable the smart multi-homed name resolution feature of the system.

If you enable this policy setting, the DNS client will not perform any optimizations. DNS queries will be issued across all networks first. LLMNR queries will be issued if the DNS queries fail, followed by NetBT queries if LLMNR queries fail.

Closing Words

Some DNS clients that you may run on Windows machines come with DNS leak protection to prevent these leaks. [OpenDNS](https://support.opendns.com/hc/en-us/articles/227988027-Preventing-circumvention-of-OpenDNS-with-firewall-rules) users may enable the block-outside-dns option for instance in the client to do so.